Руководство по подключению IP-камеры N120S

Оглавление

Глава 1. Меры предосторожности

Перед использованием устройства необходимо помнить ниж[illegible]ее.

Данный продукт удовлетворяет всем требованиям безопасно[illegible]юбой электроприбор, в случае неправильного использования может в[illegible] пожар, чт[illegible]вою очередь, может повлечь за собой серьезные последствия. **Во[illegible]ие не[illegible]ных случаев обязательно изучите инструкцию!**

ВНИМАНИЕ!
Используйте только совместимые устройства. Экспл[illegible]ия уст[illegible]тв[illegible] одобренных производителем, недопустима.

Соблюдайте инструкцию по эксплуатации!

Избегайте длительного использовани[illegible] хранения ка[illegible] в неблагоприятных условиях:

- При слишком высоких или низких [illegible]ратур[illegible]ая температура устройств от -10 до +50 °С).
- Избегайте попадания пря[illegible]ечных[illegible] в течение длительного времени, а также нахождения поблизости [illegible]льных[illegible]огревательных приборов.
- Избегайте близости [illegible]водой или источ[illegible]ами влажности.
- Избегайте близост[illegible]йствами, об[illegible]дающими большим электромагнитным эффектом.
- Недопустима установка камеры [illegible]сильной вибрацией.

ВНИМАНИЕ!
В случае неисправности кам[illegible]ным центром ООО «НПП «Бевард».

В случ[illegible]ой работы камеры:

- П[illegible]нару[illegible]и д[illegible] или необычного запаха.
- П[illegible]па[illegible]и во[illegible] посторонних объектов внутрь.
- Пр[illegible]ли повреждении корпуса:

[illegible]лните следующие действия:

- [illegible]камеру от источника питания и отсоедините все остальные провода.
- [illegible]вяжи[illegible]с сервисным центром ООО «НПП «Бевард». Контактные данные Вы [illegible]ож[illegible]айти на сайте http://www.beward.ru/.

Транспортировка

При транспортировке положите камеру в упаковку производителя [illegible]бой другой материал соответствующего качества и ударопрочности.

Вентиляция

Во избежание перегрева ни в коем случае не блокируйте цирку[illegible] [illegible]округ камеры!

Чистка

Используйте мягкую сухую ткань для про[illegible] вне[illegible]ерхностей. Для трудновыводимых пятен используйте небольшое коли[illegible]стящего средства, после чего насухо вытрите поверхность.

Не используйте летучие растворител[illegible] спиртосод[illegible]жащие средства или бензин, так как они могут повредить корпус [illegible]

Глава 2. Общие сведения

BEWARD N120S – это компактная IP-видеокамера с раз[illegible] 640x480, встроенным Wi-Fi-модулем стандарта IEEE 802.11 b/[illegible]овым видеоизображением в форматах H.264/MPEG-4/MJPEG, встроен[illegible] микрофоно[illegible]этом для установки карты памяти стандарта MicroSD и высокочувствите[illegible]ОП-сен[illegible]м.

[illegible] 1

IP-камера BEWARD N[illegible] позволяет про[illegible]атривать видео в реальном времени через стандартный Интерне[illegible] Особен[illegible]ью камеры является возможность использования профилей настр[illegible]ажения, которые Вы можете сконфигурировать зар[illegible]е. Каждый проф[illegible]ль настраивается индивидуально, благодаря чему достигается опт[illegible]отношение [illegible]чества изображения и использования полосы пропускания.

Камера [illegible] выдавать видеопоток в различных форматах сжатия: H.264/MPEG4[illegible]ат кодирования H.264 является идеальным для использования камеры в с[illegible]с ог[illegible]ченн[illegible]полосой пропускания. При его использовании достигается наименьши[illegible]фик[illegible] хоро[illegible]ачество изображения. Формат MJPEG предназначен для записи и от[illegible]наилучшем качестве, но при этом требует больших сетевых ресу[illegible] мест[illegible] диске при записи.

[illegible]ра N120S подключается к сети при помощи проводного интерфейса 10BASE-[illegible]0BA[illegible]et, а также с использованием беспроводного соединения стандарта Wi-[illegible]E[illegible].11 [illegible] Для удобства и быстроты подключения камеры к беспроводной сети ка[illegible]олн[illegible] функцией WPS. При использовании данной функции для установления беспро[illegible]оединения достаточно последовательно нажать кнопки WPS на точке доступа (при[illegible]условии поддержки данной функции со стороны устройства) и на корпусе камеры. Спустя некоторое время камера автоматически будет подключена к беспроводной сети.

Поддержка карт памяти типа MicroSD позволяет сделать сис дения еще более надежной: важная информация не пропадет при поте единения, ном объеме она может быть сохранена на карте памяти. В дал ее мож удет воспроизвести как непосредственно с карты, так и удаленно после у тех еских проблем сети.

2.1. Особенности IP-видеокамеры BEWAR 20S

- 1/4" КМОП-сенсор с прогрессивным сканир
- Поддержка карт памяти типа MicroSD/SDHC (до
- Встроенный Wi-Fi-модуль 802.11b/g/n с поддержкой W
- Профессиональное программное о каналов) в комплекте
- Одновременное многоформатное .264/MPEG4/MJPEG) для обеспечения оптимального отображе пи файлов
- Возможность просмотра за ых фа посредственно из веб-интерфейса с помощью встроенного п
- Встроенный микрофон
- Встроенный детекто жения и детект звука
- Отправка кадров и в ной почте и на FTP
- Запись на внешний файлов исле и в папку с открытым доступом на ПК, с уста енной ОС Windo или Linux)
- Поддержка

2.2. Осн актеристики

- Св ный элемент: OmniVision, 1/4'' КМОП с прогрессивным ск ван
- О 2 f3 2.0 (угол обзора 56° по горизонтали)
- Раз , 640x360, 320x240, 160x120
- вствит : 0.2 лк при F2.0
- дров: до 30 кадров в секунду для всех разрешений
- дирования: H.264, MPEG-4, MJPEG
- Однов нное кодирование в форматах: H.264, MPEG-4, MJPEG
- онний аудиоканал; компрессия: G.711 μ-law/α-law, AMR
- нный Wi-Fi-модуль IEEE 802.11 b/g/n с функцией WPS

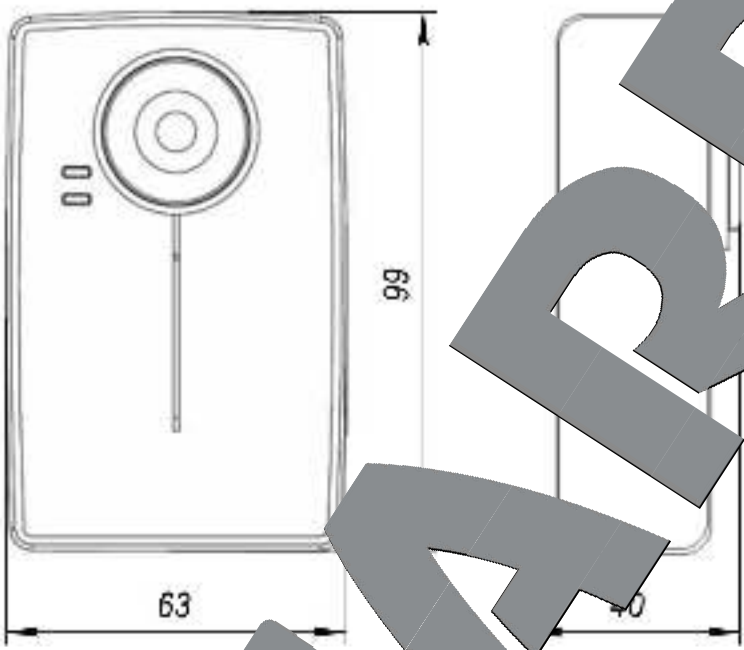
- Поддерживаемые протоколы: Bonjour, TCP/IP, DHCP, PPPoE, ARP, IGMP, ICMP, FTP, SMTP, DNS, DDNS, NTP, UPnP, RTSP, RTP, RTCP, HTTP, HT[illegible] SSL, UDP
- Питание: 5В, 0.6А (постоянный ток)
- Рабочая температура: от -10 до +50°C
- Влажность окружающей среды: 20-80% (без образовани[illegible]та)
- Поддержка отраслевого стандарта ONVIF v2.20

2.3. Комплект поставки

- IP-видеокамера с установленным объективо[illegible], f3.6 м[illegible]
- Кабель патч-корд (длина 1 м)
- Источник питания постоянного тока 5В, 1А
- Кронштейн
- Комплект крепежа
- CD-диск с программным обеспечен[illegible] докум[illegible]

Глава 3. Внешний вид

3.1. Размеры камеры N120S



...с. 3.1

Размеры указаны в миллиметрах.

3.2. Основные элем

Рис. 3.2

1 – Объектив: объектив с креплением M12.

При размытом изображении необходимо настроить фокус ка[illegible] Для этого вращайте кольцо настройки фокуса, пока не добьетесь приемлемого [illegible]

ПРИМЕЧАНИЕ!
Изначально объектив камеры сфокусирован и не требует дополнительной [illegible]

2 – Индикатор питания: загорается после подклю[illegible] к источни[illegible] питания.

- **Индикатор питания горит красным**: к IP[illegible]ре по[illegible]че[illegible] питание, идет загрузка системы.
- **Индикатор питания горит синим**: загрузка IP[illegible]ве[illegible]шена, камера готова к работе.
- **Индикатор питания мигает ф[illegible] цветом**[illegible] идет соединение с беспроводной сетью Wi-Fi посре[illegible]дикатор мигает во время процесса обновления прошивки ка[illegible] не о[illegible] питание и не закрывайте окно браузера до завершени[illegible]рошивк[illegible] загрузки камеры!
- **Индикатор питания не** [illegible] IP-[illegible] не подключено питание, либо отключена индикация в настройка[illegible]ры.

3 – Индикатор соедине[illegible]ия: индикатор за[illegible]ается при подключении камеры к сети и показывает текущую сетеву[illegible]

- **Индикатор соединени[illegible]том**: IP-камера подключена к сети с помощью проводного соединения.
- **Индикатор** [illegible]**ния не горит** [illegible]**е мигает)**: IP-камера отключена от проводной сети, либо отк[illegible]ройках камеры.

4 – Встроенн[illegible] микро[illegible] пользователю слышать то, что происходит в зоне наблюде[illegible]

5 – С[illegible]**icro**[illegible]лот для карты памяти формата MicroSD/SDHC.

Испо[illegible]те[illegible]у па[illegible]для записи видео- и аудиоданных как в режиме тревоги, так и в ре[illegible]стоян[illegible]иси. Также предусмотрена возможность автоматической резервной за[illegible]время отсутствия соединения с сетью.

[illegible]МА[illegible]
[illegible]оряча[illegible] памяти не поддерживается камерой и может привести к повреждению [illegible]ования и [illegible]е данных!
[illegible]йте[illegible]ру во время форматирования карты памяти.
Камер[illegible]рживает карты памяти, при форматировании которых было создано несколько разделов.

Рис. 3.2

6 – Разъем питания (DC 5V): предназначен для подк[illegible]лока питания 5В, 1А. Полярность подключения: ⊖—C—⊕.

ВНИМАНИЕ!

Для корректной работы камеры испол[illegible]йте тол[illegible]о[illegible]ки, рекомендованные ООО «НПП «Бевард»!

7 – Сброс настроек [R[illegible]set]: кнопка пре[illegible]значена для сброса настроек камеры в заводские установки.

Для возвращения пара[illegible]ениям по умолчанию удерживайте данную кнопку нажатой в течение 10-[illegible]удерживать кнопку нажатой менее 10 секунд, камера переза[illegible]тся без сброса п[illegible]аметров.

8 – Кнопка W[illegible]томатиче[illegible]е подключение по Wi-Fi): данная кнопка предназначена для полу[illegible]евых настроек по протоколу WPS. Для подключения ка[illegible]спроводной сети с помощью WPS необходимо нажать данную кнопку на ка[illegible] беспроводном устройстве, к которому требуется подключиться (более подр[illegible]о ин[illegible]маци[illegible]мотрите в пункте 6.2 данного Руководства).

9 – [illegible]ой [illegible]зъем [illegible]rnet): разъем для подключения камеры к сети Интернет, роутеру или [illegible]омощи стандартного RJ-45 штекера.

[illegible]е того, на задней панели камеры наклеен стикер, содержащий информацию о [illegible]укте:

- [illegible]N: се[illegible]й номер IP-камеры;
- **MAC**: [illegible]-адрес IP-камеры в сети LAN (при проводном подключении);
- [illegible]MAC-адрес IP-камеры в сети WLAN (при беспроводном подключении).

Глава 4. Установка и подключение IP-камеры

4.1. Общие сведения о подключении IP-камеры N120S к [illegible]

IP-камера N120S может подключаться к локальной сети либо [illegible]к при помощи проводного соединения (Ethernet), так и по беспровод[illegible] (Wi-Fi) со[illegible]нию. Подключение может осуществляться напрямую к ПК или при п[illegible]помога[illegible]ного сетевого оборудования (маршрутизаторы, коммутаторы, точки доступа).

Рис[illegible]

Для беспроводного под[illegible]ения камеры м[illegible]рутизатор должен быть оснащен Wi-Fi-интерфейсом.

Основные шаги и рекоменд[illegible] настройке камеры описаны далее в данном Руководстве.

4.2. Рекомендац[illegible]

В данном [illegible] приведен [illegible]кий список рекомендаций, которые необходимо учитывать пр[illegible]удования IP-видеонаблюдения.

Рек[illegible]ац[illegible]о ра[illegible]ению камеры:

- IP-[illegible]20S предназначена для осуществления видеонаблюдения в помещ[illegible]ельной температурой эксплуатации от -10 до +50°С.
- [illegible]бегайте попадания на камеру прямых солнечных лучей в течение длительного [illegible] также нахождения поблизости отопительных и обогревательных [illegible]ибор[illegible]
- [illegible]пр[illegible]вная расстановка камер видеонаблюдения приведёт к появлению [illegible]тельных «слепых» зон, которые будут оставаться вне поля зрения опе[illegible]тора.

- Избегайте близости с водой или источниками влажности.
- Избегайте близости с устройствами-генераторами мощных электромагнитных волн.
- Убедитесь в возможности размещения устройства с учетом ввода соединительных кабелей.
- Избегайте способа крепления камеры, допускающего значительную вибрацию. Данное воздействие снизит эффективность детектора движения и четкость изображения в целом.
- Камеры видеонаблюдения необходимо держать в недосягаемом месте так, чтобы как случайное, так и специальное повреждение или изменение направления обзора было невозможно.
- Направление обзора (зона видеонаблюдения) камеры должно быть твёрдо определено на момент установки.

Рекомендации по прокладке кабеля типа «витая пара»:

- В коридорах желательно прокладывать стояки электрических и слаботочных кабелей по разным кабель-каналам, проходящим по разным стенам.
- Допускается в одном кабель-канале прокладывать витопарные и электрические кабели в разных трубках или секциях, имеющих сплошные продольные перегородки с пределом огнестойкости не менее 0,25 ч. из несгораемого материала только в рабочем состоянии не более 15-ти метров, если электрическая мощность будет не более 5 кВА.
- Электрические и слаботочные кабели допускается прокладывать параллельно на расстоянии не менее [illegible] друг от друга в разных кабель-каналах или секциях кабель-каналов. Если напряженность электрического поля, образующегося от электрокабеля, будет более 3 В/м, то необходимо увеличить расстояние между электрическими и слаботочными кабелями или снизить уровень электромагнитных помех.
- Витопарные и электрические кабельные трассы должны пересекаться только под прямым углом.
- Неэкранированные витопарные кабельные трассы должны проходить на расстоянии не менее 125 мм от газоразрядных ламп дневного света (люминесцентных ламп) и других высоковольтных устройств, содержащих газоразрядники.

- Неэкранированные витопарные кабели должны прокладываться на расстоянии не менее 1.5 метров от источников сильных электромагнитных [illegible]бразующих напряженность электрического поля свыше 3 В/м.
- Распределительные устройства с заделанными неэкран[illegible]нными ви[illegible]ыми кабелями должны располагаться на расстоянии не мене[illegible]ов от ис[illegible]иков сильных электромагнитных помех, образующих напряжен[illegible]тр[illegible]ского поля свыше 3 В/м.
- Прокладка витой пары между точками подключе[illegible]оизводиться целыми кусками, при этом направление трассы след[illegible]аранее [illegible]ду[illegible]так, чтобы её протяжённость была как можно меньше.
- Минимальный радиус изгиба для кабеля – [illegible]аметра кабеля (или 1 дюйм=2,5 см), но существуют рекомендации разме[illegible]ель таким образом, чтобы обеспечивать изгиб радиусо[illegible]антиметро[illegible]).
- Максимальная длина сегмента до[illegible]метров.
- При использовании беспроводного [illegible]с[illegible]ения следует учитывать, что уровень/качество сигнала с[illegible] завис[illegible]ножества факторов: удаленности от точки доступа, от электро[illegible]бстан[illegible]нфигурации помещения и т.д.

4.3. Монтаж устройс[illegible]

Шаг 1: Прикрепите кр[illegible]ры к нес[illegible]ей поверхности, используя крепеж из комплекта поставки.

Шаг 2: Ослаб[illegible] винтовое соед[illegible]ение фиксатора кронштейна, чтобы иметь возможность повора[illegible]ру.

Шаг 3: Закрепит[illegible]тейне, выберите направление обзора и зафиксируйте её[illegible]

4.4. [illegible]нов[illegible]звл[illegible]ение карты памяти

Шаг [illegible]е пит[illegible]камеры.

Шаг [illegible]памяти MicroSD/SDHC объемом до 32 Гб в слот. Для этого разв[illegible]те кар[illegible]и к передней поверхности камеры и к слоту и вставьте до щ[illegible]

Ш[illegible]чите питание.

Д[illegible] извл[illegible]ия карты памяти нажмите на ее торец до щелчка, и пружинный м[illegible]ыто[illegible]т карту из слота.

4.5. Проводное подключение камеры к сети

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

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

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

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

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

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

Глава 5. Настройка проводного соединения

Для того чтобы IP-камера N120S работала в Вашей локальной сети совместно с другим оборудованием, необходимо выполнить ее подключение в соответствии с текущими настройками данной сети, для чего, в свою очередь, необходимо определить эти настройки.

ПРИМЕЧАНИЕ!
Названия некоторых пунктов меню и функций на скриншотах в данном Руководстве могут отличаться от таковых в Вашей версии Windows, однако алгоритм выполняемых действий является универсальным.

5.1. Определение параметров локальной сети для проводного подключения

При подключении по кабелю Ethernet необходимо определить текущие настройки кабельной сети. При подключении по Wi-Fi (или использования WPS) необходимо определить настройки как беспроводной, так и проводной сети.

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

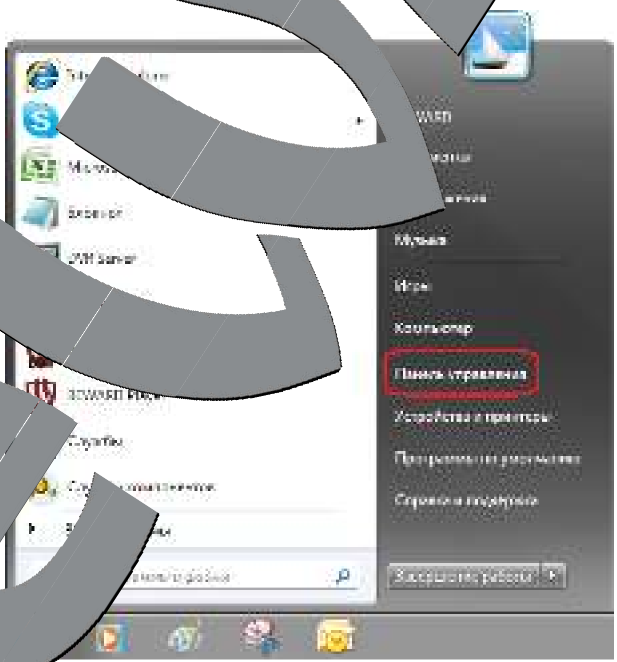


Рис. 5.1

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

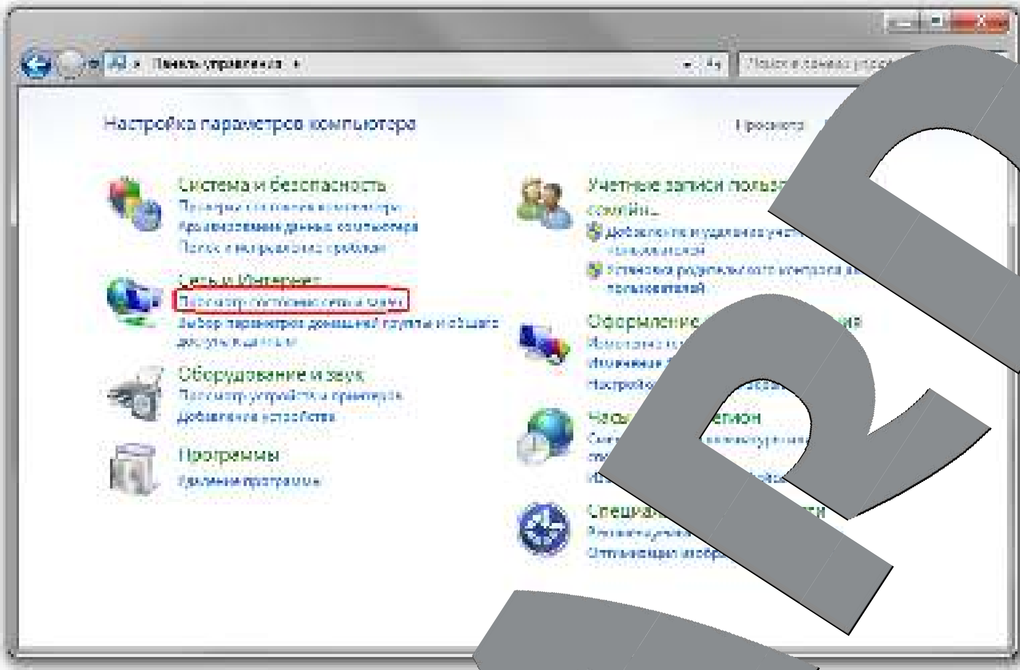


Рис. 5.2

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

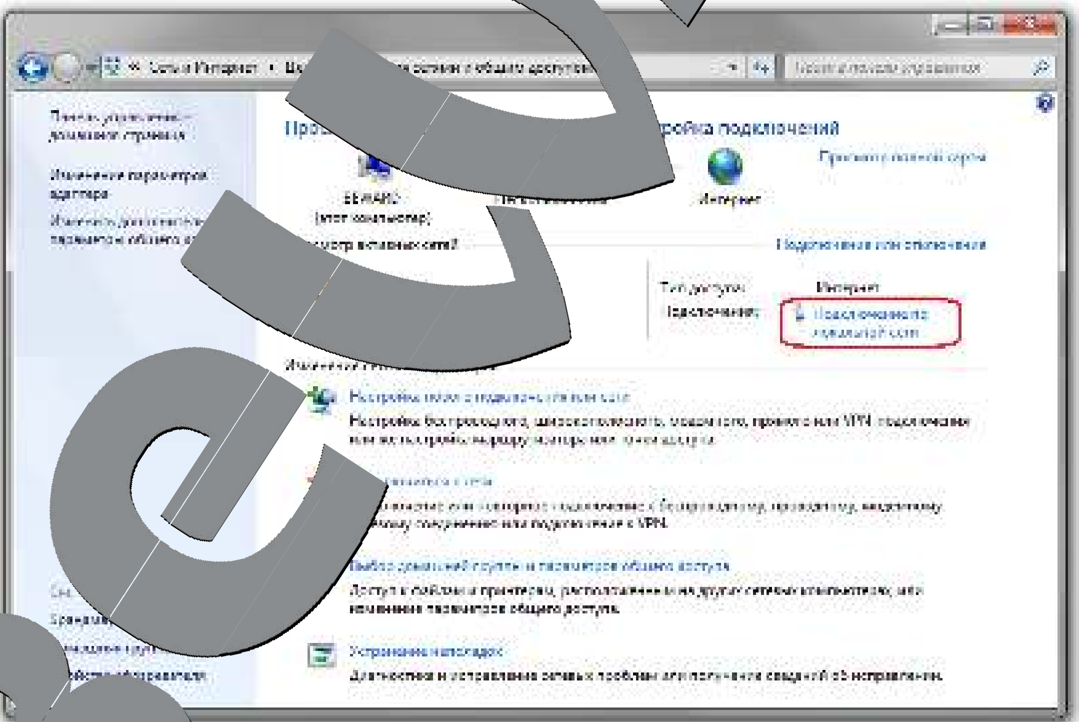


Рис. 5.3

ПРИМЕЧАНИЕ!

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

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

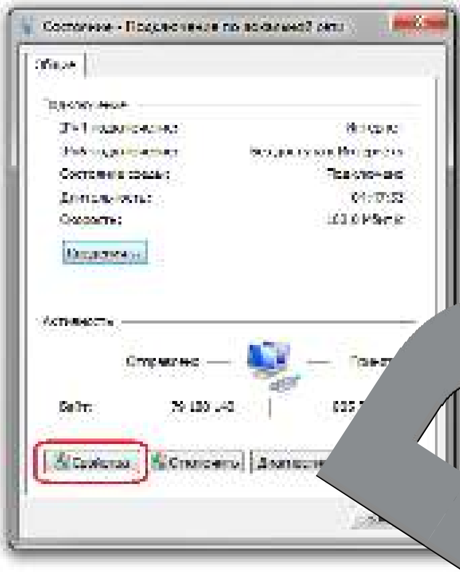


Рис. 5.4

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

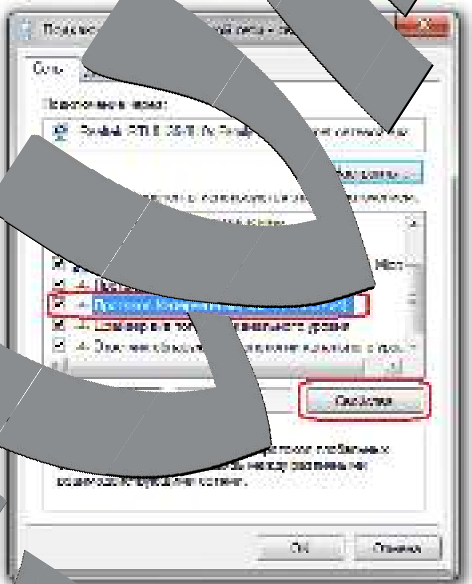
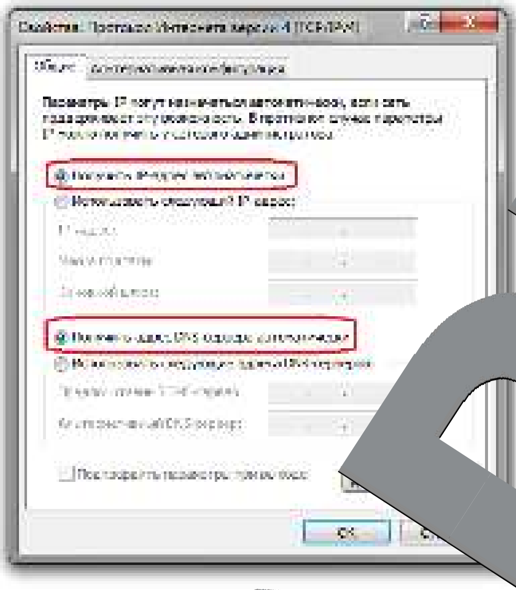


Рис. 5.5

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

- **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.



Р...

2. Использовать следующий IP-адр... адре... ся пользователем вручную (*Рис. 5.7*):

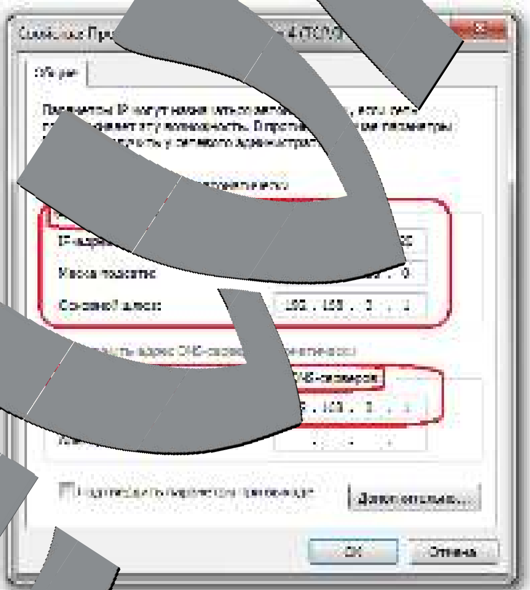


Рис. 5.7

...мните ... шите конфигурацию сетевых настроек адаптера Вашего ПК (IP-а... ети, Сетевой шлюз, DNS-сервер).

...МА...Е!

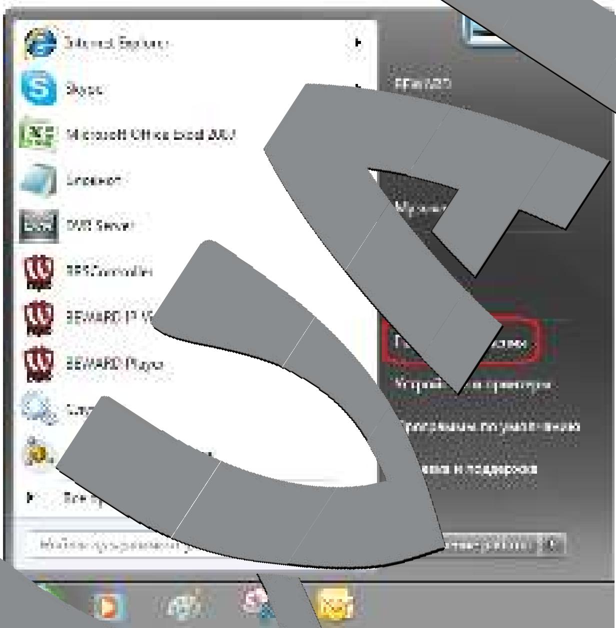
... за... и данные текущего сетевого подключения, то после настройки камеры N120S будет ... вернуть сетевые настройки компьютера в первоначальное состояние для подключени... локальной сети и/или сети Интернет!

5.1.1. Определение параметров сети при динамическом IP-адресе

> **ПРИМЕЧАНИЕ!**
> Данный пункт Руководства предназначен для определения параме[illegible]локальной [illegible] при назначении IP-адреса Вашему ПК автоматически (DHCP-сервером).

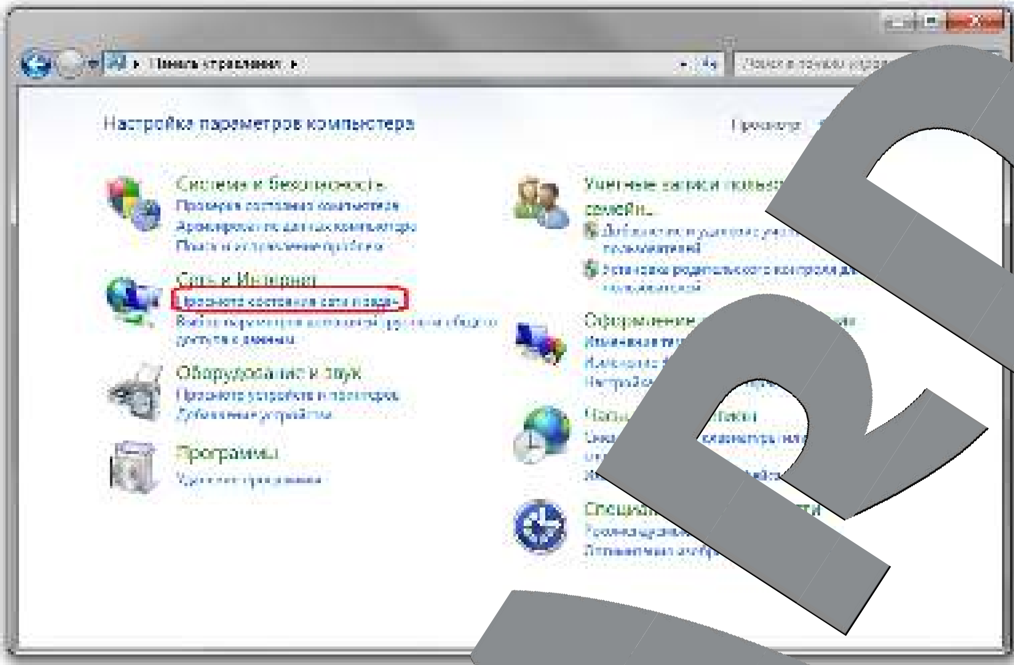
Подключите компьютер (ноутбук) с помощью кабеля [illegible] Вашей [illegible] сети и дождитесь окончания процесса подключения.

После этого для определения текущих настроек [illegible]ьютер[illegible]ока[illegible]ной проводной сети нажмите ***Пуск – Панель управления*** (*Рис. 5.8*).



[illegible].8

В откры[illegible]алоговом окне выберите пункт **[Просмотр состояния сети и задач]** в разд[illegible]тернет]** (*Рис. 5.9*).



Рис

В открывшемся диалоговом о... жмите ...лючение по локальной сети]** (*Рис. 5.10*).

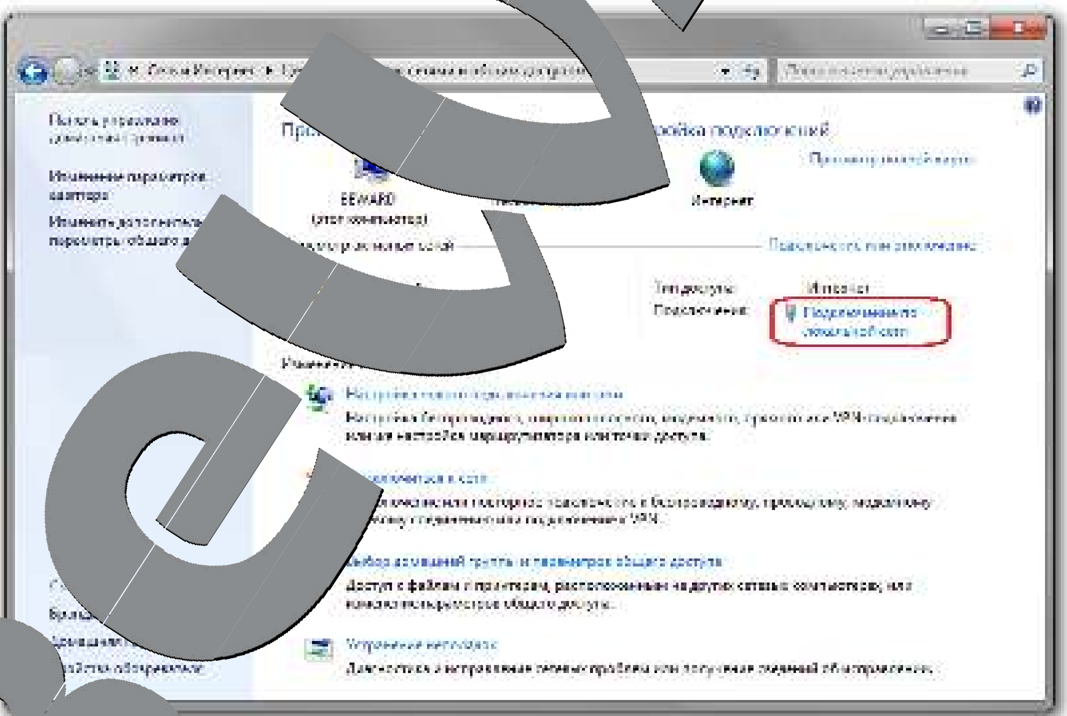


Рис. 5.10

...НИЕ

При н... ольких сетевых подключений выберите то, к которому планируется подключить IP-камеру.

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

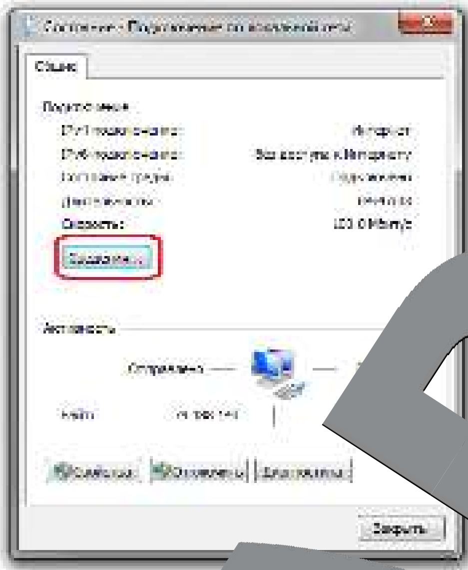


Рис. 5.11

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

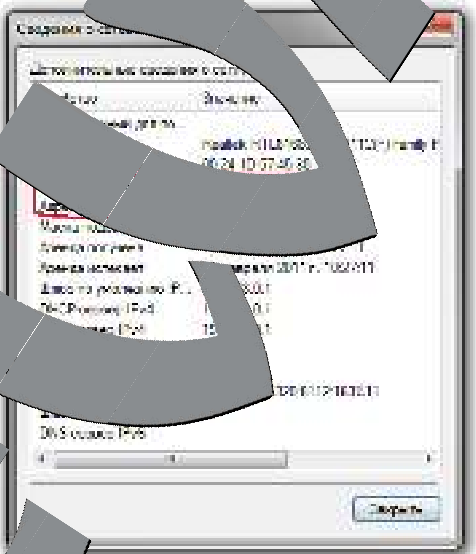


Рис. 5.12

Если в открывшемся окне Вы увидели следующие строки: **[DHCP включен]** – Да, **[Адрес IPv4 – xxx.xxx.xxx.xxx]** (где xxx.xxx.xxx.xxx – значение IP-адреса), значит Вашему ПК в процессе соединения был назначен IP-адрес, значение которого указано в строке **[Адрес IPv4]**, маска подсети указана в строке **[Маска подсети IPv4]**, адрес сетевого шлюза - в строке **[Шлюз по умолчанию IPv4]**, адрес DNS-сервера - в строке **[DNS-сервер]**. Запомните или 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 настрой[illegible]меры N120S будет невозможно вернуть сетевые настройки компьютера в первонач[illegible]е для подключения к локальной сети и/или сети Интернет!

ВНИМАНИЕ!

Если в открывшемся диалоговом окне **[Сведения о сетевом подключ[illegible]** ув[illegible]идели следующие строки: **[DHCP включен]** – Да, **[IPv4-адрес авто[illegible] – xxx.xx[illegible]xx]** (где xxx.xxx.xxx.xxx – значение IP-адреса), значит Вам не удало[illegible]к сети по кабельному соединению (DHCP-сервер не присвоил IP-адрес В[illegible] ПК). [illegible]равильность подключения к проводной сети и в случае не[illegible]и [illegible] к системному администратору Вашей сети.

5.2. Изменение параметров лока[illegible]для прово[illegible]ного подключения IP-камер

По умолчанию IP-камера N120S им[illegible]-ад[illegible]192.168.0.99. Для того чтобы подключиться к камере для первона[illegible]ой нас[illegible]необходимо, чтобы Ваш компьютер находился в той же подсети, что и [illegible] этом [illegible]еса камер, компьютеров и любых сетевых устройств в сети не должны совпада[illegible]

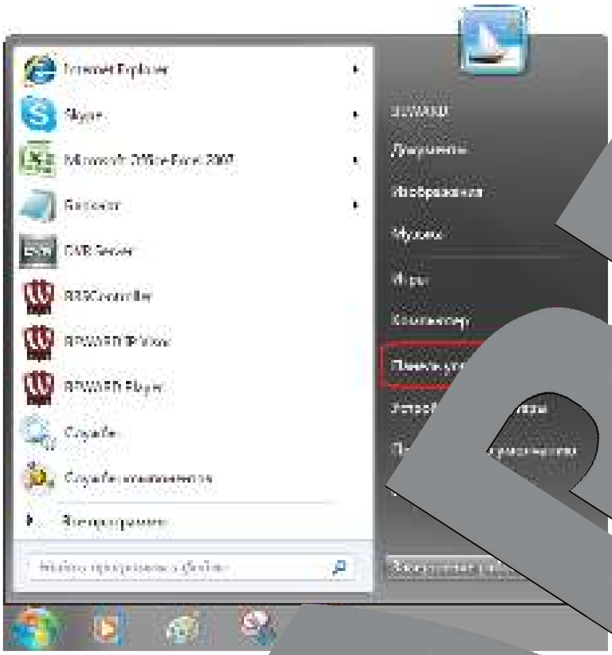
ВНИМАНИЕ!

IP-камеры BEWARD N120S по ум[illegible]ес 192.168.0.99! Если Вы планируете подключать несколько IP-камер, то для исключени[illegible]конфликта IP-адресов подключайте камеры по одной и изменяйте их [illegible] на любые своб[illegible]ные из Вашей локальной сети!

ВНИМАНИЕ!

Если Вы увере[illegible]й адаптер Вашего ПК, подключенный в проводную сеть с IP-камерой либо напрям[illegible]ка[illegible]находится в одной подсети с IP-камерой, тогда Вы можете перейти к пункту 5.3 д[illegible] Ру[illegible]ства.

Для и[illegible]настроек компьютера в локальной проводной сети нажмите **Пуск**[illegible]**нель у**[illegible](*Рис. 5.13*).



Р

В открывшемся диалоговом окне выбе пу **[Просмотр состояния сети и задач]** в разделе **[Сеть и Интернет]** 14).

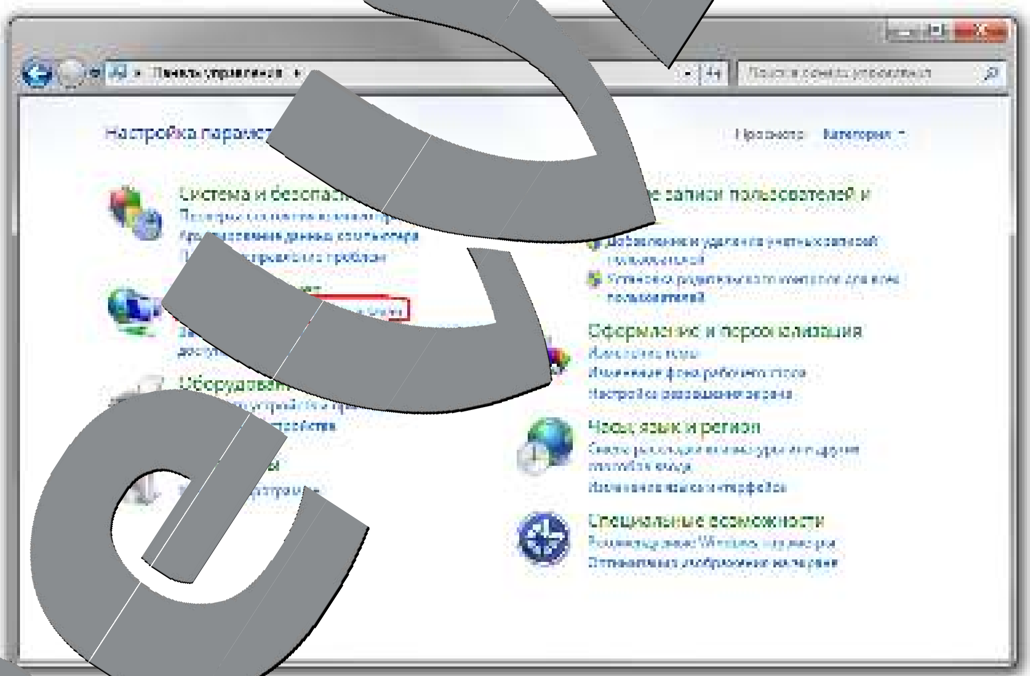


Рис. 5.14

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

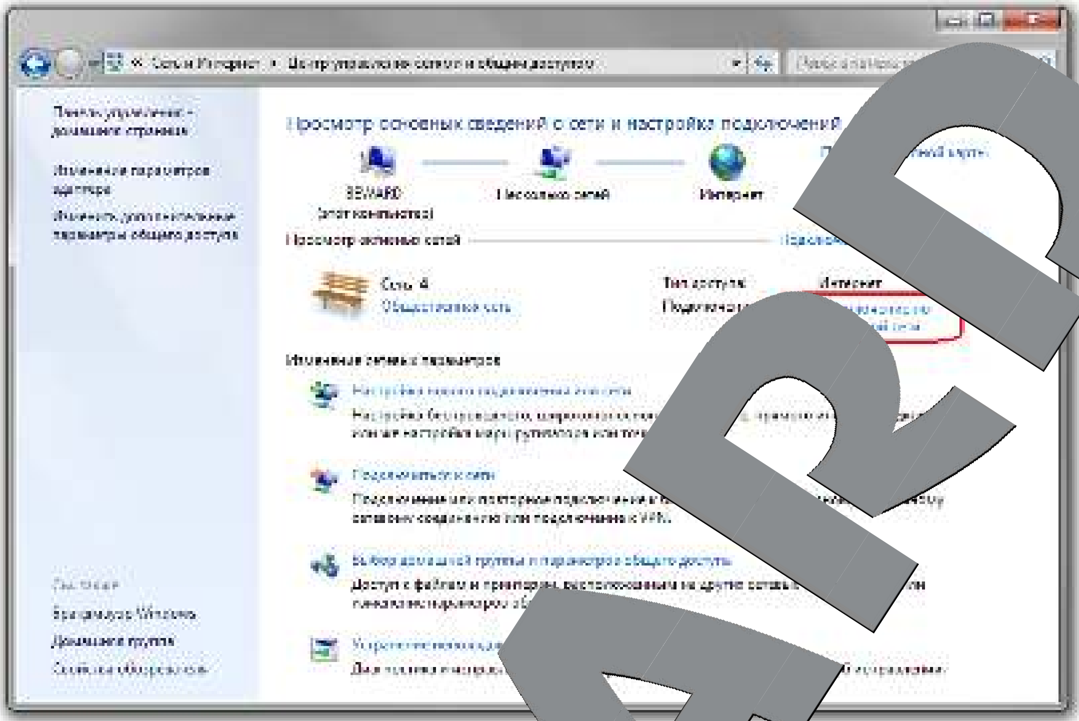


Рис. 5.15

ПРИМЕЧАНИЕ!

При наличии нескольких сетевых подключений вы[illegible]ите то, к которому планируется подключить IP-камеру.

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

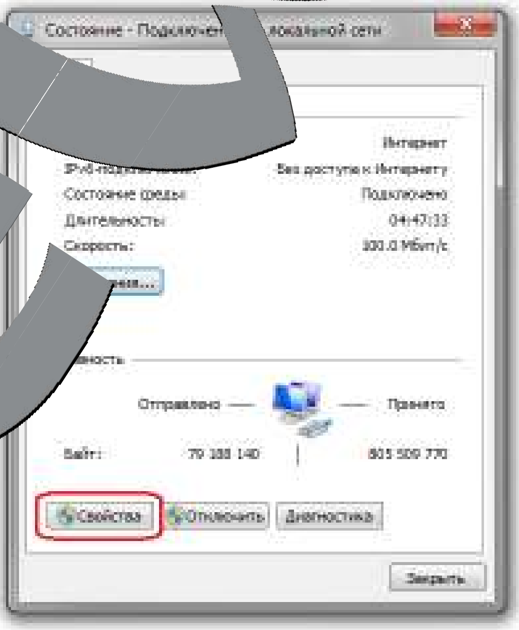


Рис. 5.16

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

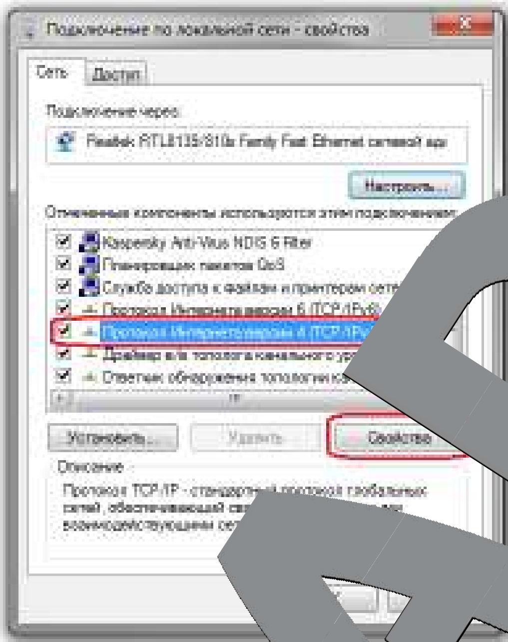


Рис. 5.17

Откроется меню, в котором необходимо установить значения IP-адреса и маски подсети. Выберите пункт **[Использовать следующий IP-адрес]** и введите свободный **[IP-адрес]** из подсети камеры, например 192.168.0.20, **[Маску подсети]** 255.255.255.0, остальные значения вводить нет необходимости (*Рис. 5.18*).

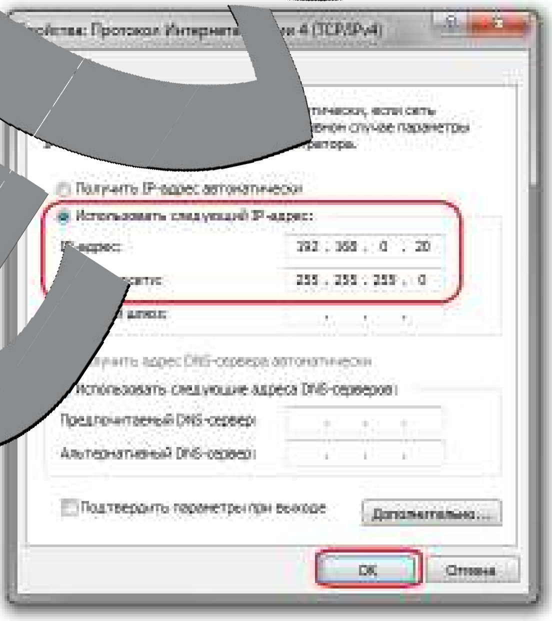


Рис. 5.18

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

5.3. Получение доступа к IP-камере

Получить доступ к IP-камере Вы можете следующими способами:

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

ВНИМАНИЕ!

При подключении IP-камеры к локальной сети необходимо учи[illegible] умолчан[illegible]P-камера имеет сетевой адрес: 192.168.0.99.

5.3.1. Установка «BEWARD IP Installer»

Вставьте диск с программным обеспечением [illegible] CD-ROM. На экране автоматически появится меню установки (*Рис.5.19*).

Для установки программного обес[illegible]рите **[BE[illegible]ARD IP Installer]** и выполните процедуру установки (подробно [illegible]**ве по эксплуатации ПО BEWARD IP Installer»**).

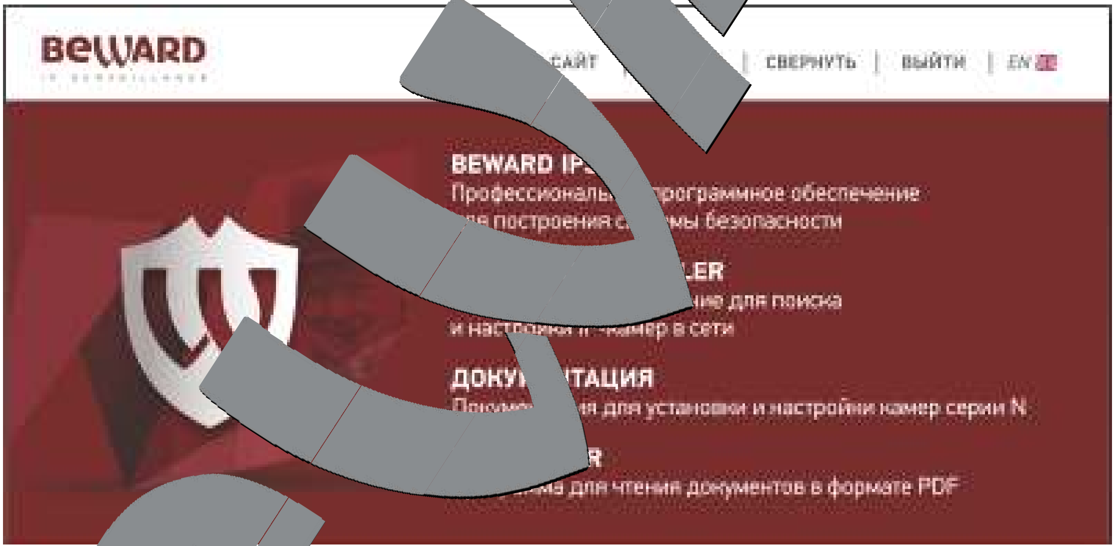


Рис. 5.19

5.3.2 [illegible]уч[illegible] дос[illegible] IP-камерам с помощью ПО «BEWARD IP Installer»

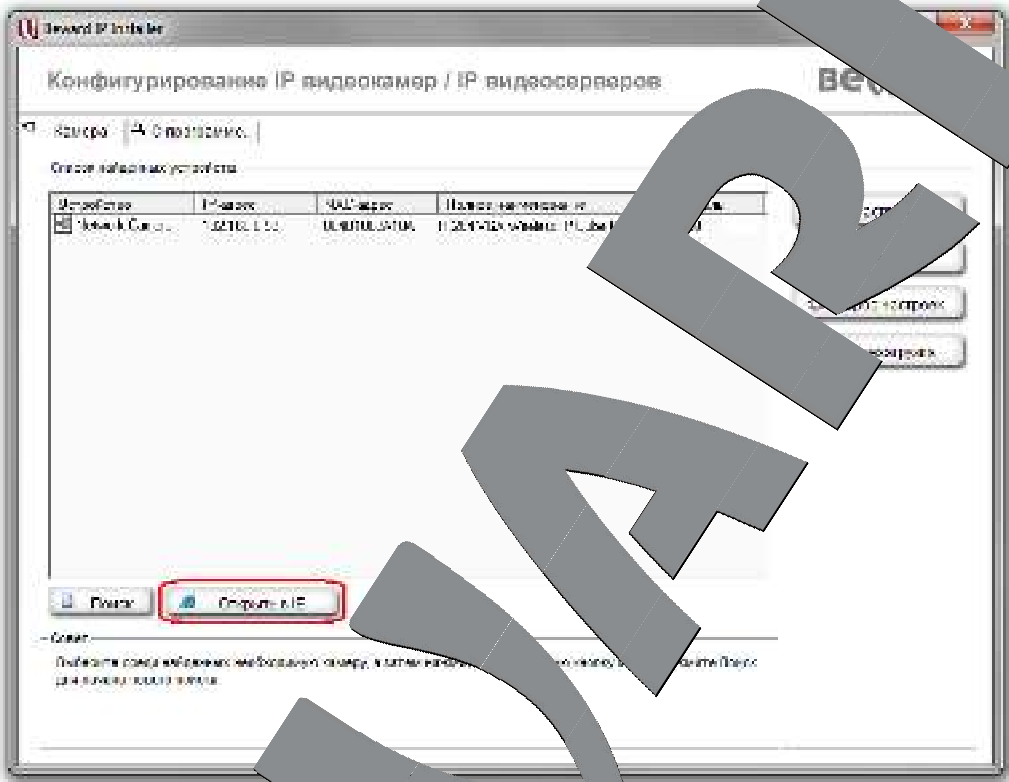
ВНИМАНИЕ!

Д[illegible] IP-кам[illegible]мощью ПО **«BEWARD IP Installer»** должна быть включена поддержка [illegible]для Вашего ПК и для IP-камеры. В ОС Windows 7 и в более поздних версиях [illegible]держ[illegible]ена по умолчанию.

[illegible]АНИЕ!

Для [illegible]WARD N120S использование поддержки технологии UPnP включено по умолчани[illegible]

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



ВНИМАНИЕ!

Для корректной работ[illegible]Installe[illegible]обходимо добавить его в список доверенных приложений Вашего антивиру[illegible]

ПРИМЕЧАНИ[illegible]

В Windows [illegible]боле[illegible]здних [illegible]сиях для корректной работы программы может потребоваться запуск BEW[illegible]P [illegible]ller о[illegible]и администратора. Для этого нажмите на ярлыке программы правой клав[illegible]вшемся контекстном меню выберите пункт **[Запуск от имени администратор[illegible]**

[illegible]МЕЧ[illegible]

[illegible]ли IP[illegible]оис[illegible]и устройства) не появилось в окне поиска, нажмите кнопку **[Обновить]** для [illegible]ия спис[illegible]ис. 5.20*).

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

ПРИМЕЧАНИЕ!
Для IP-камер BEWARD N120S использование поддержки техноло[illegible]PnP вк[illegible] по умолчанию.

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

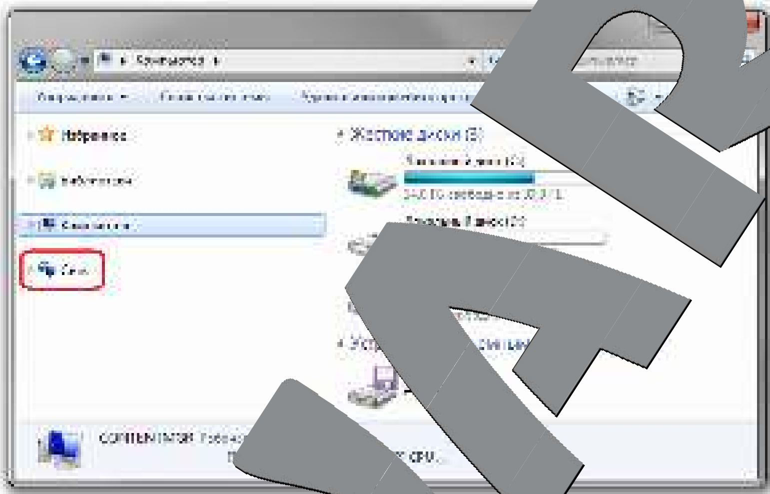


Рис 5.21

В появившемся меню [illegible] интересующ[illegible] Вас устройство и нажмите на нем два раза левой кнопкой мыши (*Рис.* [illegible]

После этого IP-камера N120S [illegible] браузере, который установлен по умолчанию.

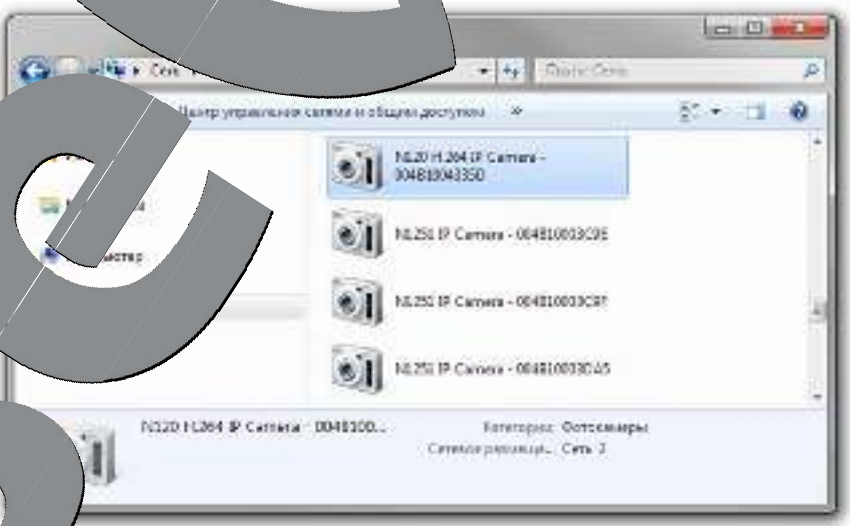


Рис 5.22

Ес[illegible]с по умолчанию выбран браузер, отличный от Internet Explorer, то для того чтобы открыть камеру в Internet Explorer, перейдите в пункт 5.3.4.

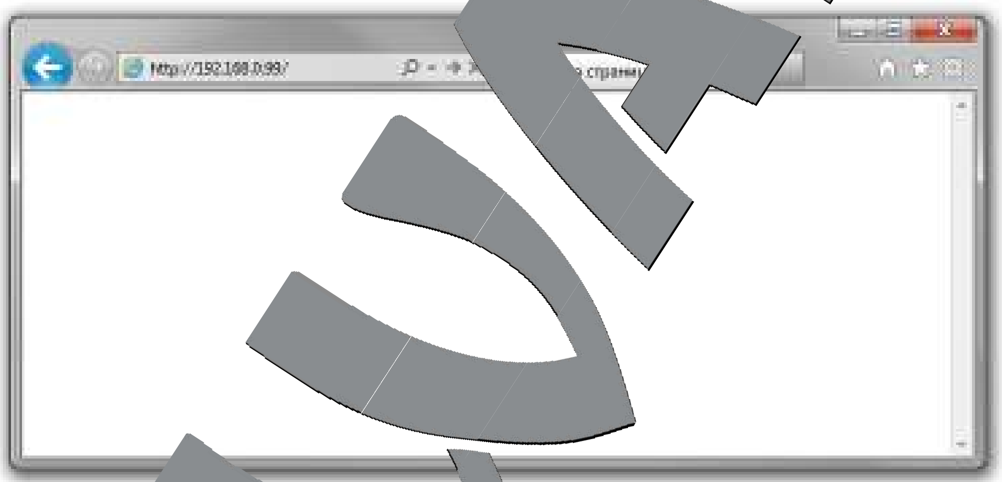
5.3.4. Получение доступа к IP-камерам с помощью браузера Internet Explorer

Для доступа к камере с помощью браузера Internet Explorer нео[illegible]о запустить браузер и в адресной строке ввести запрос: http://<IP>:<port>/, где:

<IP> – IP-адрес камеры, а **<port>** – значение http-порта), после че[illegible]кать **[Пер[illegible]** либо **[Ввод]** (*Рис. 5.23*).

ВНИМАНИЕ!
IP-камера BEWARD N120S по умолчанию имеет сетевой адре[illegible]http – порт [illegible].

ПРИМЕЧАНИЕ!
Если для http-порта используется значение 80, тогда для д[illegible]ме[illegible]браузере достаточно ввести строку http://<IP>/, где <IP> – IP-адрес камеры.



Ри[illegible]5.23

5.4. Получе[illegible]досту[illegible]рфейсу IP-камеры

После [illegible]лучили доступ к IP-камере любым из способов, рассмотренных пунктах 5.3.[illegible]3, 5.[illegible]данн[illegible]го Руководства, будет запущен браузер Internet Explorer, где откроется о[illegible]вто[illegible]ции д[illegible]лучения доступа к веб-интерфейсу устройства.

ПРИМЕЧАНИ[illegible]
Дл[illegible]тной ра[illegible]-интерфейса IP-камеры необходима версия браузера Internet Explorer [illegible]

Вв[illegible]ите и[illegible]ользователя и пароль, после чего нажмите **[ОК]** (*Рис. 5.24*).

ВНИ[illegible]
Имя польз[illegible]ля по умолчанию: **admin**. Пароль по умолчанию: **admin**.

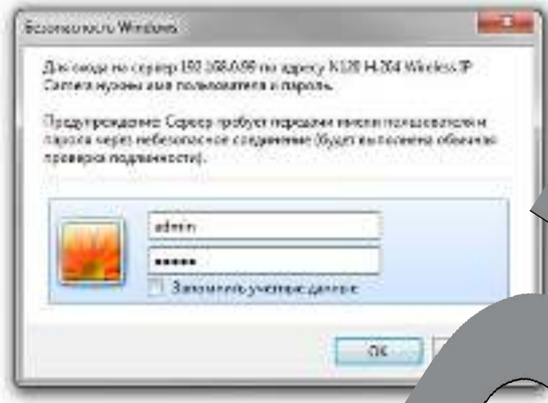


Рис. 5.24

После удачной авторизации, при первом под[illegible] ОС Windows будет блокировать установку приложения ActiveX (необходимо дл[illegible]тра изображения с камеры), о чем будет свидетельствовать [illegible]домление в нижней части окна Internet Explorer. Нажмите на кнопку **[Устано[illegible]** [illegible] установки (*Рис. 5.25*).

ВНИМАНИЕ!
Установка компонентов ActiveX возмо[illegible]а 32-[illegible]ерсию браузера Internet Explorer.

ПРИМЕЧАНИЕ!
Названия некоторых пунктов [illegible] функций на [illegible]иншотах в данном Руководстве могут отличаться от таковых в Вашей ве[illegible]горитм приведенных действий является универсальным.

Рис. 5.25

Система безопасности бр[illegible] [illegible]plorer также будет автоматически блокировать установку [illegible]tiveX. Для продо[illegible]ения установки нажмите кнопку **[Установить]** в окне подтверждения [illegible] (*Рис. 5.26*).

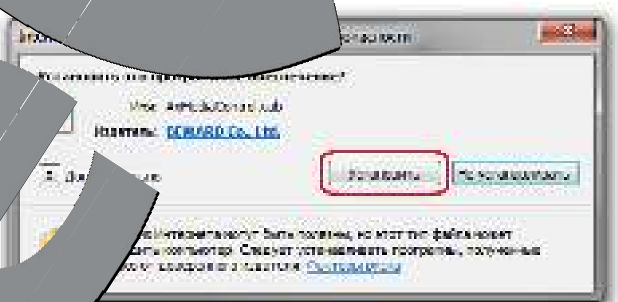


Рис. 5.26

[illegible]МЕЧ[illegible]

[illegible] у[illegible]ке [illegible] в ОС Windows 7 и в более поздних версиях при включенном контроле [illegible]записей [illegible]ет дополнительно производиться блокировка установки, о чем пользователю буд[illegible] [illegible]лнительное оповещение. Для разрешения установки необходимо положительно ответить [illegible]вшемся диалоговом окне.

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

5.5. Изменени[illegible]строек подкл[illegible]ения IP-камеры через веб-интерфейс

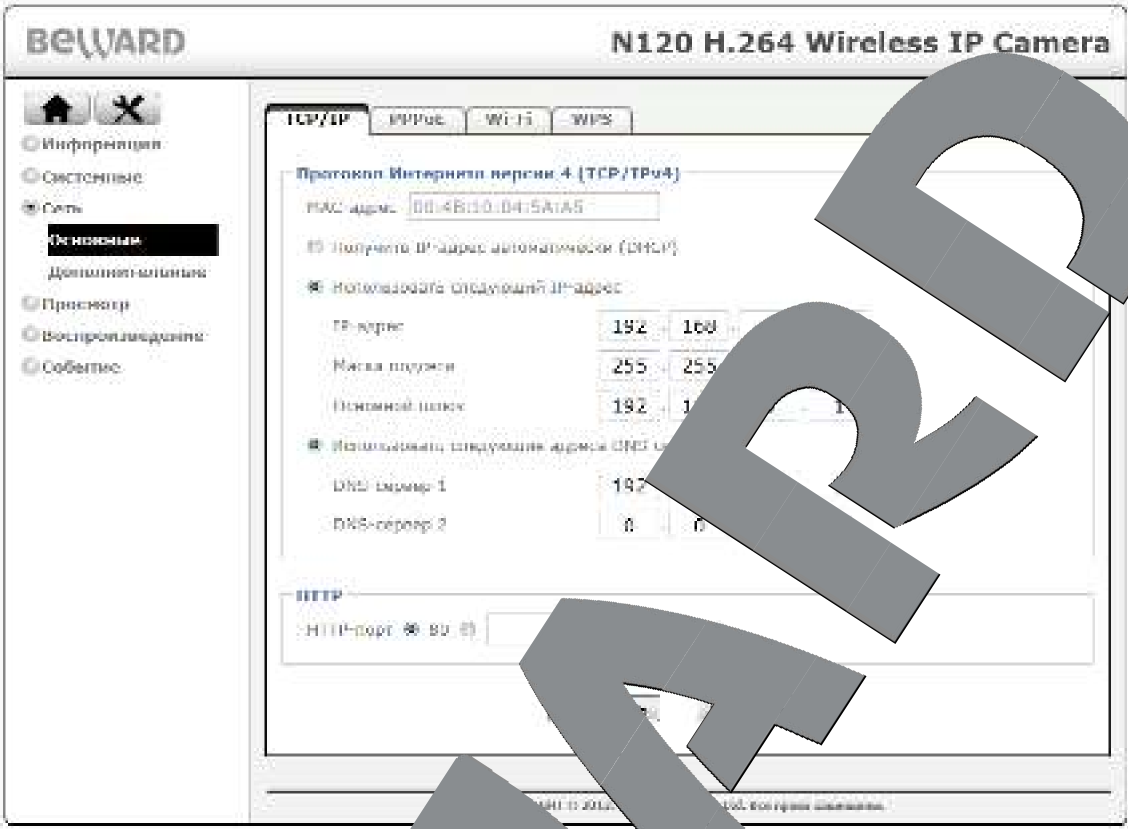
После подклю[illegible]амере N1[illegible]S по проводной сети необходимо изменить настройки камеры таким [illegible] находилась в одной подсети с остальным оборудованием [illegible] Вашим ПК).

ВНИМАНИ[illegible]

Для работ[illegible] и Ва[illegible] ПК необходимо, чтобы совпадали три части IP-адреса, за исключение[illegible]еобходимо, чтобы полностью совпадала маска подсети.

Напри[illegible], IP-а[illegible]К: 192.168.50.40. IP-адрес разделен точками на четыре октета. В д[illegible]мере: 1 октет – 192, 2 октет – 168, 3 октет – 50, 4 октет – 40. Вам необходимо изменить [illegible]дрес[illegible]бы у него первые три октета совпадали, то есть чтобы было значение вида [illegible].168[illegible]. [illegible]тый октет обязательно должен быть отличным от значения на Вашем ПК, а [illegible]угого се[illegible] оборудования Вашей сети (если такое имеется).

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



[illegible]28

Во вкладке **[TCP/IP]** н[illegible]о ввести таки[illegible]значения IP-адреса и других сетевых параметров для IP-камеры, [illegible] находи[illegible]сь в одной подсети с остальным оборудованием (*Рис. 5.28*).

ПРИМЕЧАНИЕ!
В случае необходимости [illegible] настроек устройствам обратитесь к Вашему сетевому администр[illegible].

Для с[illegible]ения [illegible]енений сетевых настроек проводного соединения нажмите кнопку **[Сохранить** [illegible]сле[illegible] в по[illegible]ихся окнах необходимо нажать кнопку **[ОК]**.

На э[illegible]тройка п[illegible]ного 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*).

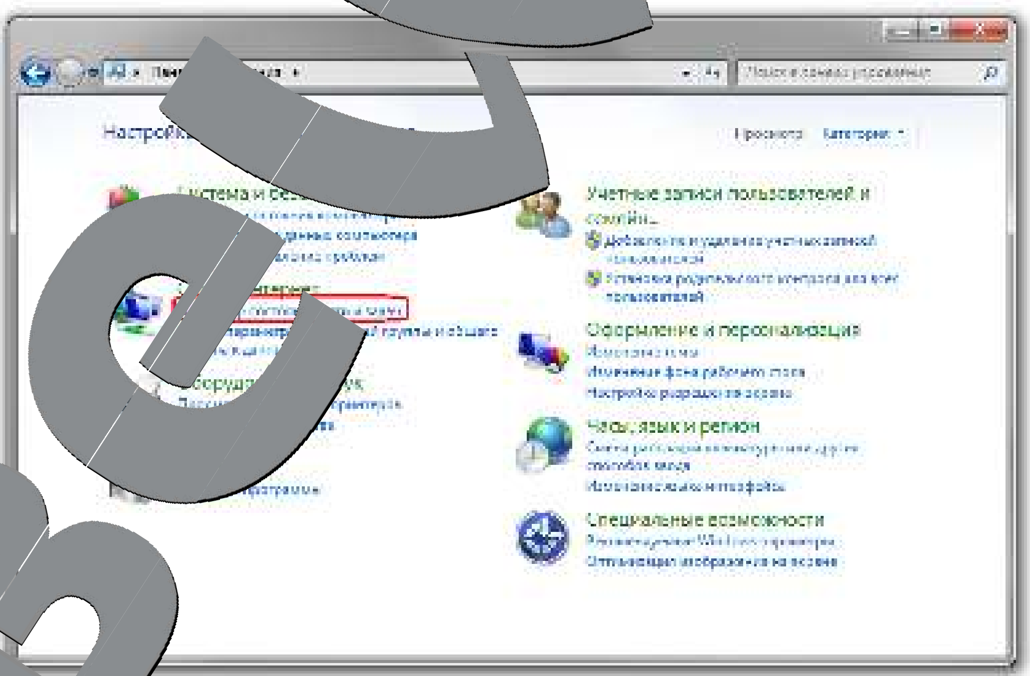


Рис. 5.30

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

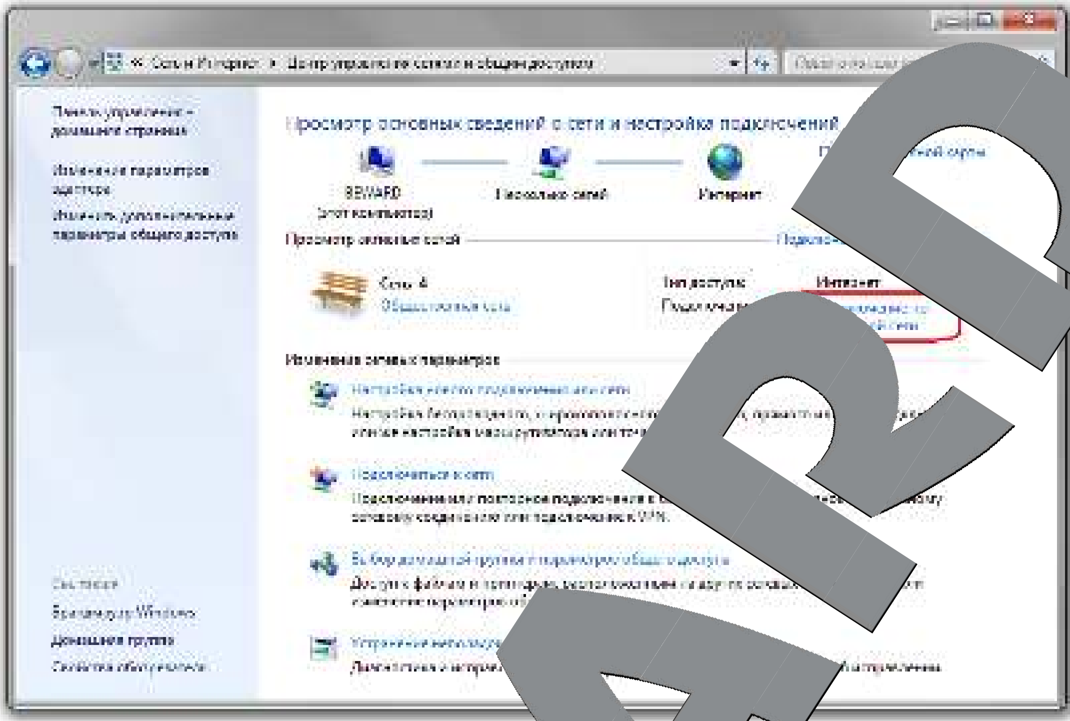


Рис. 5.31

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

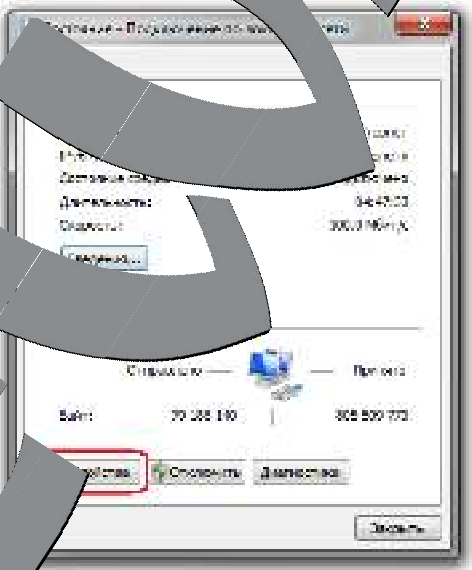
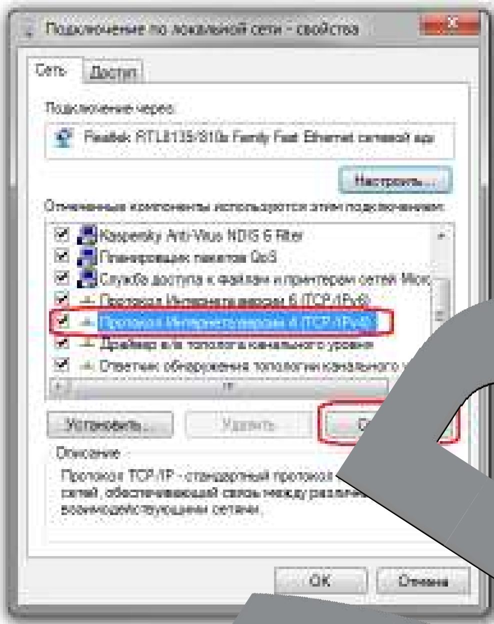


Рис. 5.32

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



Р[illegible]

Откроется меню, в котором [illegible]необход[illegible]ад[illegible]ь значения сетевых настроек, установленных изначально (см. пун[illegible] 1.1 д[illegible] Руководства).

Если изначально IP-адрес Вашему [illegible] назна[illegible] автоматически, тогда выберите пункты **[Получить IP-адрес автоматическ[illegible]** и **[Получить адрес DNS-сервера автоматически]**, после чего [illegible] кнопку **[ОК]** д[illegible] всех открытых окон (*Рис. 5.34*).

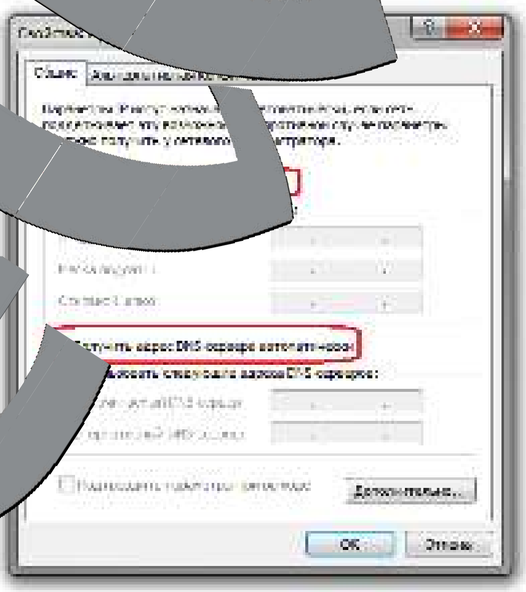
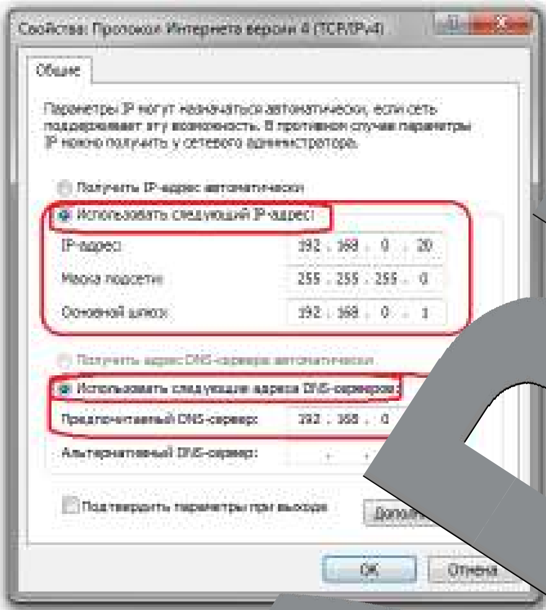


Рис. 5.34

[illegible]и[illegible]льно IP-адрес Вашему ПК был задан вручную, тогда выберите пункт **[Исполь[illegible]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*).



Р[illegible]

5.7. Проверка правиль[illegible] нас[illegible] подключения IP-камеры к локальной сети

Для контроля правильности сетевых [illegible]строек камеры и компьютера нужно подключиться к камере через [illegible]р Internet Expl[illegible]r.

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

Введите в [illegible]ной строке [illegible] адрес, присвоенный камере (например: http://192.168.0.99) (*Р[illegible]*

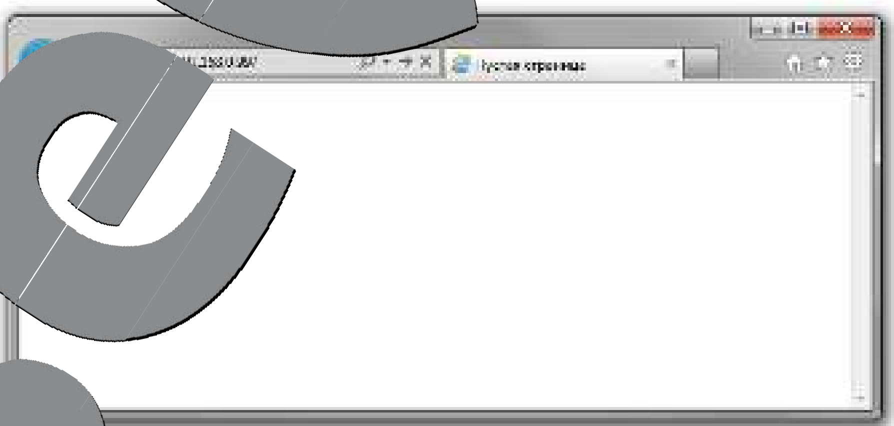


Рис. 5.36

[illegible]льных настройках откроется меню авторизации. Для авторизации введите имя пользов[illegible]ля и пароль, после чего нажмите **[ОК]** (*Рис. 5.37*).

ВНИМАНИЕ!

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

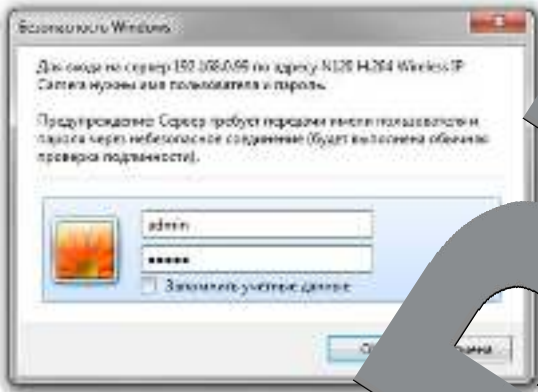


Рис. 5.37

При правильно выполненных действ[illegible]жете зайти [illegible] веб-интерфейс через браузер и увидеть изображение с Вашей IP-[illegible]

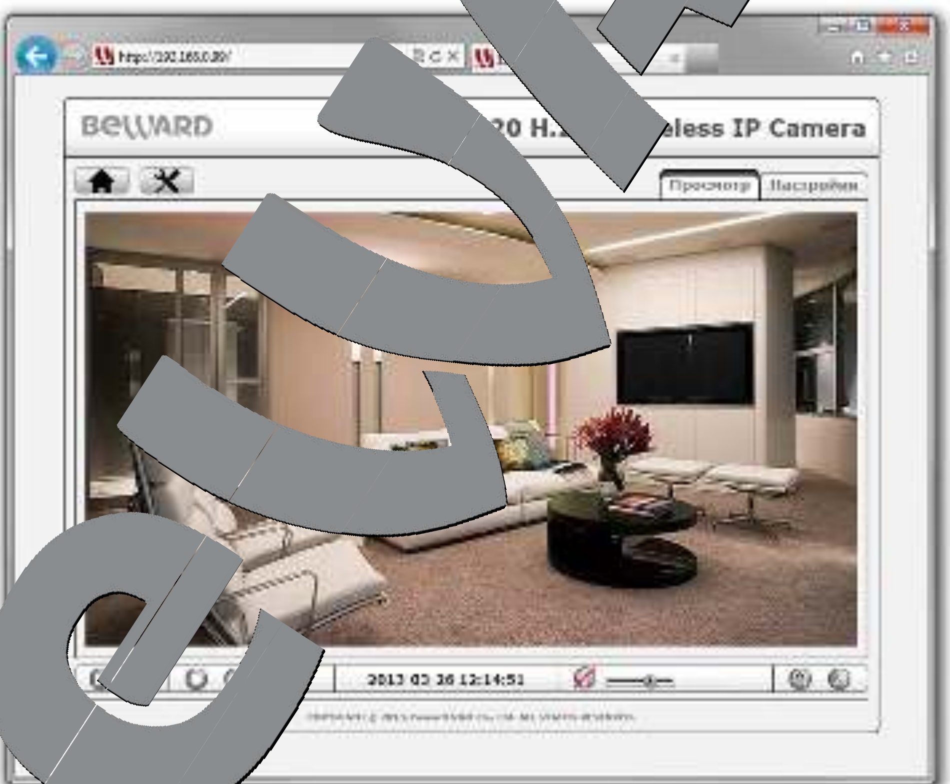


Рис. 5.38

[illegible]ИМЕ[illegible]

[illegible]е неуда[illegible] соединения с камерой проверьте правильность подключения к проводной се[illegible] [чало](#) данной главы и повторите настройку. В случае необходимости обратитесь к систем[illegible]инистратору Вашей сети.

Глава 6. Настройка беспроводного Wi-Fi-соединения

6.1. Общие сведения о беспроводном Wi-Fi-подключении IP-[illegible]20S

Для того чтобы IP-камера BEWARD N120S работала в Ва[illegible] сети совместно с другим оборудованием, необходимо подключить IP[illegible]ру в соотв[illegible]и с текущими настройками данной беспроводной сети. Подклю[illegible]кно в[illegible]нить следующими способами:

- Подключить IP-камеру, используя технолог[illegible] котора[illegible]озволяет автоматически получать данные, требуемые с[illegible]ои [illegible]ы беспроводной сети (при условии, что сеть является защищенно[illegible]

ВНИМАНИЕ!
Настройка IP-камеры с помощью функции WPS возможна только при [illegible], что маршрутизатор, к которому Вы хотите подключиться по Wi-Fi, по[illegible]ую функци[illegible].

- Подключить камеру без исп[illegible]ан[illegible]ехнологии WPS. Для этого необходимо сначала опре[illegible]ть нас[illegible]ребуемого Wi-Fi-соединения при помощи меню настроек В[illegible]рути[illegible](см. инструкцию по эксплуатации маршрутизатора) или посредством [illegible]ого о[illegible]рудования, подключенного к нему (например, ноутбука)

6.2. Подключение к бесп[illegible]ти с помощью WPS

Способы подкл[illegible]ения к беспров[illegible]ной сети с помощью WPS можно условно разделить на два тип[illegible]

- Способ настрой[illegible]одимо сделать соответствующие изменения в веб[illegible]йсе IP-камеры, а также в веб-интерфейсе того Wi-Fi-мар[illegible] которому Вы собираетесь подключиться.
- С[illegible] наст[illegible]и, п[illegible]котором нет необходимости заходить в веб-интерфейс Wi-Fi[illegible]йс[illegible]а до[illegible]но всего лишь поочередно нажать кнопки WPS на их ко[illegible]

О[illegible]а спо[illegible]ения более подробно описаны ниже.

6.[illegible]ение с использованием веб-интерфейса IP-камеры

[illegible]чите[illegible]туп к веб-интерфейсу IP-камеры любым из способов проводного [illegible] оп[illegible]ных в пункте 5.3 данного Руководства.

[illegible]емся окне введите имя пользователя и пароль (*Рис. 6.1*).

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

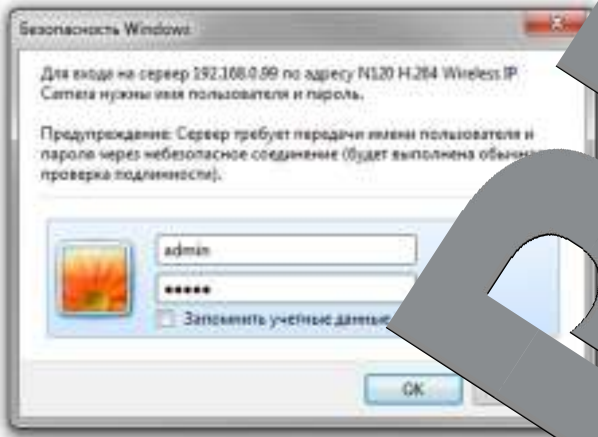
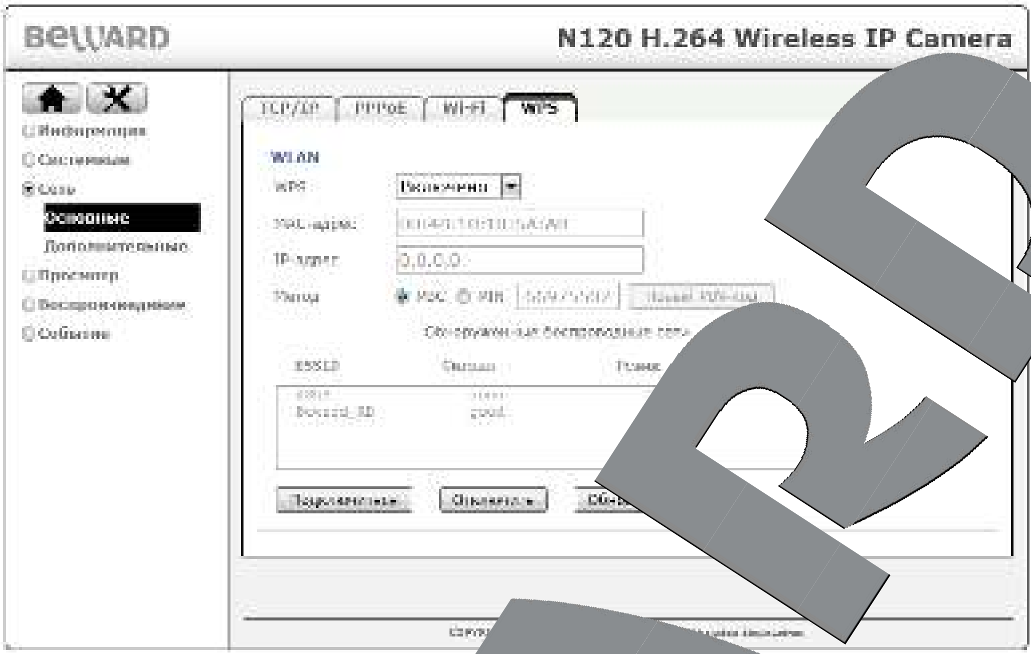


Рис. 6.1

После успешной авторизации в браузе[illegible]вит[illegible]е меню веб-интерфейса IP-камеры. Нажмите в этом меню кнопку [illegible]стройки[illegible] (*Рис. 6.2*).

Рис. 6.2

[illegible]йдите в меню ***Сеть – Основные – WPS***. Для включения функции **WPS** в данном м[illegible] выберите опцию **«Включено»**, после чего станут доступны пункты, показанные на *Рисунке 6.3*.



Поле **[Обнаруженные беспроводны[illegible]и]** [illegible]едназначено для отображения доступных к подключению беспровод[illegible]тей с [illegible]ной функцией WPS.

ВНИМАНИЕ!

Беспроводные сети с функци[illegible]PS отображают[illegible] в данном поле только тогда, когда на маршрутизаторе включена дан[illegible]находится [illegible]анный момент в активном состоянии! На некоторых моделях маршрутизатор[illegible]е WPS длится 2 минуты. Подробное описание работы функц[illegible] WPS для Вашего маршрутизатора должно находиться в прилагаемой к нему инструкции..

В пункте меню **[Метод]** [illegible]пны два метода настройки:

- **[PBC]** [illegible] настройки беспроводного соединения через WPS путем по[illegible]дного [illegible]катия кнопки WPS на обоих устройствах. После нажатия кнопки не[illegible]дим[illegible]одож[illegible] некоторое время, пока завершится процесс передачи на[illegible] между [illegible]утизатором и IP-камерой. Как правило, у большинства Wi-Fi устр[illegible]жкой технологии WPS процедура передачи и применения [illegible]тевых на[illegible]оек длится примерно 2 минуты.
- [illegible]нный способ отличается от способа **[PBC]** тем, что для настройки [illegible]о соединения необходимо ввести PIN-код, сгенерированный IP-камер[illegible] соответствующие настройки WPS на маршрутизаторе, после чего [illegible]и беспроводного соединения будут переданы не любому Wi-Fi устройству с[illegible]ержкой WPS, а только Вашей IP-камере, на которой был сгенерирован PIN-код. PIN-код отображается в небольшом поле рядом с положением переключателя

[PIN]. Для создания нового PIN-кода используйте кнопку **[Новый PIN-код]** (*Рис 6.3*).

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

ВНИМАНИЕ!
Подробное описание ввода PIN-кода для конкретной моде ... ршру ... ра ... рамках данного Руководства не рассматривается, так как предполага ... что оно ... инструкции к маршрутизатору. Такая инструкция может находить ... йте ... водителя Вашего маршрутизатора или идти в его комплектации.

Если выбран метод настройки **[P** ... установки соединения следует выполнить следующие шаги:

Шаг 1: включите функцию WPS на Ваше ... ир ... аторе в активное состояние. Для этого есть два способа:

- Физически нажать кнопку ... усе ... маршрутизатора.
- Нажать кнопку в настройках веб-инте ... йса В ... шего маршрутизатора.

Выбор способа включ ... активного сос ... ния WPS не имеет значения. После выполнения данного шага д ... активного состояния WPS будет продолжаться ограниченный промежуток времени, ... мо будет за это время выполнить остальные шаги (обыч ... а это отводится д ... таточно времени – около 2-х минут).

Шаг 2: нажми ... **[Обновить]** ... еню настроек камеры ***Сеть – Основные – WPS***, затем дождитесь по ... ей беспроводной сети (*Рис. 6.4*).

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

Шаг 4 ... пку **[Подключиться]**, после чего на экране появится окно с ожиданием ... ойки ... ключ ... ия (*Рис.6.4*).

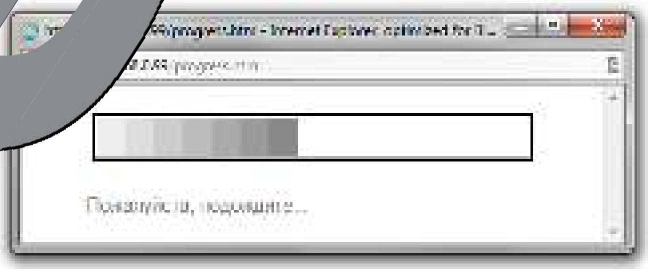


Рис 6.4

Ш ... дождите около двух минут для завершения операции настройки.

После выполнения **Шага 1** появится окно, отображающее ход подключения (*Рис 6.4*). Пока данное окно открыто, между маршрутизатором и IP-камерой про[illegible] установка беспроводного соединения. В случае успешного завершения настро[illegible] в окне появится надпись вида: **Connecting to AP(BEWARD)...success!** (*Р*[illegible]). В скобк[illegible]зано имя маршрутизатора (точки доступа), к которому произошл[illegible]чение, в[illegible]ном примере это **BEWARD**.

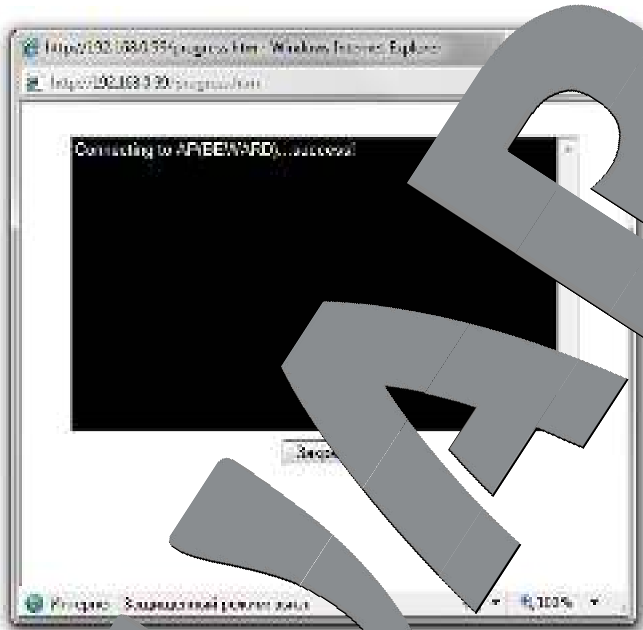


Рис 6.5

Если подключение пройдет [illegible]окончании операции в данном окне появится надпись: **Fail**[illegible]*Рис 6.6*). В этом [illegible]чае попробуйте повторно провести настройку, предварительно закр[illegible]шибке.

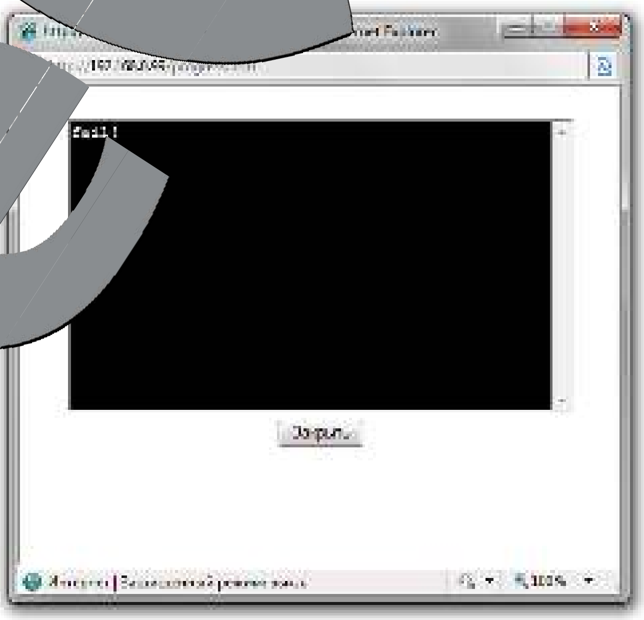


Рис 6.6

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

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

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

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

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

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

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

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

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

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

ВНИМАНИЕ!
Порядок настройки функции WPS для конкретной модели маршрутизатора в рамках данного руководства не рассматривается и должна быть описана в инструкции к маршрутизатору.

6.2.2 Подключение без использования веб-интерфейса IP-камеры

Функция WPS позволяет также осуществить подключение к беспроводной сети без необходимости дополнительной настройки IP-камеры или маршрутизатора через веб-интерфейс. Пользователю необходимо нажать кнопки WPS поочередно на маршрутизаторе и на IP-камере в течение отведенного для этого временного интервала, который составляет примерно 2 минуты.

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

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

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

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

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

Шаг 4: проверьте доступность камеры по беспроводному соединению.

6.2.3. Проверка доступности IP-камеры

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

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

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

На этом настройка беспроводного [illegible] соеди[illegible]рез WPS для IP-камеры завершена.

6.3. Подключение к беспроводн[illegible]i-Fi-с[illegible] без использования WPS

На сегодняшний день [illegible]ольшинство ма[illegible]утизаторов с поддержкой Wi-Fi также поддерживают и технологи[illegible] несмотря н[illegible] то многие маршрутизаторы не имеют данной функции. В этом случае [illegible] определить настройки беспроводной сети. Определить настройки беспроводного [illegible]одключения можно двумя способами:

- Зайти чер[illegible] интерфейс в [illegible]еню настроек Вашего маршрутизатора и определить на[illegible]ючения маршрутизатора (см. инструкцию по эксплуатации Вашего [illegible]а).
- Опре[illegible]ойки Wi-Fi подключения при помощи другого оборудования, по[illegible]енно[illegible] маршрутизатору (например, ноутбука).

Ниж[illegible]вед[illegible]имер[illegible]деления настроек требуемой беспроводной сети, а также рассмотрен[illegible]астрой[illegible]проводного подключения Вашей IP-камеры.

[illegible] Определ[illegible]е текущих настроек Wi-Fi-сети

[illegible]ИМЕ[illegible]НЕ:

[illegible]е устан[illegible]и настройки соединения выполнено на примере Windows 7 Максимальная. На[illegible]еню и некоторых функций может отличаться от Вашей версии Windows, однако алгорит[illegible]енных действий является универсальным.

ПРИМЕЧАНИЕ!

Если настройки беспроводной сети Вам известны, тогда Вы можете пропусти... нный пункт инструкции и перейти к пункту 6.3.2 данного Руководства.

Рассмотрим процесс определения настроек беспроводн... Fi сети с ... щью подключенного к ней ноутбука.

Для определения текущих настроек беспроводной Wi-Fi сети ноут... чите от него кабель Ethernet и подключитесь к Вашей беспроводн...

После подключения к Wi-Fi сети нажмите ***Пуск – ...ль упр...ени...*** (*Рис. 6.8*).

В открывшемся ...иалоговом окне ...берите пункт **[Просмотр состояния сети и задач]** в разделе **[Се... ...нет]** (*Рис. 6...*

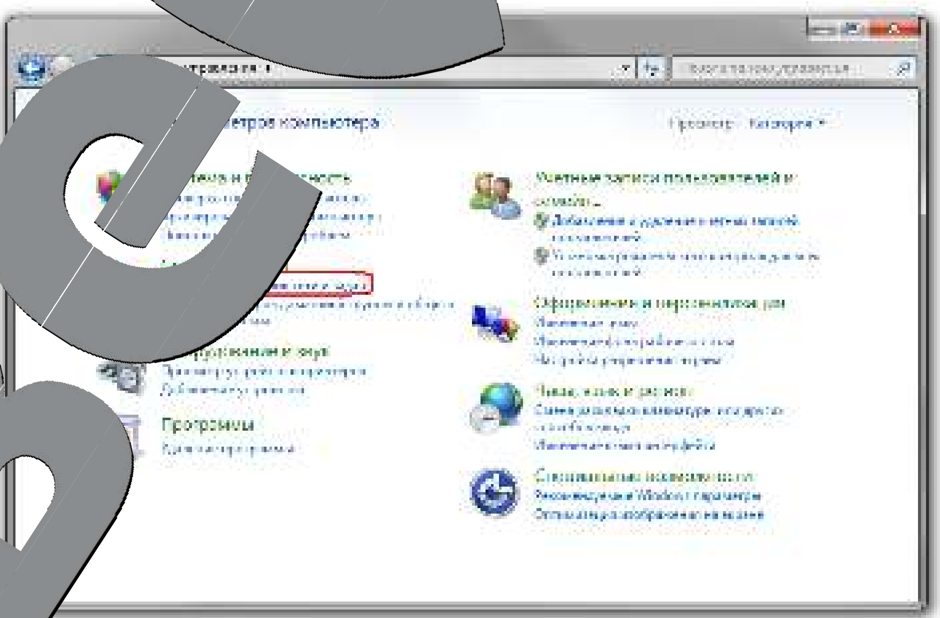


Рис. 6.9

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

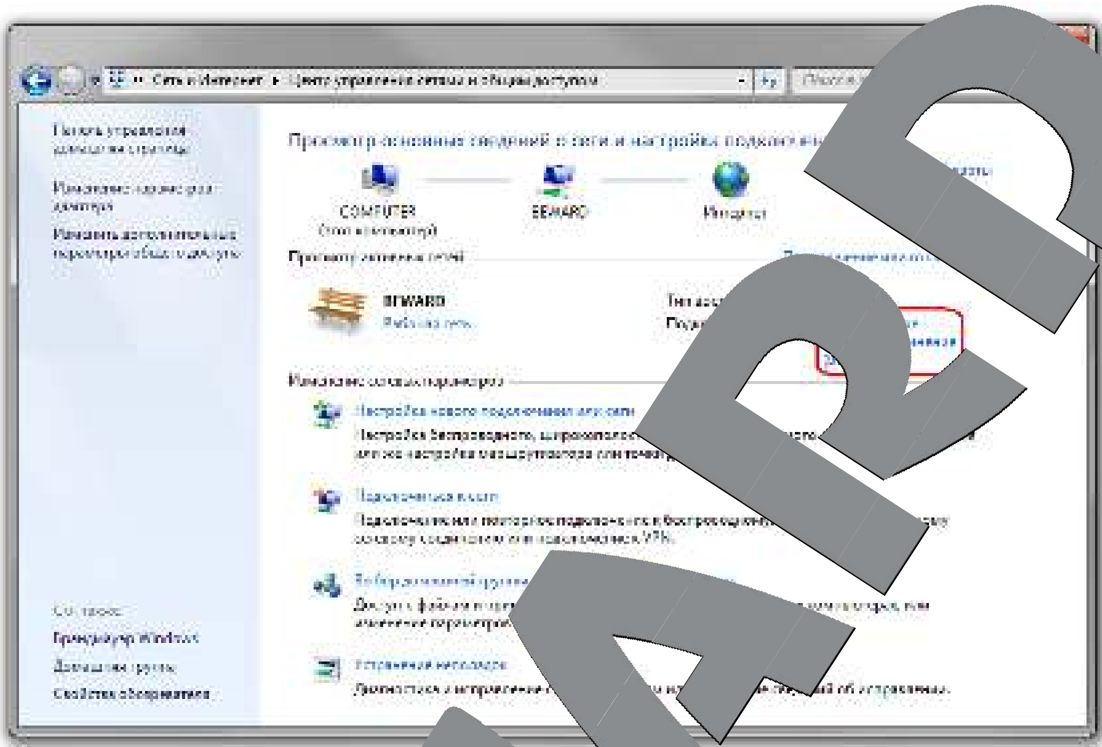


Рис. 6.10

ПРИМЕЧАНИЕ!

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

ВНИМАНИЕ!

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

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

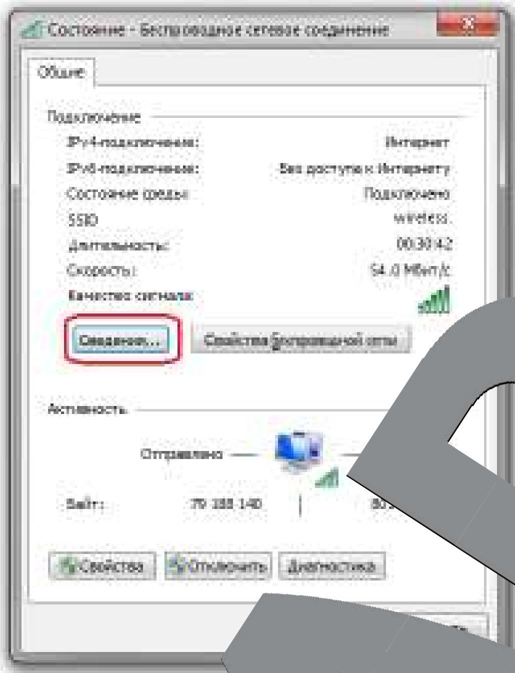


Рис.

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

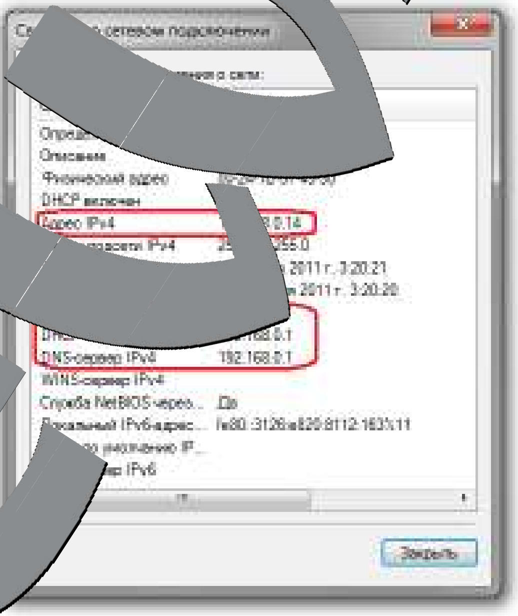


Рис. 6.12

... шит... ченные на *Рисунке 6.12* данные: **[Адрес IPv4]**, **[Маска подсети IPv4]**, **... вер IP... [Шлюз по умолчанию]**.

... бходимо подключить IP-камеру N120S к Вашей беспроводной сети. При этом каме... 120S должна быть включена в Вашу проводную локальную сеть для первоначальной настройки.

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

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

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

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

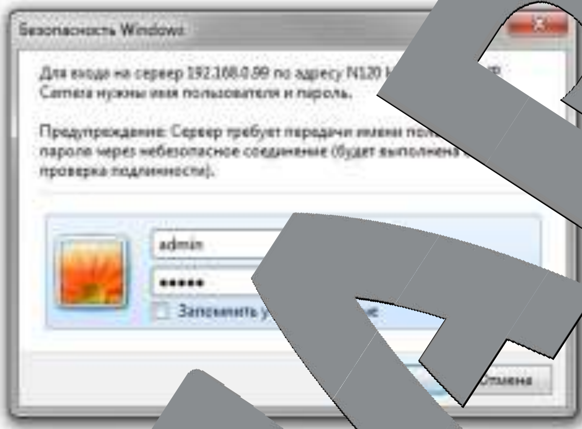


Рис. 6.13

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

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

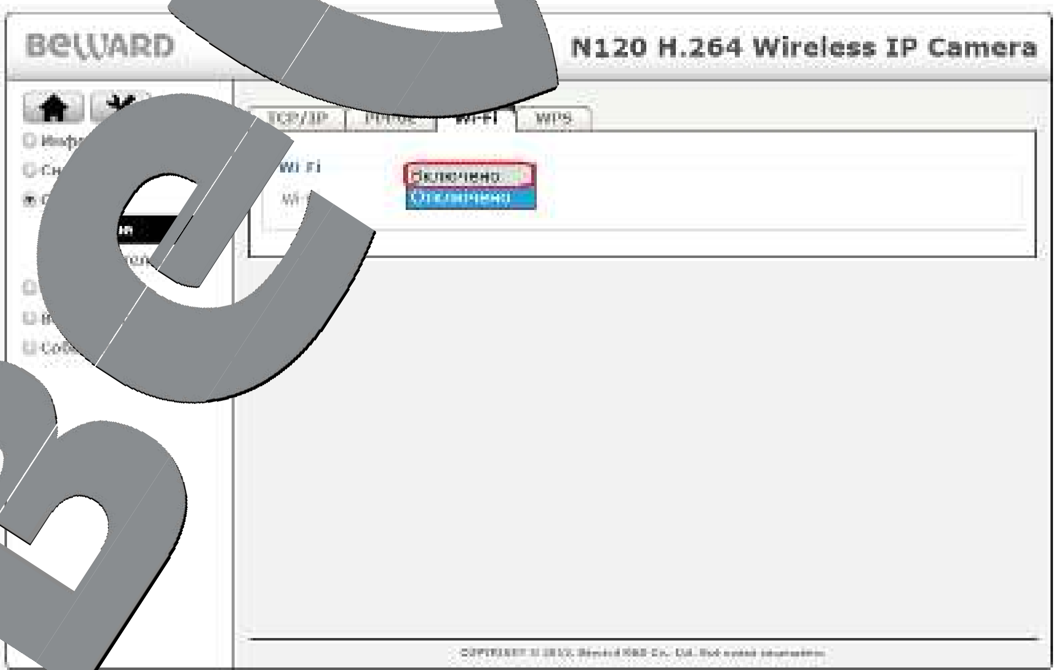


Рис. 6.14

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

Выберите среди найденных беспроводных сетей Вашу, щ[illegible] левой кнопкой мыши (*Рис. 6.15*).

ПРИМЕЧАНИЕ!

Чтобы найти Вашу сеть в таблице **[Обнаруженные беспровод[illegible]ети]**, на[illegible]ку, для которой значение столбца **[ESSID]** совпадает с записанным [illegible]ем **[ESSI[illegible]** см. пункт 6.3.1 данного Руководства).

Р[illegible] 15

После это[illegible]тоит выбрать способ настройки соединения с сетью. Существует два варианта[illegible]:

- **А[illegible]тич[illegible]й** - кн[illegible]ка **[Подключиться]**
- **Р[illegible]на[illegible]ойка[illegible]** [illegible]ка **[Вручную]**

Если [illegible]оводной сети есть DHCP-сервер, который назначает дина[illegible]ские I[illegible]ройствам в сети, то Вы можете выбрать вариант автоматической н[illegible]Wi-Fi подключения. Для этого нажмите кнопку **[Подключиться]**, после чего [illegible]вится [illegible]денное на *Рисунке 6.16*.

Е[illegible] сеть [illegible]щищена от несанкционированного подключения, то потребуется ввести кл[illegible]ова[illegible]пароль) данной сети. Введите ключ шифрования в поле **[Пароль]**, затем повтор[illegible]е тот же ключ шифрования в поле **[Повторно]** (*Рис. 6.16*). Значения настроек в п[illegible]ях **[Аутентификация]** и **[Шифрование]** определяются автоматически.

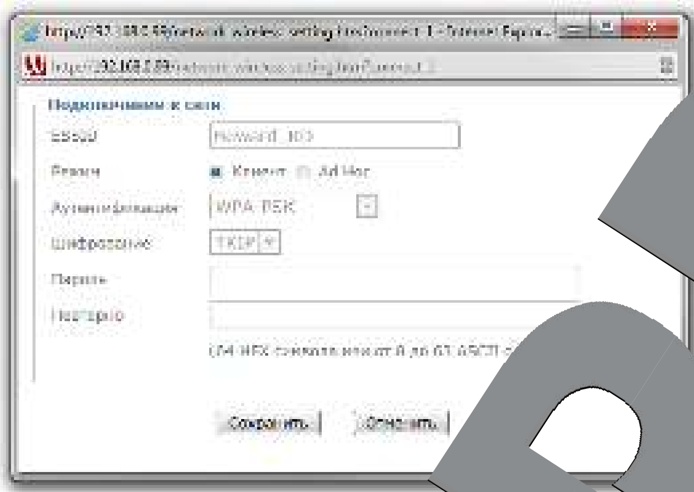


Рис. 6.16

Для сохранения изменений сетевых ... беспроводн... соединения нажмите кнопку **[Сохранить]**. Если все настройки ... то подключение пройдет успешно, после чего появится окно, приведен... *Рис...*

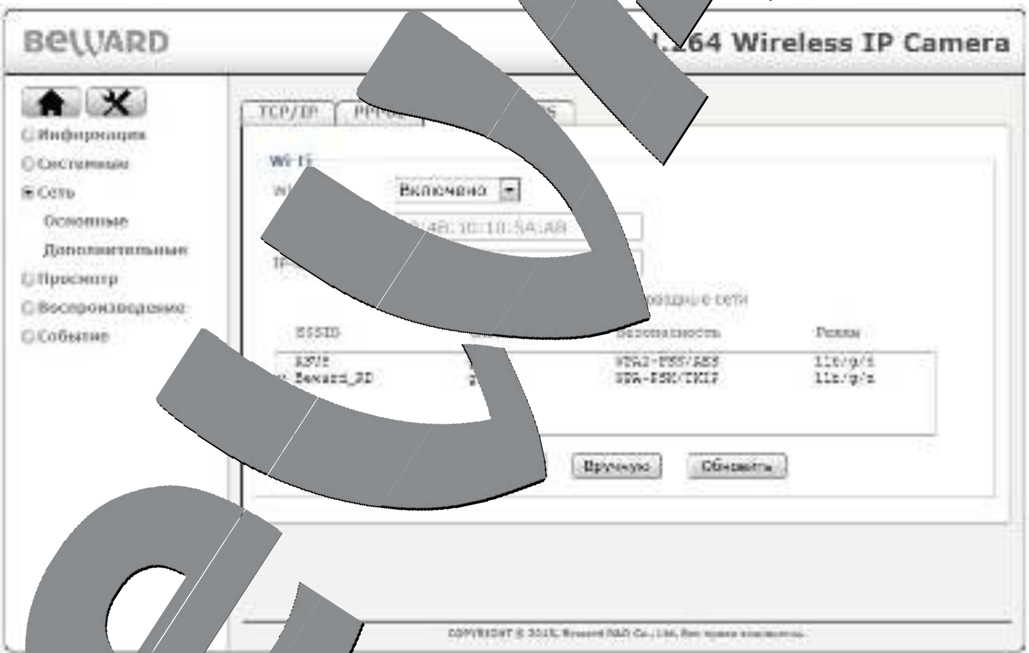
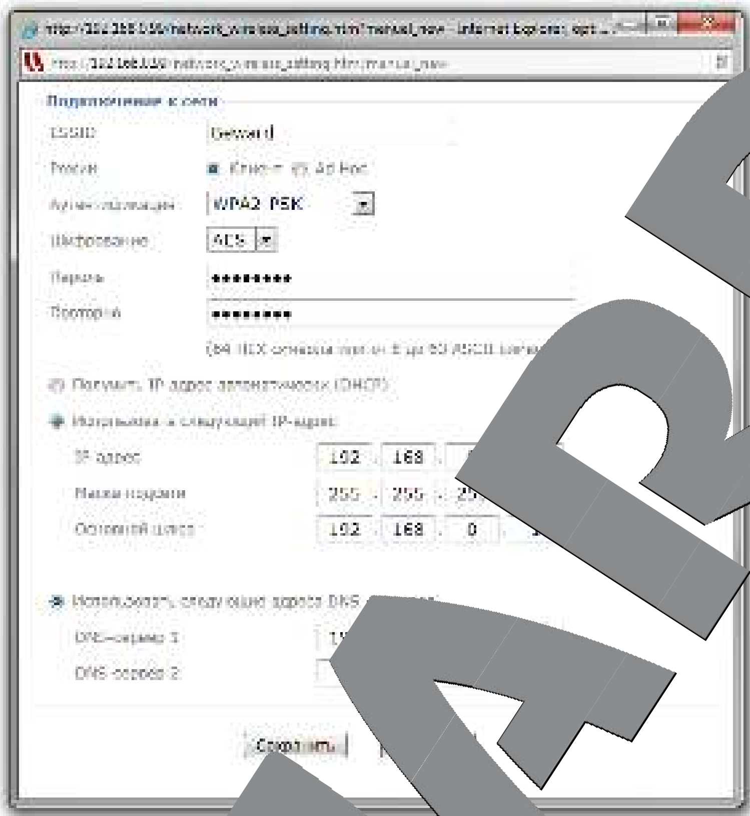


Рис. 6.17

...анном ...ке **[IP-адрес]** указан IP-адрес, присвоенный DHCP-сервером для б...ого соединения камеры. Используя данный IP-адрес, Вы сможете зайти на ...еру ч... ...одное соединение.

Е... в В... беспроводной сети нет DHCP-сервера либо по каким-то причинам не уд... ...ано... соединение автоматическим способом, описанным выше, то Вы можете исполь... ...ную настройку беспроводного подключения. Для настройки подключения вручную наж...те кнопку **[Вручную]**. Появится окно, приведенное на *Рисунке 6.18*.



[illegible] 18

На *Рисунке 6.18* пока[illegible] поля, котор[illegible] будет необходимо заполнить вручную. Введите в данные поля знач[illegible]тствующие [illegible]араметрам Вашей беспроводной сети, которые были определены с помо[illegible]кт 6.3.1 данного Руководства).

ESSID: введите [illegible]я Вашей беспроводной сети.

[Аутентифика[illegible] [illegible]берите тип а[illegible]ентификации в Вашей сети. Для большей безопасности рекоменду[illegible]ентификации WPA2 при условии поддержки со стороны маршр[illegible]тора.

[Шифр[illegible] [illegible]рите тип шифрования, который используется в Вашей сети. Определяет[illegible]тома[illegible]ски, [illegible]о доступен для изменения и при необходимости может быть изменен по[illegible]ате[illegible] на д[illegible]значение.

Паро[illegible] [illegible]сет[illegible]дена от несанкционированного подключения, то потребуется ввести ключ [illegible] (пароль) данной сети. Введите ключ шифрования в поле **[П[illegible]** [illegible]тем повторно введите тот же ключ шифрования в поле **[Повторно]** (*Рис. 6.18*).

IP[illegible]дите значение из той же подсети, что и значение IP-адреса, записанное [illegible]и в[illegible]те 6.[illegible]анного Руководства, но отличающейся от него и других адресов в сети.

[illegible]**ска п**[illegible]**ти**: введите значение маски подсети.

[illegible]**шлюз**: введите значение основного шлюза.

Пред[illegible]**итаемый DNS-сервер**: введите значение DNS-сервера.

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

В появившемся окне необходимо нажать кнопку **[ОК]** (*Рис. 6.1*[illegible]

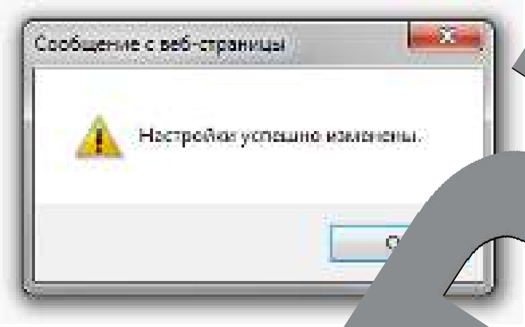


Рис. 6.19

Подождите некоторое время (около 30 секунд) для п[illegible]ия новых настроек камеры и завершения процесса подклю[illegible]роводному соединению. После завершения настройки беспроводного сое[illegible]я в [illegible]**адрес]**, как показано на *Рисунке 6.18*, должен появиться тот IP-а[illegible]ко[illegible]и вы назначили камере для беспроводного соединения.

6.3.3. Проверка правильности настро[illegible]i-Fi-с[illegible]единения IP-камеры

Для контроля правил[illegible]и сетевых нас[illegible]ек беспроводного Wi-Fi подключения камеры и компьютера нужн[illegible]ся к каме[illegible] через браузер Internet Explorer. Для этого нажмите ***Пуск – Все Прогр***[illegible]троку **[Internet Explorer]**. Введите в адресной строке IP-ад[illegible], присвоенный ка[illegible]ере для беспроводного Wi-Fi соединения (*Рис. 6.20*).

ВНИМАНИЕ!

Для проверки [illegible]Wi-Fi-соединения введите в браузере IP-адрес, указанный в пункте 6.3.2 данног[illegible]водст[illegible]

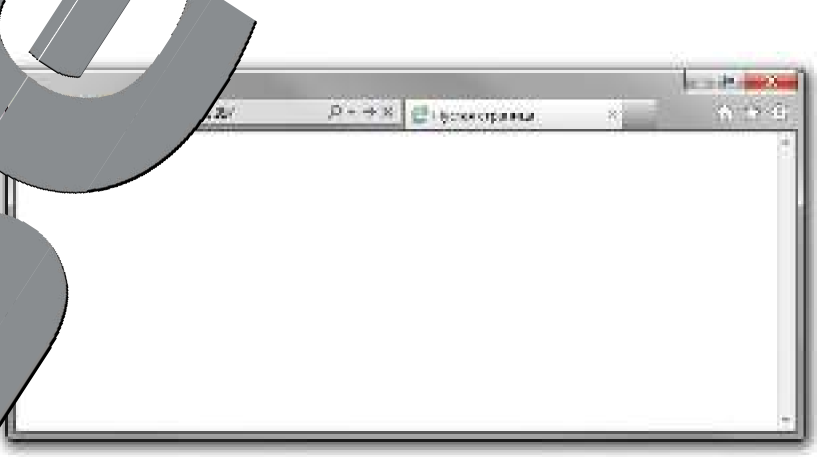
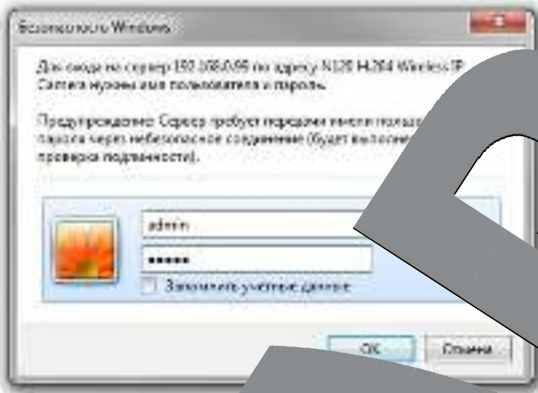


Рис. 6.20

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

ВНИМАНИЕ!

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



Ри

При правильно выполненных йствиях м кете увидеть через веб-браузер изображение с Вашей IP-камеры (*Р*

Рис. 6.22

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

Глава 7. Подключение IP-камеры к сети Интернет

7.1. Общие сведения о подключении IP-камеры к сети Ин[illegible]

При установке IP-камеры N120S в квартире, коттедже или о[illegible]обы[illegible]уется иметь к ней доступ не только из локальной сети того или иного [illegible]щения, но [illegible] сети Интернет.

В этом случае для одновременной работы компьютеров, но[illegible]Р-ка[illegible]мер и другого оборудования в сети Интернет, чаще всего, испол[illegible]ршрутиза[illegible]При этом для подключения по Wi-Fi требуется, чтобы маршрутиза[illegible]ме[illegible]ержку беспроводного интерфейса.

При организации доступа к IP-видеокамера[illegible]ти [illegible]ет, как правило, используются следующие три варианта:

- Имеется выделенный провайдером внешний статиче[illegible]-адрес или PPPoE-соединение. При этом, данный I[illegible]PPoE-соединение) используется для подключения только одной IP-[illegible]ы и н[illegible]ыть назначен еще какому-либо устройству.
- Имеется выделенный пр[illegible]ром [illegible]й статический IP-адрес, который используется для подключе[illegible]Инте[illegible]фисной или домашней локальной сети, к которой, в свою очередь, пла[illegible]уется подключить одну или несколько IP-камер. При таком [illegible]чении испол[illegible]ется маршрутизатор. При этом число подключаемых каме[illegible]осно[illegible]м, от количества переназначаемых маршрутизатором портов.
- Провайдер [illegible]ыделяет внешни[illegible] статический IP-адрес. IP-адрес назначается провайдеро[illegible]ки, то есть [illegible]ак, что при каждом новом подключении этот адрес присваива[illegible]яется в процессе работы (такая ситуация особен[illegible]рна при работе через ADSL и GPRS). В этом случае, чтобы обе[illegible]ожность подключения одной или нескольких камер к сети И[illegible]ет, в[illegible]ависи[illegible]ти от того, какой IP-адрес выделен провайдером в данный м[illegible]обхо[illegible] задействовать интернет-службы, работающие с ди[illegible]ами.

[illegible]ее, э[illegible] организации доступа к IP-камерам из сети Интернет будут р[illegible] подробнее.

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

7.2.1. Использование статического IP-адреса

Для подключения IP-камеры к сети Интернет необходи[illegible]зменить ее [illegible]вые параметры в соответствии с данными, полученными от провайде[illegible]вило, п[illegible]дер предоставляет следующие сетевые настройки: IP-адрес (в данном [illegible]ский), Маска подсети, Сетевой шлюз и адрес DNS-сервера.

Для получения доступа к IP-камере через сеть И[illegible]тическому IP-адресу необходимо выполнить следующие шаги:

Шаг 1: подключите IP-камеру напрямую к Ваш[illegible]

Шаг 2: измените сетевые настройки проводного [illegible] камеры (см. пункт 5.5 данного Руководства) в соответствии с настройками, предос[illegible]и Вашим Интернет-провайдером (*Рис. 7.1*).

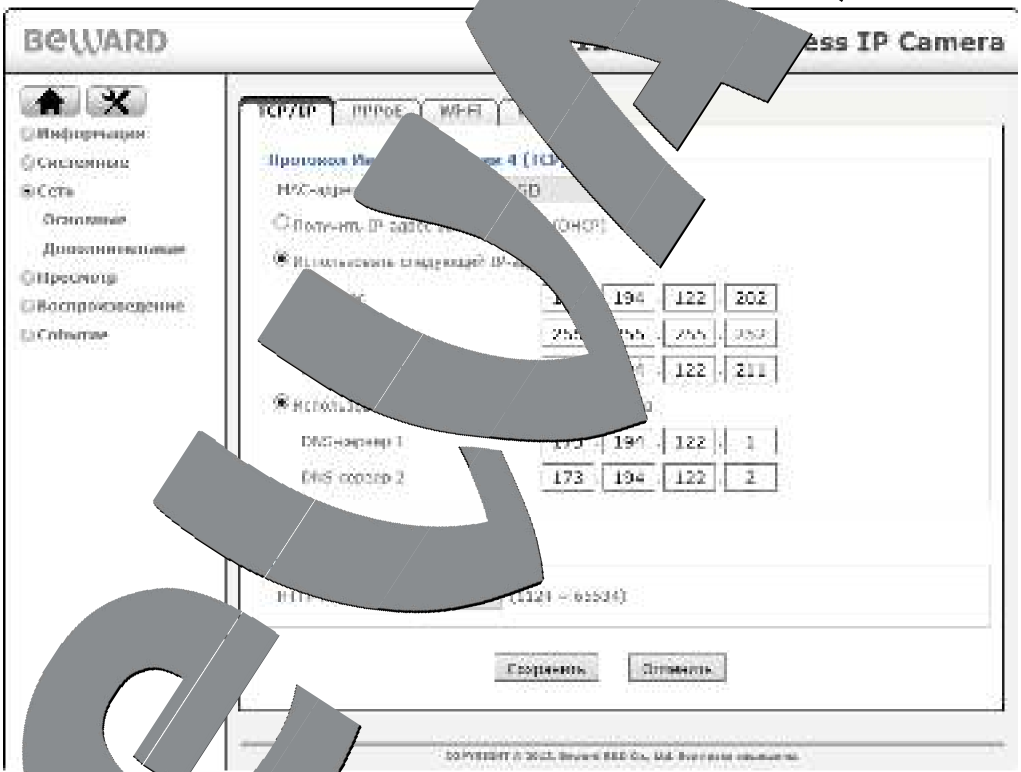


Рис. 7.1

Шаг 3: [illegible]амеру к выделенной сети Ethernet.

[illegible] все параметры указаны верно, камера должна быть доступна в сети Интернет.

В [illegible]м примере провайдер предоставил следующие данные:

- **[illegible]ад[illegible]** [illegible]73.194.122.202
- **Маск[illegible]сети:** 255.255.255.252
- **[illegible]ой шлюз:** 173.194.122.211
- **[illegible]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>** – [illegible]с камеры, **<Port>** – значение HTTP-порта. Так как в данном примере исполь[illegible] HTTP-порта, заданное по умолчанию («80»), то, чтобы обратиться [illegible]-камере [illegible] сеть Интернет, необходимо набрать запрос «http://173.194.122.202».

ПРИМЕЧАНИЕ!
При подключении к камере через HTTP-порт, заданный по [illegible]начение р[illegible]но «80»), запрос в адресной строке браузера имеет вид: **http://<IP>**,– [illegible]> – IP[illegible]с ка[illegible]ры.

7.2.2. Использование PPPoE-соединения

Интернет-провайдер не всегда может обеспечить по[illegible] по статическому IP-адресу. Чаще всего, провайдер организу[illegible] к сети [illegible]рнет через PPPoE-соединение. В этом случае, он предоставля[illegible]**зователя** и **пароль.**

IP-камера N120S поддерживает PP[illegible] дл[illegible]пользования необходимо выполнить следующие шаги:

Шаг 1: подключите IP-камеру [illegible] локал[illegible]ти или напрямую к ПК (см. Главу 5).

Шаг 2: войдите в меню PPPoE-на[illegible] IP-ка[illegible]ы: ***НАСТРОЙКИ*** – ***Сеть – Основные – PPPoE***.

Шаг 3: в текстовых п[illegible]**зователь]**, [illegible]**ароль]** введите значения, полученные от Интернет-провайдера (*Рис. 7.*[illegible]

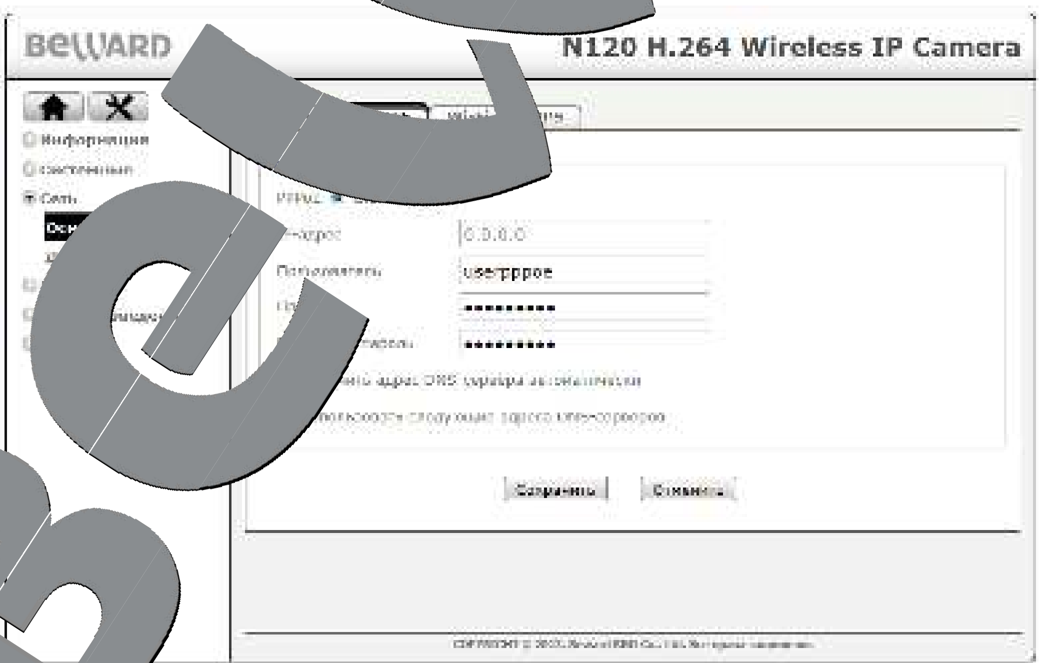


Рис. 7.2

Ша[illegible]я 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 буде[illegible] доступна в [illegible]ет под IP-адресом, присвоенным ей Вашим провайдером и отображае[illegible] **[illegible]P-адрес]** ([illegible]ис. 7.2*).

ПРИМЕЧАНИЕ!

Для удобства, IP-адрес камеры, под которым она доступ[illegible] [illegible]жет быть сообщен на указанный Вами адрес электронной почты (функция «IP-уве[illegible]). Для настройки данной опции, пожалуйста, обратитесь к Руководству по эксплуатации.

Для обращения к IP-камере через [illegible] [illegible]ресной строке браузера вводится следующий запрос: **http://<IP>:<Port[illegible]** [illegible] IP-адрес камеры, назначенный Вашим провайдером при установлен[illegible] PPPoE-с[illegible]ния, **<Port>** – значение HTTP-порта (по умолчанию равное «80»).

ПРИМЕЧАНИЕ!

При подключении к камере че[illegible] заданный [illegible] умолчанию (значение равно 80), запрос в адресной строке браузера имеет [illegible] – IP-адрес камеры.

7.3. Подклю[illegible] через сеть [illegible]тернет к IP-камерам, находящимся в локальной [illegible]

Если доступ [illegible] Интер[illegible]вляется по выделенной линии Ethernet или по ADSL, для по[illegible]льной сети используется маршрутизатор.

ВНИМАНИ[illegible]

Для исполь[illegible] данного [illegible]да подключения необходимо заранее приобрести у Вашего провайдера [illegible]ТИЧЕСКИЙ IP-адрес. Провайдер предоставляет, как правило, ДИ[illegible]ЕСКИЙ [illegible]НИЙ IP-адрес, который доступен только в подсети провайдера. [illegible]ип используемого Вами IP-адреса заранее.

Для того [illegible]ы подключиться к IP-камере из сети Интернет, надо обратиться по IP-ад[illegible] провайдером («внешний» IP-адрес маршрутизатора), и к определенному HTTP-по[illegible]

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 этого требуется выполнить следующие действия:

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

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

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

7.3.1. Использование технологии UPnP

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

- Разрешить использование и настроить функции UPnP Вашего маршрутизатора.

ВНИМАНИЕ!

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

- Разрешить использование и настроить функцию UPnP IP-камеры.

Чтобы настроить функцию UPnP IP-камеры, выполните следующие действия:

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

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

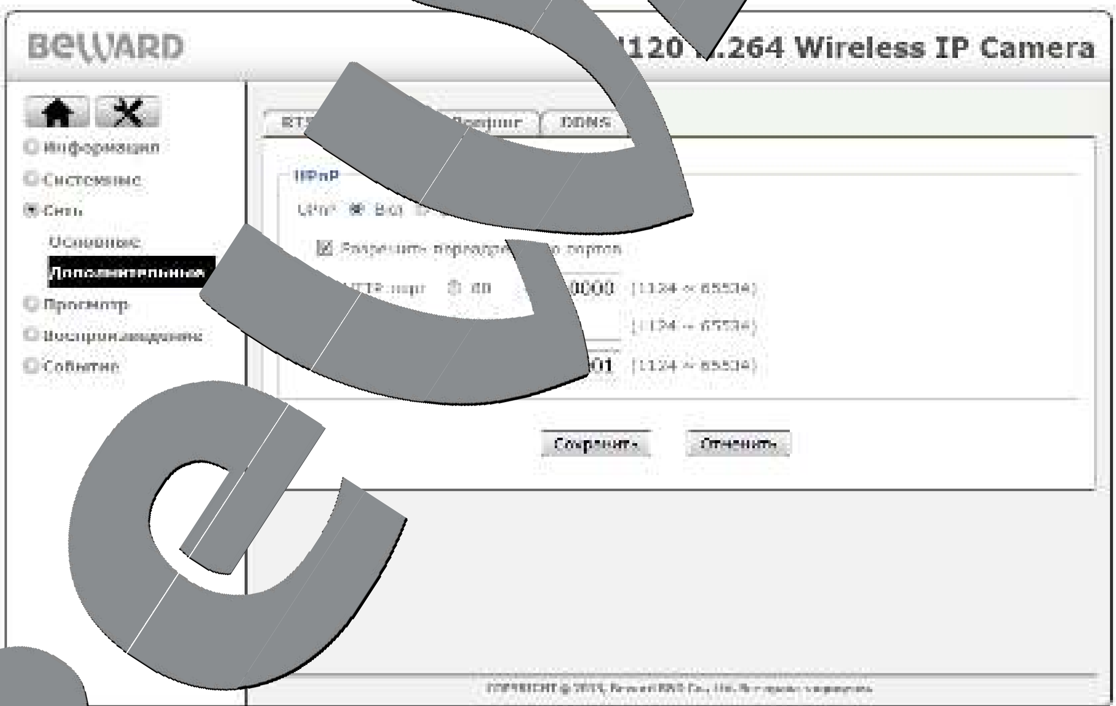


Рис. 7.3

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

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

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

ВНИМАНИЕ!
Для применения сетевых параметров требуется перезагрузка устройства.

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

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

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

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

7.3.2. Настройка ручной переа[illegible]з маршрутизатора.

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

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

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

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

Для подключения IP-камеры к сети Интернет требуется назначить порты, через которые будет осуществляться внешний доступ к ее настройкам и видеопотоку. В локальной сети эти порты по умолчанию имеют следующие значения: HTTP-порт – «80», RTSP-порт – 554.

ВНИМАНИЕ!

При обращении из сети Интернет для всех камер, находящихс[illegible]й локальн[illegible]ети, существует только один IP-адрес (выданный провайдером). Поэтому для [illegible]тим[illegible]рам необходимо каждой назначить свои группы портов.

Для изменения портов IP-камеры выполните сле[illegible]е де[illegible]я:

ВНИМАНИЕ!

HTTP-порты камер можно перенаправлять с помощью виртуаль[illegible]ра, однако RTSP-порты должны быть разными у всех камер и транслироваться «порт в пор[illegible]ветственно, для всех камер необходимо задать различные значения [illegible]

Шаг 1: откройте раздел меню ***НАСТР[illegible]*** [illegible] ***Сеть – Дополнительные – RTSP***.

Шаг 2: введите в поле **[R[illegible]** [illegible] новое [illegible]ние порта RTSP, отличное от значения по умолчанию. Например, пусть в ка[illegible]тве R[illegible]SP-порта используется порт 3001 (*Рис. 7.4*).

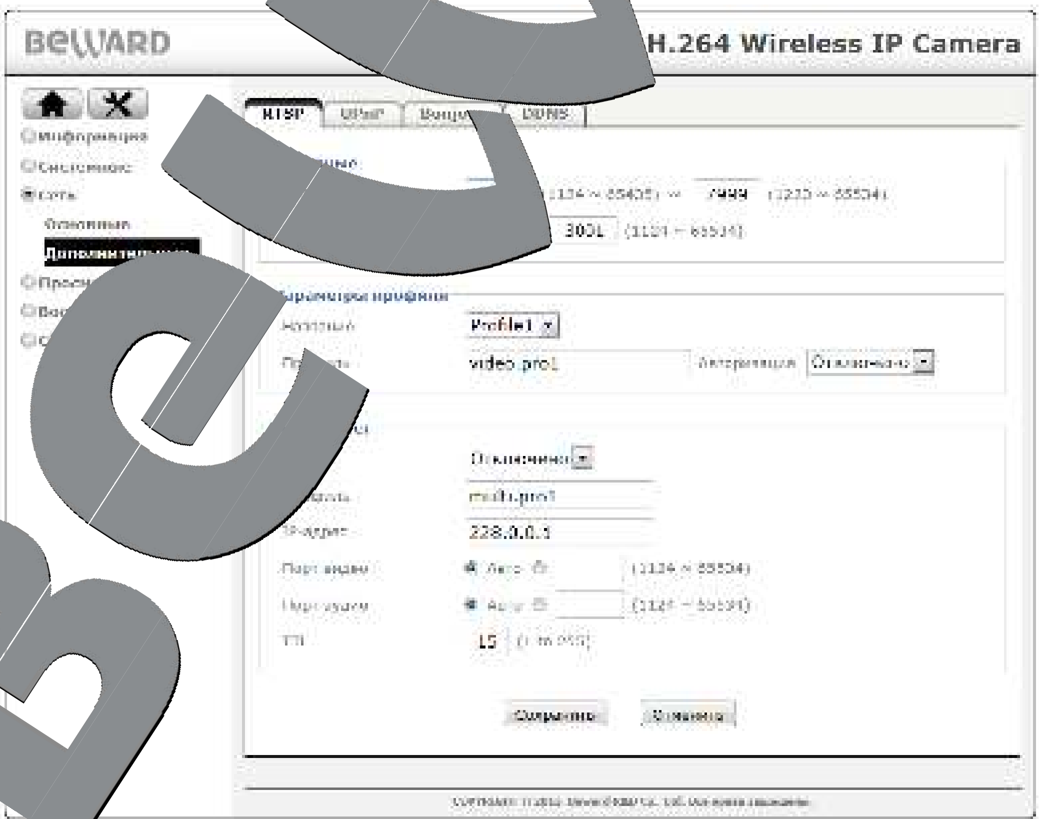


Рис. 7.4

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

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

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

Камера настроена. Осталось правильно настроить маршрутизатор.

Для настройки маршрутизатора выполните следующие действия:

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

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

Рис. 7.6

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

[Service Port]: укажите порт, который будет использоваться д ере из сети Интернет.

ПРИМЕЧАНИЕ!
Во избежание конфликтов не используйте для перенаправлен ртов за анные значения. Рекомендуется использование портов диапазона 1 чения по в от 0 до 1123 официально зарегистрированы под различные протоко ужбы, жен я.)

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

[IP Address]: укажите IP-адрес камеры которой настра ся перенаправление.

Остальные пункты не требуют настр

Добавьте правило для порта HTTP (*Р*

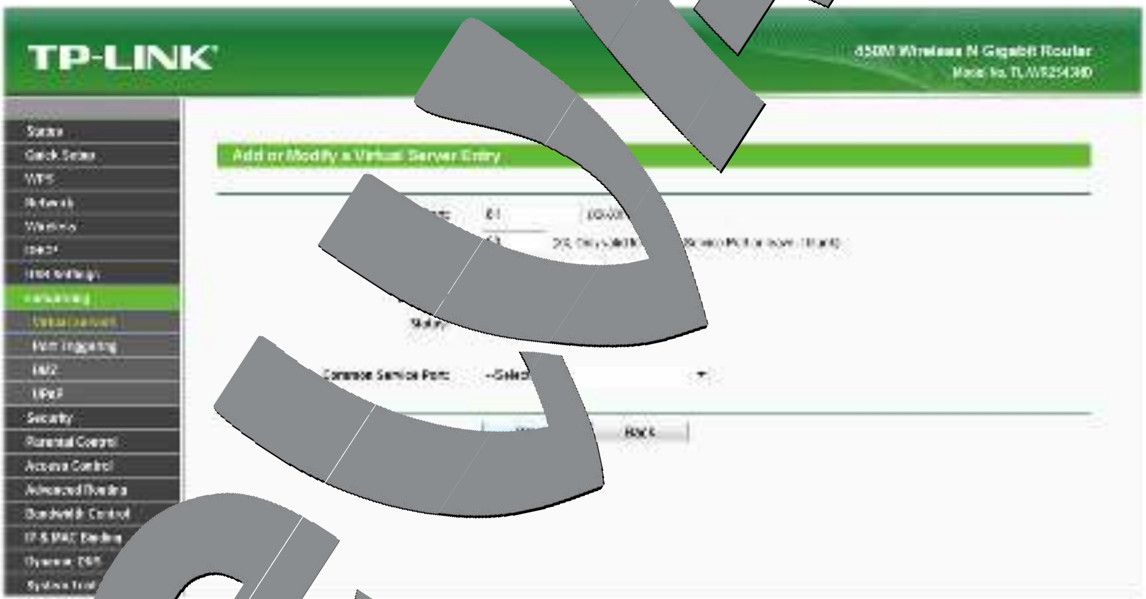


Рис. 7.7

Шаг ите кн **ave]**, чтобы сохранить правило. Правило добавлено (*Рис. 7.8*):

Р

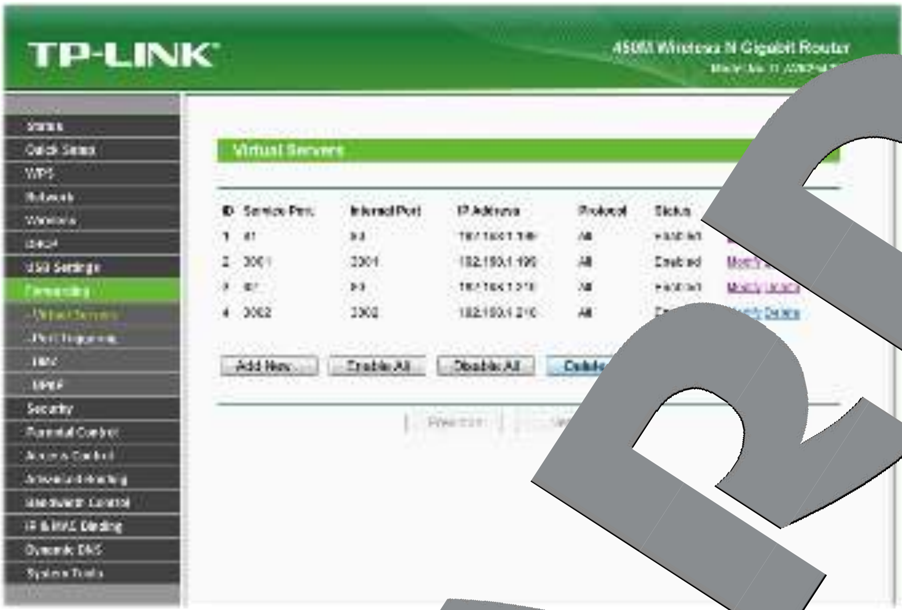
Шаг 5: тем же способом добавьте пра... ...я по... (*Рис. 7.9*):

ВНИМАНИЕ!

HTTP-порты камер можно перенаправлят... ...ью ви... ...ьного сервера, однако RTSP-порты должны быть разными у всех камер и транслирова... «порт в порт»! Например, порт 3001 камеры №1 транслируется в порт 3... ...аршрутизатора, ...рт 3002 камеры №2 – в порт 3002 маршрутизатора и т.д.

Рис. 7.9

Ш... ...ли Вы используете несколько камер, то Вам необходимо повторить **шаги 2-5** для остальных камер (*Рис.7.10*).



Р[illegible]

Настройка маршрутизатора завершен[illegible]

Теперь, чтобы получить доступ к камер[illegible]ти[illegible]ерн[illegible], надо обратиться к ней по IP-адресу, выданному провайдером ([illegible]ний» [illegible]с маршрутизатора), и назначенному ей порту HTTP.

В рассмотренном примере IP-адрес ма[illegible]тизат[illegible]ра – «173.194.122.201». HTTP-порт, назначенный камере для пер[illegible]есации,– «81». [illegible]ачит, для обращения к камере из сети Интернет необходимо в адре[illegible]браузера н[illegible]рать запрос: http://173.194.122.201:81/.

7.4. Пример подключения через сеть Интернет с использованием DDNS

7.4.1. Общие сведения о подключении через Интернет с испол[illegible]м DDNS

В случае если IP-адрес выдается компьютеру на определен[illegible] всего лишь на один сеанс связи), такой адрес называют динамическим[illegible]ольшинств[illegible]чаев Интернет-провайдеры предоставляют пользователям динамиче[illegible]реса. Од[illegible] для того, чтобы можно было обратиться к оборудованию из сети Интерне[illegible]мо[illegible], оно должно иметь постоянный или фиксированный адрес. С это[illegible]емой ле[illegible]вляется служба Dynamic DNS (DDNS).

Сервис Dynamic DNS предоставляет Вам [illegible]зможно[illegible] с[illegible] IP-камеры легкодоступными из сети Интернет, даже если [illegible]м [illegible]нии постоянно меняющийся, динамический IP-адрес. Внешние пользова[illegible]а будут иметь доступ к оборудованию, обращаясь к нему по его доменному имени.

В этом случае вместо того, чтобы [illegible] оборудов[illegible]ию по IP-адресу, Вы обращаетесь к нему по доменному имени ви[illegible]s.org.

Для этого надо зарегистрироваться на [illegible] пр[illegible]де[illegible] сервиса DDNS (например, www.dyndns.com), сообщить один ра[illegible]ущий I[illegible] оборудования и выбрать доменное имя, по которому в дальнейшем Вы [illegible]ращат[illegible]борудованию.

Тогда при смене IP-адреса или при н[illegible] подк[illegible]чении к сети Интернет устройство получает от Интернет-провай[illegible]ра новый IP-а[illegible]с. Он обрабатывается встроенным в камеру ПО, которое обращ[illegible]йт провай[illegible]ра DDNS для того, чтобы сообщить значение текущего IP-адреса. [illegible]ит в соответствие этому IP-адресу зарегистрированное Ва[illegible]и ранее доменное имя.

Рассмотрим п[illegible]боты с DDNS[illegible]ровайдером http://www.dyndns.com. Методика регистрации и работы с д[illegible]DDNS аналогична данной.

> **ПРИМЕЧАНИ[illegible]**
> Услуги пров[illegible] DDN[illegible]гут предоставляться на платной основе.
> Внешний ви[illegible]виса[illegible]S мо[illegible]личаться от приведенного на скриншотах ниже.
> Рассматрив[illegible]ример сл[illegible]олько для общего ознакомления с работой сервиса DDNS.

[illegible] досту[illegible]евому ресурсу с использованием доменного имени выполните с[illegible]

- [illegible]ебе учетную запись (Account) на сайте www.dyndns.com для дальне[illegible]й регистрации на сервере.
- [illegible] на сайте www.dyndns.com доменное имя (Hostname) для своего сервера. [illegible]ожете выбрать любое незанятое в этом домене имя для своего

оборудования, например, camera184. Соответственно получите домен третьего уровня для своего оборудования www.camera184.dyndns.org.

- Настройте соответствующим образом оборудование.

7.4.2. Регистрация на сервере DynDNS

Шаг 1: зайдите на сайт www.dyndns.com, для создания уче… си… мите справа вверху **[Sign In]** и в выпавшем списке выберите ст… **[Create a… …t]** (*Рис. 7.11*).

Рис. 7.11

Далее Вы автома… …раницу создания учетной записи (*Рис. 7.12*).

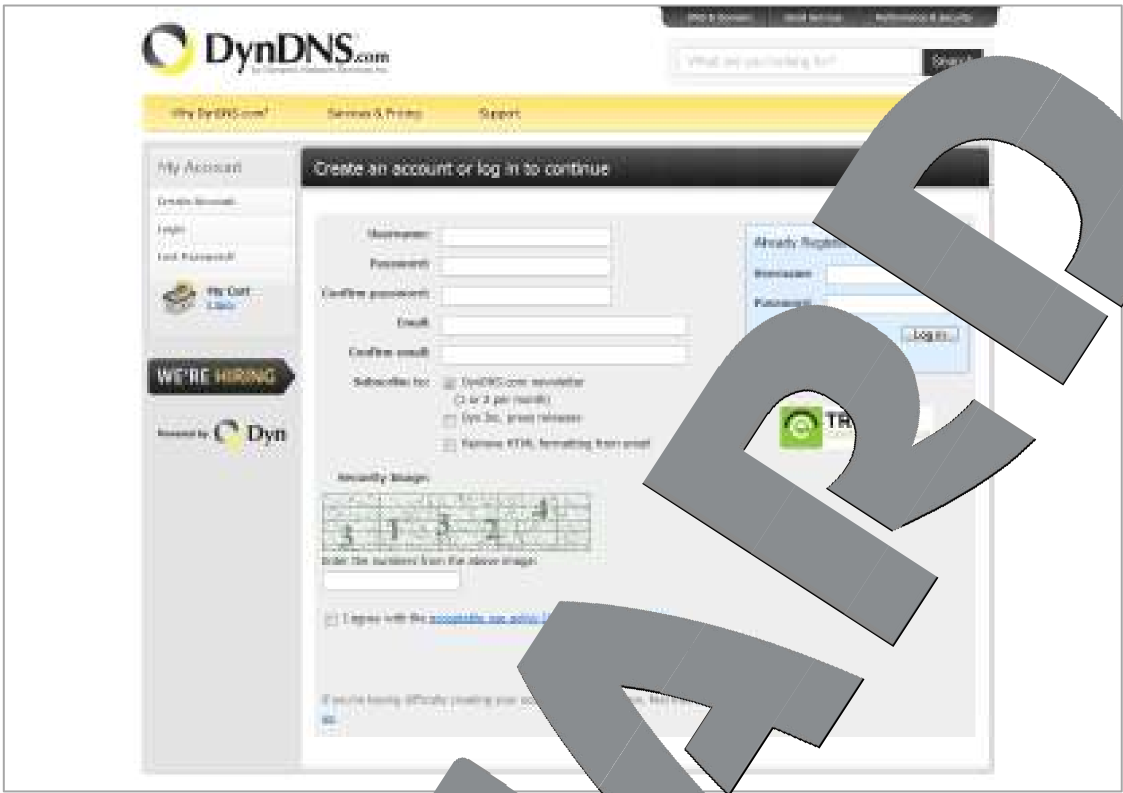


Рисунок 7.12

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

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

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

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

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

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

Введите код, который видите на картинке, и поставьте фл[illegible] для пунк[illegible]**gree with the acceptable use policy (AUP) and privacy policy]**. [illegible]чает со[illegible]е с условиями лицензионного соглашения для создания одного бесплатно[illegible]а.

В качестве примера используется: имя пользователя **[**[illegible]**me]** – с[illegible]4, адрес электронной почты **[E-mail]** – camera184@yandex.ru[illegible]оизвольн[illegible]й пароль (например, 123456).

Для завершения регистрации и окончания [illegible] акк[illegible]мите на кнопку **[Create Account]** (*Рис. 7.13*).

Рис. 7.13

Шаг [illegible] заполнении формы Вы получите сообщение о том, что оста[illegible]один ш[illegible]я учетной записи: **[One more step to go...]** (*Рис. 7.14*).

Ри[illegible]

Шаг 4: через несколько минут на [illegible]онны[illegible]ый ящик, указанный при регистрации, придет письмо от [illegible]лужбы [illegible] D[illegible] Support» (почтовый адрес: support@dyndns.com). Для подтвер[illegible]гистр[illegible]етной записи необходимо перейти по указанной в нем ссылке.

После перехода по а[illegible]есу, указанном[illegible] теле письма, откроется страница с подтверждением создания [illegible]ии Вашей у[illegible]тной записи. Для входа на сайт под созданной учетной записью вве[illegible] **[Confirm Account]** (*Рис. 7.15*).

Рис. 7.15

Ш[illegible]дание учетной записи для сервиса DynDNS завершено (*Рис. 7.16*).

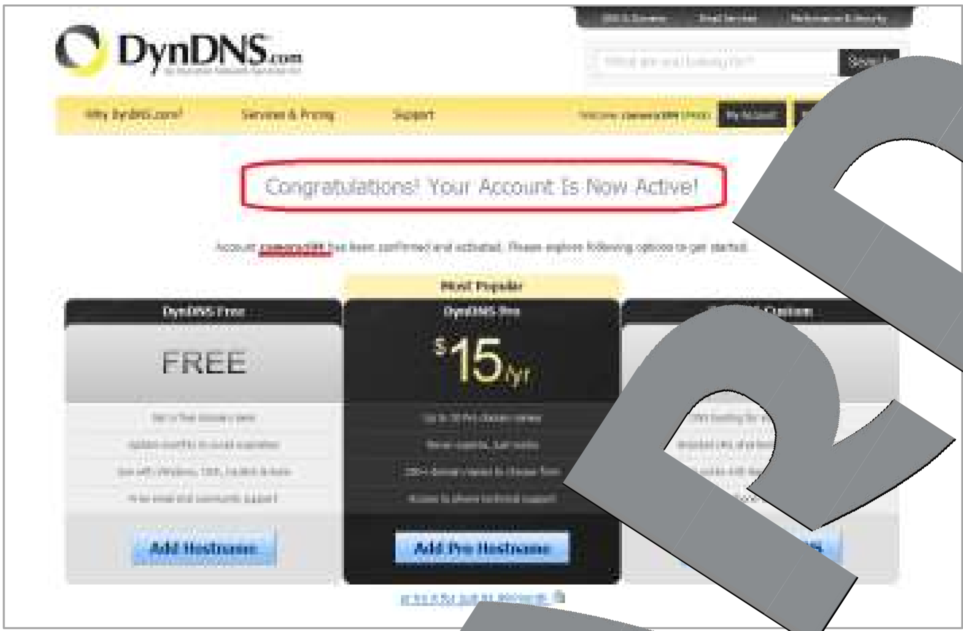


Рис. 7.16

7.4.3. Создание доменного имени на сервере DynDNS

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

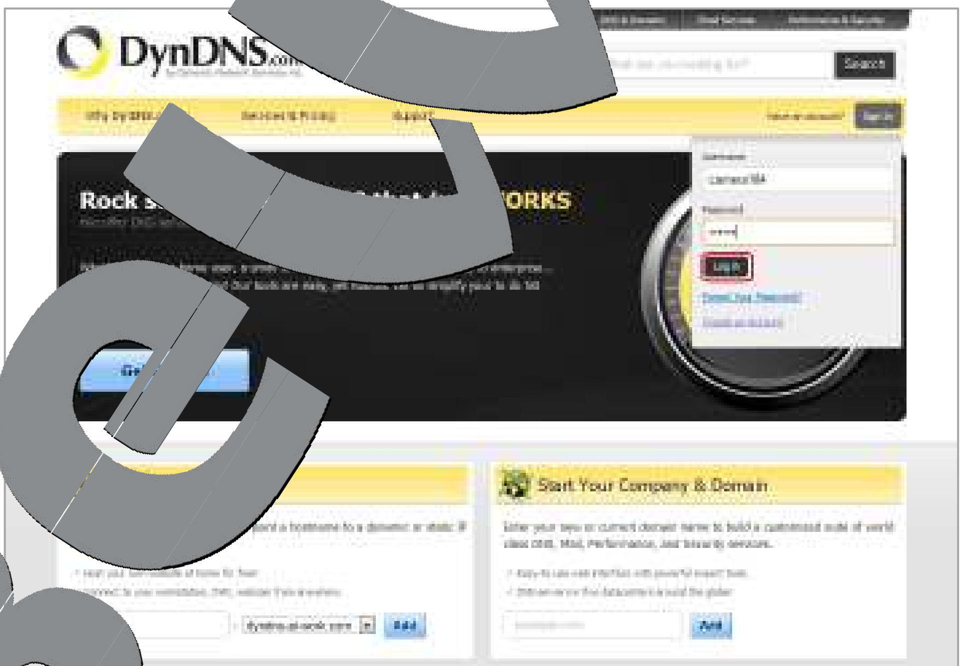


Рис. 7.17

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

Рис. 7.18

Шаг 3: на открывшейся странице [illegible] необходимо настроить параметры соединения с устройством. Выберите желаемое имя домен[illegible] dyndns.org.

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

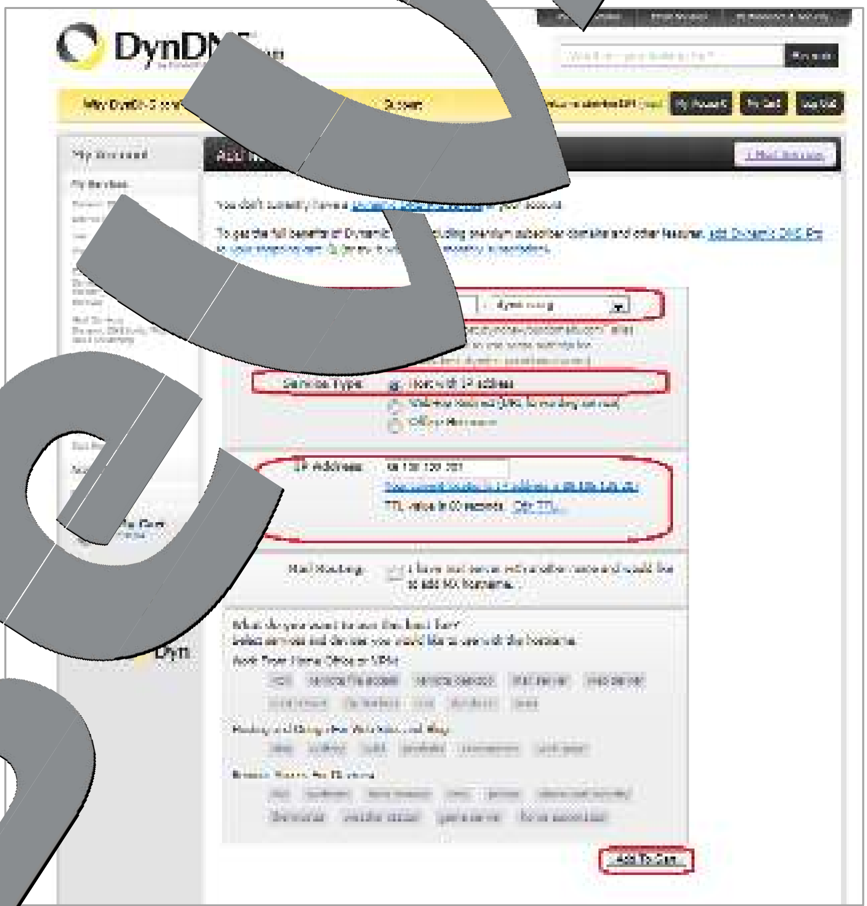


Рис. 7.19

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

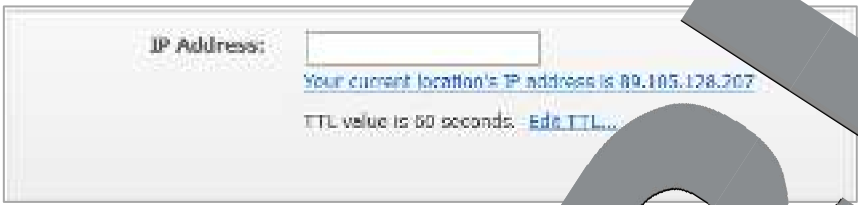


Рис. 7.20

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

Шаг 4: при успешном создании ...ого имени ...роется страница с подтверждением этого. Так для примера, о... указан созданный аккаунт camera184.dyndns.org. Для активации доменн...ени ...нопку **[Next]** (*Рис. 7.21*).

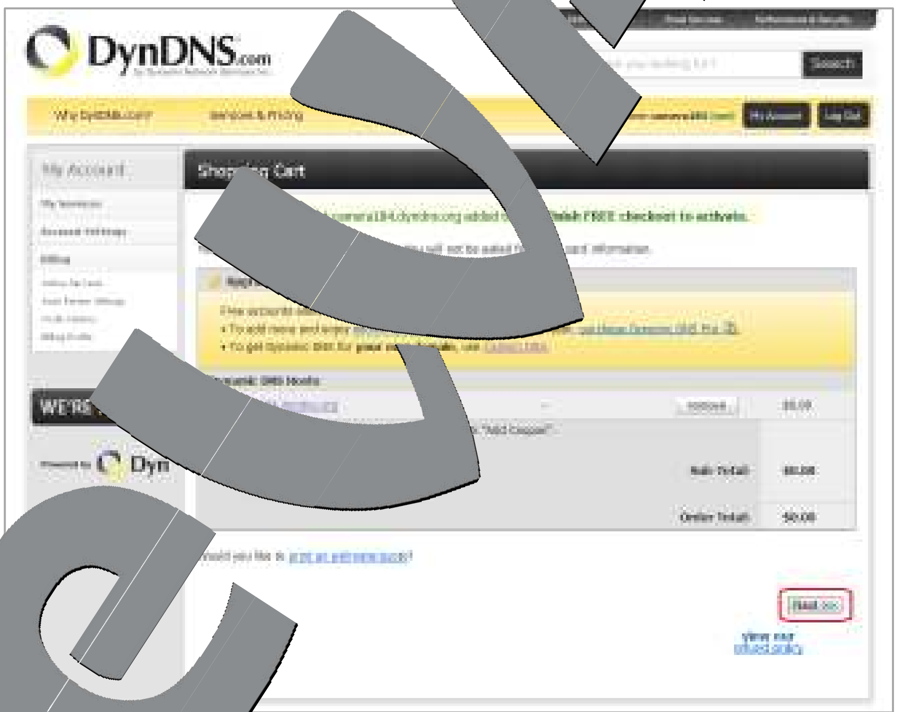


Рис. 7.21

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

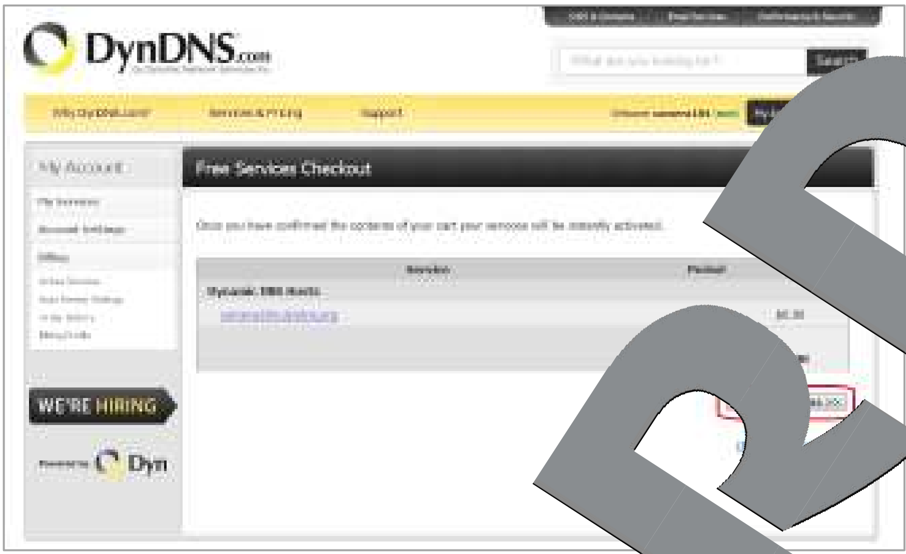


Рис. 7.22

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

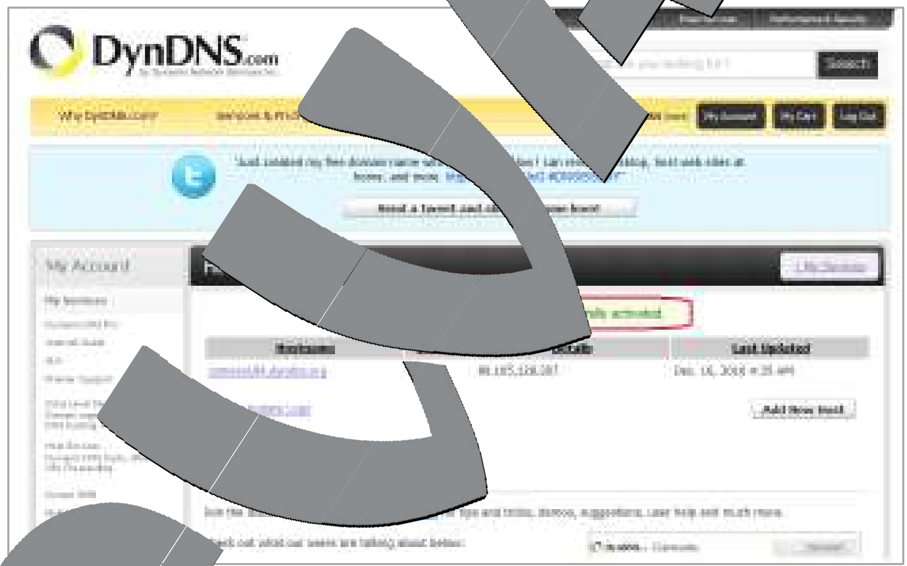


Рис. 7.23

Шаг 6: создание доменного имени на сервере DynDNS завершено.

7.4.4. Настройка оборудования для работы с сервисом DynDNS

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

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

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

ВНИМАНИЕ!

IP-камера должна быть подключена к сети Интернет напрямую.

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

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

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

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

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

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

ВНИМАНИЕ!

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

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

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

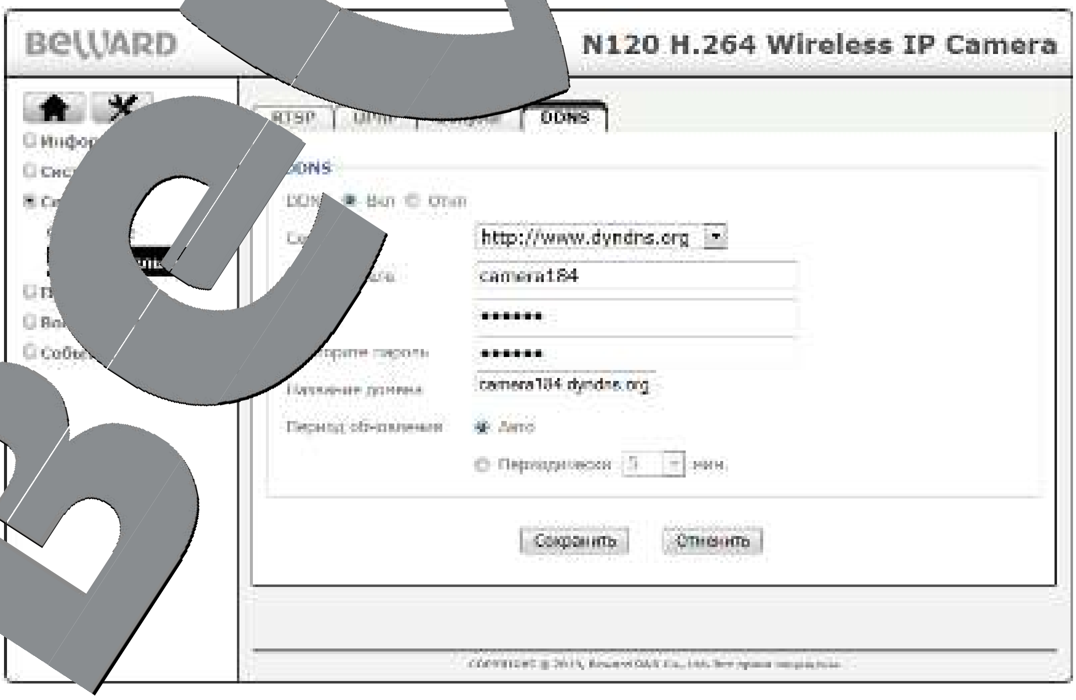


Рис. 7.24

ВНИМАНИЕ!
Для применения сетевых параметров требуется перезагрузка устройства.

ВНИМАНИЕ!
Если обновление IP-адреса для Вашего доменного имени не будет [illegible]иться в те[illegible] 35 дней, это доменное имя будет освобождено!

Шаг 8: настройка IP-камеры для работы с сервисом [illegible]ершена.

Рассмотрим пример настройки DDNS для марш[illegible]атор[illegible] примере Planet XRT-412. Оборудование других марок настраивается ана[illegible]о, в со[illegible] инструкцией по эксплуатации к применяемому оборудованию. Ч[illegible]ро[illegible]аршрутизатор для работы с сервисом DynDNS выполните следующие действия[illegible]

ВНИМАНИЕ!
Маршрутизатор должен поддерживать функци[illegible]ты с [illegible]ен быть подключен к сети Интернет и иметь соответствующие сетевые настр[illegible]

Шаг 1: введите в адре[illegible] бр[illegible] IP-адрес маршрутизатора. В появившемся окне запроса введите логин и п[illegible]ль. По[illegible]е удачной авторизации откроется основная страница настроек м[illegible]утизатора. Вы[illegible]ите пункт **[General Setup]** (*Рис. 7.25*).

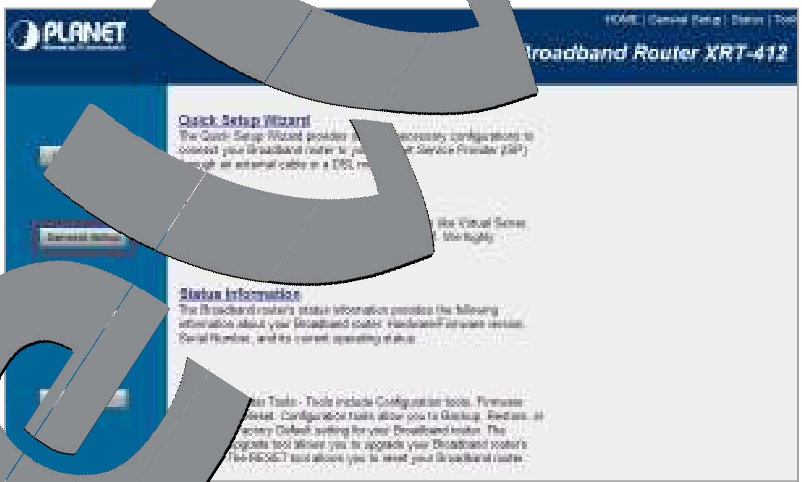


Рис. 7.25

[illegible]2: в появившемся меню выберите пункт **[DDNS]**. Активизируйте DDNS-клиент, [illegible]вив[illegible]nable]**.

[illegible]: в [illegible]етствии с данными, полученными при регистрации на сервисе DynDNS [illegible]7.4.2, 7[illegible] данного Руководства), в поле **[Provider]** выберите www.dyndns.org, в поле [illegible]me]** необходимо указать camera184.dyndns.org, в поля **[Account]** и **[Passwor[illegible]**[illegible]дите соответственно camera184 и 123456. (*Рис. 7.26*).

Рис. 7.26

ВНИМАНИЕ!
Будьте внимательны: при некорректном заполнении маршрутиз[illegible]ожет подключиться к серверу DDNS.

Шаг 4: для сохранения изменений на[illegible] **Apply**[illegible]

Шаг 5: настройка маршрутизатора для р[illegible]с[illegible]исом DynDNS завершена.

Если все настройки выполн[illegible]рно, [illegible]рь Ваш собственный ресурс сети открыт для доступа из любой точки [illegible]а по[illegible]м уникальным именем, понятным и удобным для запоминания.

Теперь для обраще[illegible] камере до[illegible]аточно в браузере ввести запрос http://camera184.dyndns.org, и[illegible]ройки в[illegible]олнены корректно, то Вы попадете на главную страницу камеры.

Приложения

Приложение A. Значения используемых портов

Назначение порта	Значение по умолчанию	[illegible]азон зн[illegible]
HTTP	80	[illegible]24..65534
Переадресация HTTP с помощью UPnP	80	[illegible]
Переадресация HTTPS с помощью UPnP	443	1124..655[illegible]4
RTSP	554	[illegible]..65534
Переадресация RTSP с помощью UPnP	554	1124..65534
Начальный порт диапазона RTP	[illegible]	1124..65435
Конечный порт диапазона RTP	799[illegible]	1223..65534
Порт видео для Мультикаст	[illegible]	1124..65534
Порт аудио для Мультикаст	-	1124..65534
SMTP	25	1..65535
Порт удаленного сервера журнала событий	[illegible]	1124..65534
Порт сервера соб[illegible]	[illegible]	1..65535
Порт прокси	[illegible]	1..65535
Детектор дв[illegible]	[illegible]999	-
Поток MP[illegible]	80	1124..65534
Поток M[illegible] (HT[illegible]	80	1124..65534

Приложение В. Заводские установки

Ниже приведены некоторые значения заводских установок

Наименование	Зна[illegible]е
IP-адрес	19[illegible]0.99
Маска подсети	255.2[illegible]
Шлюз	192.168.0.[illegible]
Имя пользователя (администратора)	[illegible]in
Пароль (администратора)	[illegible]n
HTTP-порт	[illegible]
RTSP-порт	5[illegible]4
SMTP-порт	[illegible]

Приложение C. Общие сведения о безопасности беспроводных соединений

Для предотвращения несанкционированного доступа к бесп[illegible]ению необходимо особое внимание к вопросам безопасности.

Беспроводная точка доступа поддерживает несколько ви[illegible]ты Wi-F[illegible]ти с использованием различных методов и алгоритмов шифрования и ид[illegible]ци[illegible]WEP, 802.1x, 802.1x с WEP, WPA-PSK, WPA-AES и WPA RADIUS).

Использование того или иного вида шифрования [illegible]ительно снизить риск перехвата информации и несанкционированного подк[illegible]ния к Ва[illegible]водной сети. Наиболее простой и одновременно наименее защи[illegible]ото[illegible]ования это WEP с длиной ключа 64 бит. Его следует использовать только [illegible]ае, если подключаемое оборудование не поддерживает других алгоритмов шифровани[illegible]

Протоколы защиты WEP (Wired Eq[illegible]), WPA и WPA2 обеспечивают единую инфраструктуру для управления [illegible]и шифрования данных, пересылаемых между беспроводной точкой до[illegible]и б[illegible]ным клиентом. Для защиты подключения на точке доступа необх[illegible] активи[illegible]ть WEP или WPA.

В основе протокола WPA, [illegible]ишел[illegible]ену WEP, лежит подмножество стандарта IEEE 802.11i, а WPA2 основан [illegible]конча[illegible]льной редакции стандарта IEEE 802.11i. В WPA применяется н[illegible]лько способов [illegible]алгоритмов, в частности TKIP (Temporal Key Integrity Protocol) и AES[illegible] Encryption [illegible]tandard) для повышения надежности методов управления ключами и [illegible]инство современных беспроводных устройств совместимы [illegible]WPA.

WEP и WPA ш[illegible]анные, перес[illegible]аемые между Точкой доступа и удаленными клиентами. То есть, клю[illegible]естный как беспроводной Точке доступа, так и клиенту, испол[illegible] для шиф[illegible] восстановления данных, пересылаемых между этими устрой[illegible]мщик, завладевший ключом, может расшифровать данные, пересылаем[illegible]межд[illegible]еспр[illegible]одными AP и клиентом или установить соединение с беспроводн[illegible]чк[illegible]оступ[illegible]

Суще[illegible]ок WEP – это необходимость вручную вводить ключ, используемый [illegible]ия, как на беспроводной точке, так и на клиенте.

[illegible]странения недостатков WEP-шифрования протокол WPA дополнен функциями [illegible]влен[illegible] Как и в WEP, ключ здесь используется для шифрования данных. [illegible]ко[illegible]ввод[illegible] один раз, а впоследствии с помощью этого ключа WPA генерирует [illegible]клю[illegible] шифрования данных. WPA периодически меняет ключ. Следовательно, в слу[illegible] ключа шифрования, тот будет полезен только до тех пор, пока беспроводн[illegible]очка доступа и клиент автоматически не изменят его.

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

Для настройки использования режима WPA-PSK нужно выбра[illegible]A Pre-Shared Key. В точке доступа реализованы три алгоритма WPA: T[illegible]ES и сов[illegible]ный. TKIP - это устаревший протокол, предназначенный для[illegible]чтобы у[illegible]нить многочисленные проблемы WEP до широкого распространения п[illegible]сп[illegible]щего поколения WPA (WPA2). В TKIP используется тот же алгорит[illegible]ования, [illegible]WEP, но многие изъяны WEP устранены благодаря динамической [illegible] шифрования данных, шифрованию данных настройки, представленных об[illegible]м текс[illegible] в [illegible], и проверке целостности сообщений. AES - это новый, исключит[illegible]ежн[illegible]м шифрования, базируемый на стандарте 802.11i и WPA2. Однако [illegible] не реализован во всех аппаратных средствах и программном обеспечении. По возмож[illegible]дует выбирать AES.

После выбора режима работы вводит[illegible]PA Shared K[illegible]. Необходимо ввести один и тот же ключ на всех клиентах, к[illegible]связь с точкой доступа. Следует выбирать длинный, трудно разга[illegible]мый [illegible] длина ключа не менее 8 символов, но не более 63 символо[illegible]SCII. [illegible]емая длина ключа не более 20 символов.

ПРИМЕЧАНИЕ!
Не рекомендуется вводить кл[illegible]больше 20 AS[illegible] символов, так как длинный ключ может существенно замедлить работу бе[illegible]

Если клиенты [illegible]стимы с WPA, [illegible]чше использовать WEP, чем вовсе отказаться от защиты. Для настр[illegible]ать режим безопасности Shared Key (Меню Advanced Setting), выбрать [illegible]зования в качестве стандартного ключа передачи (клю[illegible]т 1 до 4) и длину WEP ключа (64 или 128) с представлением в шестнадцате[illegible]м [illegible]ASCII-формате. Ключ следует ввести в поле Key, которое соответств[illegible]ыбр[illegible]му с[illegible]ртному ключу передачи. Например, если выбран 64-х разрядный [illegible]дцатери[illegible]люч, то можно ввести строку из десяти шестнадцатеричных цифр. Эту к[illegible]P-ключа необходимо повторить во всех клиентах, поэтому сле[illegible]бирать [illegible]настройки, приемлемый для всех устройств.

[illegible]ИМЕ[illegible]
[illegible]ду[illegible] наст[illegible] WEP-шифрования может различаться для различного оборудования в [illegible]тепе[illegible]ем настройка WPA, поэтому рекомендации по WEP труднее адаптировать к конкре[illegible]ии.

Приложение D. Гарантийные обязательства

D1. Общие сведения

а) Перед подключением оборудования необходимо ознакоми[illegible]ом по эксплуатации.

б) Условия эксплуатации всего оборудования должны со[illegible]ать ГОС[illegible]150-69, ГОСТ В20.39.304-76 (в зависимости от исполнения устройства).

в) Для повышения надежности работы оборудования [illegible] от бро[illegible]тающей сети и обеспечения бесперебойного питания следует [illegible] сетевые фильтры и устройства бесперебойного питания.

D2. Электромагнитная совместимость

Это оборудование соответствует требованиям электро[illegible] совместимости EN 55022, EN 50082-1. Напряжение радиопо[illegible]мых аппа[illegible]турой, соответствует ГОСТ 30428-96.

D3. Электропитание

Должно соответствовать пар[illegible]казан[illegible]Руководстве по эксплуатации для конкретного устройства. Для устройств [illegible]строе[illegible]ым источником питания – это переменное напряжение 220 [illegible]±10%, частото[illegible]0 Гц ±3%. Для устройств с внешним адаптером питания – стаби[illegible]й источни[illegible]итания 5 В ±5% или 12 В ±10% для устройств с 12-вольтовым питани[illegible]аций – не более 0.1 В.

D4. Заземлен[illegible]

Все устройства, и[illegible]лок питания, должны быть заземлены путем подключения к [illegible]альным [illegible]электропитания с заземлением или путем непосредстве[illegible]ния корпуса, если на нем предусмотрены специальные крепежные [illegible]енты[illegible]емл[illegible]ние электропроводки здания должно быть выполнено в соответстви[illegible]ниям[illegible] (Правила Устройства Электроустановок). Оборудование с выносны[illegible] и адаптерами также должно быть заземлено, если это предусмотрено[illegible]корпуса или вилки на шнуре питания. Монтаж воздушных ли[illegible]тропередачи и линий, прокладываемых по наружным стенам зданий и на [illegible]ках[illegible]ть выполнен экранированным кабелем (или в металлорукаве), и линии [illegible]ены с двух концов. Причем, если один конец экрана подключается [illegible]ственн[illegible]шине заземления, то второй – подключается к заземлению через разр[illegible]

D5. Молниезащита

Молниезащита должна соответствовать РД 34.21.122-87 "Инстру[illegible] устройству молниезащиты зданий и сооружений" и ГОСТ Р 50571.18-2000, ГОСТ [illegible] ГОСТ Р 50571.20-2000. При прокладке воздушных линий и линий, ид[illegible] по наруж[illegible]тене зданий и по чердачным помещениям, на входах оборудования [illegible]быть уста[illegible]ены устройства молниезащиты.

D6. Температура и влажность

Максимальные и минимальные значения темп[illegible]ры экс[illegible]та[illegible]и хранения, а также влажности, Вы можете посмотреть в [illegible]ском[illegible]ми конкретного оборудования. Максимальная рабочая температура – э[illegible]ратура, выше которой не должен нагреваться корпус устройства в процессе длительной [illegible]

D7. Размещение

Для вентиляции устройства необходи[illegible]авит[illegible]нимум по 5 см свободного пространства по бокам и со стор[illegible] задн[illegible]е[illegible] устройства. При установке в телекоммуникационный шкаф и[illegible] до[illegible]быть обеспечена необходимая вентиляция. Для этого рекомендуется у[illegible]авли[illegible]ь в шкафу специальный блок вентиляторов. Температура о[illegible]ужающего возд[illegible] и вентиляция должны обеспечивать необходимый температурн[illegible] оборудова[illegible]я (в соответствии с техническими характеристиками конкретного об[illegible]

Место для разме[illegible]ения оборудования должно отвечать следующим требованиям:

а) Отсутствие [illegible]ости помеще[illegible].

б) Отсутствие в в[illegible]ессивных сред.

в) В помещ[illegible] где у[illegible]ся оборудование, не должно быть бытовых насекомых.

г) За[illegible]ется [illegible]мещать на оборудовании посторонние предметы и перекрывать вентиляцио[illegible]отв[illegible]ия.

D8. Об[illegible]

[illegible]удование необходимо обслуживать с периодичностью не менее одного раза в [illegible] це[illegible]ия из него пыли. Это позволит оборудованию работать без сбоев в [illegible]ение [illegible]дол[illegible]ьного времени.

[illegible]чение интерфейсов

Обо[illegible]вание должно подключаться в строгом соответствии с назначением и типом установленных интерфейсов.

D10. Гарантийные обязательства

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

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

а) несоблюдения правил транспортировки и условий хранения;

б) форс-мажорных обстоятельств (таких как пожар, наводнение, землетрясение и др.);

в) нарушения технических требований по размещению, подключению и эксплуатации;

г) неправильных действий при перепрошивке;

д) использования не по назначению;

е) механических, термических, химических и иных видов воздействий, если их параметры выходят за рамки допустимых эксплуатационных характеристик, либо не предусмотрены технической спецификацией на данное оборудование;

ж) воздействия высокого напряжения (удар молнии, статическое электричество и т.п.).

Приложение Е. Права и поддержка

Е1. Торговая марка

Некоторые пункты настоящего Руководства, а также ра[illegible]ы меню у[illegible]ения оборудования могут быть изменены без предварительного уведо[illegible]

BEWARD является зарегистрированной торговой маркой ООО [illegible]ва[illegible]. Все остальные торговые марки принадлежат их владельцам.

Е2. Ограничение ответственности

ООО «НПП «Бевард» не гарантирует, что[illegible]ые [illegible]будут работать должным образом во всех средах и приложениях, и не[illegible]антий и представлений, подразумеваемых или выраженных относительно качества, [illegible]характеристик, или работоспособности при использовании в [illegible]х целях. ООО «НПП «Бевард» приложило все усилия, чтобы сделать это Р[illegible]ации наиболее точным и полным. ООО «НПП «Бевард» отказывается [illegible]вет[illegible]ти за любые опечатки или пропуски, которые, возможно, произо[illegible]при на[illegible]данного Руководства.

Информация в любой части[illegible]а по [illegible]тации изменяется и дополняется ООО «НПП «Бевард» без предварительно[illegible]омле[illegible]я. ООО «НПП «Бевард» не берет на себя никакой ответственно[illegible]а любые погре[illegible]ости, которые могут содержаться в этом Руководстве. ООО «НПП «Б[illegible]ерет на се[illegible]ответственности и не дает гарантий в выпуске обновлений или сохра[illegible]кой-либо информации в настоящем Руководстве по экспл[illegible]тации, и оставляет за собой право вносить изменения в данное Руководство и/или [illegible] описанные [illegible]нем, в любое время без предварительного уведомления. Если Вы [illegible]ководстве информацию, которая является неправильной или[illegible]олной, [illegible] в заблуждение, мы будем Вам крайне признательны[illegible]ентарии и предложения.

Е3. [illegible]пр[illegible]ения [illegible]

Это [illegible]ание [illegible]ротестировано и признано удовлетворяющим требованиям положения о[illegible]ройствах, принадлежащих к классу А, части 15 Правил Фе[illegible]й комиссии по связи (FCC). Эти ограничения были разработаны в целях [illegible]ече[illegible]ы от вредных помех, которые могут возникать при использовании [illegible]уд[illegible]я [illegible]ерческих целях. Это оборудование может излучать, генерировать и [illegible]ать [illegible]ию в радиочастотном диапазоне. Если данное оборудование будет уста[illegible] будет использоваться с отклонениями от настоящего Руководства, оно может ока[illegible]ь вредное воздействие на качество радиосвязи, а при установке в жилой зоне, возможно, – на здоровье людей. В этом случае владелец будет обязан исправлять последствия вредного воздействия за свой счет.

E4. Предупреждение CE

Это устройство может вызывать радиопомехи во внешне[illegible]ии. В это[illegible]чае пользователь может быть обязан принять соответствующие меры.

E5. Поддержка

Для информации относительно сервиса и п[illegible]жки, п[illegible] свяжитесь с сервисным центром ООО «НПП «Бевард». Контакт[illegible]ые В[illegible] найти на сайте http://www.beward.ru/.

Перед обращением в службу технической поддерж[illegible]уйста, подготовьте следующую информацию:

- Точное наименование и IP-адре[illegible] (в случае приобретения IP-оборудования), дата покупки.
- Сообщения об ошибках, ко[illegible]е появл[illegible] с [illegible]омента возникновения проблемы.
- Версия прошивки и че[illegible] обор[illegible]е работало устройство, когда возникла проблема.
- Произведенные Ва[illegible]ействия (по ша[illegible]), предпринятые для самостоятельного решения проблем[illegible]
- Скриншоты настроек и п[illegible]ия.

Чем полнее бу[illegible]т представленная Вами информация, тем быстрее специалисты сервисного центра с[illegible]ь Вам реши[illegible] проблему.

Приложение F. Глоссарий

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

ActiveX – это стандарт, который разрешает компонентам программного обеспечения взаимодействовать в сетевой среде независимо от языка, используемого для их создания. Веб-браузеры могут управлять элементами управления ActiveX, документами ActiveX и сценариями ActiveX. Элементы управления ActiveX загружаются и инсталлируются автоматически, как запрашиваемые. [illegible] 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, преобразующая аналоговые сигналы, передаваемые посредством стандартной телефонной линии, в цифровые сигналы (пакеты данных), позволяя во время работы [illegible]ть зво[illegible].

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

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

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

Authentication / Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. О[illegible] способов аутентификации в компьютерной системе состоит во вводе Ваш[illegible]ьского идентификатора, в просторечии называемого «логином» (login [illegible]егистраци[illegible] имя пользователя) и пароля — некой конфиденциальной инф[illegible] знание [illegible]рой обеспечивает владение определенным ресурсом. Получив введенный[illegible]тел[illegible]логин и пароль, компьютер сравнивает их со значением, которое[illegible]тся в с[illegible]ой базе данных, и, в случае совпадения, пропускает пользовател[illegible]

Auto Iris / АРД (Авторегулируемая д[illegible]агма) [illegible]оматическое регулирование величины диафрагмы для контрол[illegible]тва[illegible] попадающего на матрицу. Существует два варианта автоматической регул[illegible]афрагмы: Direct Drive и Video Drive.

Biterate / Битрейт (Скорость перед[illegible] [illegible]льно, скорость прохождения битов информации. Битрейт принято испол[illegible] при[illegible]ии эффективной скорости передачи информации по каналу, то есть с[illegible]едачи «полезной информации» (помимо таковой, по каналу может п[illegible]ться с[illegible]ая информация).

BLC (Back Light Compensation / К[illegible]саци[illegible]фоновой засветки, компенсация заднего света). Типичный пр[illegible]ер необходимос[illegible] использования: человек на фоне окна. Электронный затвор камеры [illegible]ает интегра[illegible]ную, т.е. общую освещенность сцены, «видимой» камерой через объек[illegible] малая фигура человека на большом светлом фоне окна выл[illegible]ется в итоге "засве[illegible] картинки. Включение функции «BLC» может в подобных сл[illegible]править работ[illegible]втоматики камеры.

Bonjour – протоко[illegible]аружения сервисов (служб), используемый в операционной си[illegible]ac OS X, [illegible] с версии 10.2. Служба Bonjour предназначается для использо[illegible]ных сетях и использует сведения (записи) в службе доменных имён (DNS)[illegible] обн[illegible]ения других компьютеров, равно как и иных сетевых устройств (например, [illegible]ер[illegible] бли[illegible]ем сетевом окружении.

CIDR [illegible]дресация (англ. *Classless Inter-Domain Routing*, англ. *CIDR*) – мет[illegible]пресац[illegible]яющий гибко управлять пространством IP-адресов, не используя ж[illegible]ассовой адресации. Использование этого метода позволяет экономно [illegible]льзо[illegible]енный ресурс IP-адресов, поскольку возможно применение различных [illegible]подсетей [illegible]личным подсетям.

[illegible]**матрица** – это светочувствительный элемент, использующийся во многих цифровых[illegible]рах и представляющий собой крупную интегральную схему, состоящую из сотен тысяч зарядов (пикселей), которые преобразуют световую энергию в электронные сигналы. Размер матрицы изменяется по диагонали и может составлять 1/4", 1/3", 1/2" или 2/3".

CGI (Единый шлюзовый интерфейс) – специфи[illegible]ющая взаимодействие web-сервера с другими CGI-программами. Н[illegible]ер, HTML-[illegible]ица, содержащая форму, может использовать CGI-программу для обра[illegible]ых фор[illegible]

CMOS / КМОП (Complementary Metal Oxide Semiconductor / К[illegible]тарный металлооксидный полупроводник) – это широко ис[illegible] тип полу[illegible]водника, который использует как отрицательную, так и по[illegible]тельну[illegible]лектрическую цепь. Поскольку только одна из этих типов цепей может бы[illegible]ючена в [illegible]ное время, то микросхемы КМОПа потребляют меньше электроэнер[illegible] микр[illegible]емы, использующие только один тип транзистора. Также датчики изображения К[illegible]которых микросхемах содержат схемы обработки, однако это пре[illegible]щество невозмо[illegible]спользовать с ПЗС-датчиками, которые являются также более [illegible]стве.

DDNS (Dynamic Domain Name Syste[illegible]nDN[illegible] [illegible]нология, применяемая для назначения постоянного доменного и[illegible]и устро[illegible](ко[illegible]пьютеру, сетевому накопителю) с динамическим IP-адресом. Это мо[illegible]P-адр[illegible]ученный по DHCP или по IPCP в PPP-соединениях (например, при удален[illegible]оступ[illegible]ерез модем). Другие машины в Интернете могут устанавливат[illegible]оединение с это[illegible]ашиной по доменному имени.

DHCP (Dynamic H[illegible]ration P[illegible]tocol / Протокол динамической конфигурации узла) – это сетев[illegible]яющий компьютерам автоматически получать IP-адрес и д[illegible]ие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает [illegible]и «клиент-[illegible]вер». Для автоматической конфигурации компьютер-клиент на [illegible] сетевого устройства обращается к так называемому сер[illegible]ICP и полу[illegible]его нужные параметры.

DHCP[illegible] [illegible] программа, которая назначает клиентам IP-адреса внутри заданного [illegible]зона[illegible] опре[illegible]енный период времени. Данную функцию поддерживают практически [illegible]вр[illegible]енны[illegible]шрутизаторы.

Digital [illegible]ое увеличение – это увеличение размера кадра не за счет опт[illegible]помощью [illegible]дрирования полученного с матрицы изображения. Камера ничего не [illegible]чив[illegible]олько вырезает нужную часть изображения и растягивает ее до [illegible]вона[illegible]ешения.

[illegible]main [illegible]er / Сервер доменных имен – также домены могут быть использованы органи[illegible]которые хотят централизованно управлять своими компьютерами (на которых ус[illegible]влены 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 [illegible] который аутентифицирует пользователей в сети.

Ethernet – пакетная технология передачи данных преим[illegible]твенно в л[illegible]ных компьютерных сетях. Стандарты Ethernet определяют пр[illegible] соеди[illegible] и электрические сигналы на физическом уровне, формат кадров и пр[illegible]ра[illegible]ления доступом к среде – на канальном уровне модели OSI.

Factory default settings / Заводские установ[illegible] умо[illegible]ию [illegible] это установки, которые изначально использованы для устройства, ко[illegible]о отгру[illegible]вода в первый раз. Если возникнет необходимость переустановить ус[illegible]ло[illegible]заводских установок по умолчанию, то эта функция применима для большинст[illegible]тв, и она полностью переустанавливает любые установки, которые [illegible] изменены по[illegible]телем.

Firewall / Брандмауэр – брандмауэ[illegible]ботает как барьер между сетями, например, между локальной сетью [illegible]ерн[illegible]ндмауэр гарантирует, что только зарегистрированным пользова[illegible]ям буд[illegible]е[illegible]ен доступ из одной сети в другую сеть. Брандмауэром может быть п[illegible]е об[illegible]ие, работающее на компьютере, или брандмауэром может быть автономное [illegible]атное [illegible]ройство.

Focal length / Фокус[illegible] расстояние [illegible]змеряемое в миллиметрах фокусное расстояние объектива камер[illegible]щее шир[illegible] горизонтальной зоны обзора, которое в свою очередь измеряется в граду[illegible] как расстояние от передней главной точки до переднего ф[illegible]са (для передн[illegible] фокусного расстояния) и как расстояние от задней главной точк[illegible] фокуса (дл[illegible]аднего фокусного расстояния). При этом, под главными точками под[illegible]пересечения передней (задней) главной плоскости с опти[illegible]сью.

Fps / [illegible]ва[illegible]ота – количество кадров, которое видеосистема (компьютерная игра, телев[illegible]DVD[illegible]ер, в[illegible]файл) выдаёт в секунду.

Fram[illegible]др – [illegible] является полное видеоизображение. В формате 2:1 чересстрочно[illegible]интерфейса RS-170 и в форматах Международного кон[illegible]вного ко[illegible]та по радиовещанию, кадр создается из двух отдельных областей [illegible]ч[illegible]й развѐртки 262.5 или 312.5 на частоте 60 или 50 Гц для того, чтобы [illegible]рми[illegible]в[illegible]й кадр, который отобразится на экране на частоте 30 или 25 Гц. В [illegible]мерах [illegible]огрессивной разверткой каждый кадр сканируется построчно и не явл[illegible]очным; большинство из них отображается на частоте 30 и 25 Гц.

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

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

G.711 – стандарт для представления 8-битной компрессии PCM (ИКМ) сигнала с частотой дискретизации 8000 кадров/секу[illegible]. Таким образом, G.711 кодек создаёт поток 64 Кбит/с.

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

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

H.264 – это международный стандарт кодирования аудио и видео, (другое название 'MPEG-4 ра[illegible] или AVC (Advanced Video Coding)). Данный стандарт содержит ряд новых возможностей, [illegible] значительно повысить эффективность сжатия видео по сравнению с более ранними стандартами (MPEG-1, MPEG-2 и MPEG-4), обеспечивая также б[illegible]кость применения в разнообразных сетевых средах. Используется в цифровом телевидении высокого разрешения (HDTV) и во многих других областях цифрового видео.

HTTP (Hypertext Transfer Protocol / Протокол передачи гипертекста) – это набор правил [illegible]у файлами (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 / Защищённы[illegible]дачи гипертекста) – расширение протокола HTTP, поддерживающ[illegible]ифрование. [illegible]ные, передаваемые по протоколу HTTP, «упаковываются» в криптогр[illegible]й прото[illegible]SSL или TLS, тем самым обеспечивается защита этих данных. В отличие от [illegible] HT[illegible]PS по умолчанию используется TCP-порт 443.

Hub / Сетевой концентратор - сетевой концентр[illegible] испол[illegible]тся для подключения многочисленных устройств к сети. Сетевой концентра[illegible]редает[illegible]в устройства, подключенные к нему, тогда как коммутатор только пе[illegible]нь[illegible]устройство, которое специально предназначено для него.

ICMP (Internet Control Message Pro[illegible]сетевой п[illegible]токол управляющих сообщений) – сетевой протокол, входящи[illegible]TCP/IP. В основном ICMP используется для передачи сообщений об о[illegible]х и[illegible]сключительных ситуациях, возникших при передаче данных, напр[illegible]ер, запр[illegible]е[illegible]я услуга недоступна или хост или маршрутизатор не отвечают.

IEEE 802.11 / Стандарт IEEE 802.11 – [illegible] семе[illegible]тво стандартов для беспроводных локальных сетей. Стандарт [illegible]1 поддерживае[illegible]ередачу данных на скорости 1 или 2 Мбит/сек на полосе 2.4 ГГц[illegible] 802.11[illegible]адает скорость передачи данных 11 Мбит/сек на полосе 2.4 ГГц, в то в[illegible]02.11a позволяет задать скорость до 54 Мбит/сек. на полосе[illegible]ГГц.

Interlaced vide[illegible]рочная р[illegible]звертка – это видеозапись со скоростью 50 изображений (называемых [illegible] которых каждые 2 последовательных поля (полукадра) за[illegible]няются в 1 кадр. Чересстрочная развертка была разработана много лет на[illegible]ового телевидения и до сих пор широко применяется. Она дает хорошие р[illegible]тать[illegible] про[illegible]тре движения в стандартном изображении, хотя всегда существует[illegible]ро[illegible]искаж[illegible]изображения.

Interne[illegible] серия браузеров, разрабатываемая корпорацией Microsoft с 19[illegible]ходит в [illegible]лект операционных систем семейства Windows. Является наиболее [illegible]ым веб-браузером.

I[illegible] (Ing[illegible] Protection) – это стандарт защиты оборудования, который описывает [illegible]влаго[illegible]щиту камеры видеонаблюдения. Первая цифра обозначает уровень защи[illegible]ания твёрдых частиц (например, цифра 6 обозначает полное исключение попадания [illegible]и). 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 котор[illegible]дача видеопотока в цифровом формате по сети Ethernet, использующей [illegible]окол IP.

JPEG (Joint Photographic Experts Group / Стандарт [illegible]ной [illegible]ппы экспертов в области фотографии) – один из популярн[illegible] графи[illegible]орматов, применяемый для хранения фотоизображений и подобн[illegible]жений. [illegible] создании изображения JPEG имеется возможность настройки ис[illegible]зуемо[illegible]эфф[illegible]циента сжатия. Так как при более низком коэффициенте сжат[illegible]е. са[illegible]ом качестве) увеличивается объем файла, существует выбор межд[illegible]м [illegible]ражения и объемом файла.

Kbit/s (Kilobits per second / Кбит/сек) [illegible] измерения [illegible]рости потока данных, т.е. это скорость, на которой определенное [illegible]дят заданную точку.

LAN (Local Area Network / Локальная [illegible]ли[illegible]ная сеть) – компьютерная сеть, покрывающая обычно относительно [illegible]льшую [illegible]рию или небольшую группу зданий (дом, офис, фирму, институт), то ес[illegible]нную [illegible]фическую зону.

Lux / Люкс – единица измерения осве[illegible]ности. Определяется как освещенность поверхности площадью 1 кв.[illegible]вым потоком [illegible]люмен. Используется для обозначения чувствительности камер.

MAC-адрес (Media Access Contro[illegible] Аппаратный адрес устройства) – это уникальный идентиф[illegible]рисоединенно[illegible]к сети устройства или, точнее, его интерфейс для подключения к сети[illegible]

Mbit/s (Me[illegible]per seco[illegible]/сек) – это мера измерения скорости потока данных, т.е. э[illegible] которой биты проходят заданную точку. Этот параметр обычно используетс[illegible]обы [illegible]дста[illegible]ть «скорость» сети. Локальная сеть должна работать на скорости 1[illegible]00 [illegible]т/се[illegible]

MJPE[illegible] – покадровый метод видеосжатия, основной особенностью кото[illegible]вляет[illegible]каждого отдельного кадра видеопотока с помощью алгоритма с[illegible]бражений JPEG. При сжатии методом MJPEG межкадровая разница не [illegible]ыва[illegible]

[illegible]PEG-4 – [illegible]международный стандарт, используемый преимущественно для сжатия циф[illegible] и видео. Стандарт MPEG-4 в основном используется для вещания (потоково[illegible]о), записи фильмов на компакт-диски, видеотелефонии (видеотелефон) и широковещания, в которых активно используется сжатие цифровых видео и звука.

Multicast / Групповая передача – специальная форма широковещания, при которой копии пакетов направляются определённому подмножеству адре[illegible] Наряду с приложениями, устанавливающими связь между источником и [illegible]телем, существуют такие приложения, где требуется, чтобы источник по[illegible] информа[illegible]разу группе получателей. При традиционной технологии IP-адре[illegible]ебуется [illegible]ому получателю информации послать свой пакет данных, то есть одна [illegible]ация передается много раз. Технология групповой адресации пре[illegible]ет собой [illegible]ение IP-адресации, позволяющее направить одну копию пакета с[illegible]учателям. [illegible]ножество получателей определяется принадлежностью каждого [illegible]х к кон[illegible]ой [illegible]ппе. Рассылку для конкретной группы получают только члены этой [illegible]

Технология IP Multicast предоставляет ряд сущест[illegible]еимуществ по сравнению с традиционным подходом. Например, добавление новых поль[illegible] не влечет за собой необходимое увеличение пропускной способ[illegible] Значительн[illegible] сокращается нагрузка на посылающий сервер, который бо[illegible]ддерживать множество двухсторонних соединений.

Для реализации групповой а[illegible]ции в [illegible]ной сети необходимы: поддержка групповой адресации стеком прото[illegible]P, пр[illegible]ная поддержка протокола IGMP для отправки запроса о присоединении к груп[illegible]получ[illegible]ии группового трафика, поддержка групповой адресации сетевой [illegible]той, приложен[illegible] использующее групповую адресацию, например, видеоконференци[illegible] «мульти[illegible]ст» использует адреса с 224.0.0.0 до 239.255.255.255. Поддерживается [illegible]намическая адресация. Примером статических адресов [illegible]яются 224.0.0.1 [illegible] адрес группы, включающей в себя все узлы локальной сети, 224[illegible]е маршрути[illegible]торы локальной сети. Диапазон адресов с 224.0.0.0 по 224.0.0.25[illegible]я протоколов маршрутизации и других низкоуровневых [illegible]олов поддержки групповой адресации. Остальные адреса динамически[illegible]я приложениями. На сегодняшний день большинство маршрутиза[illegible] под[illegible]ива[illegible] эту опцию (в меню обычно есть опция, разрешающая IGMP протокол и[illegible]т).

NTP [illegible] **otocol / Протокол синхронизации времени)** – сетевой прот[illegible]ля си[illegible]и времени с использованием сетей. NTP использует для своей р[illegible]UDP.

N[illegible]l Television System Committee / Стандарт NTSC) – стандарт NTSC [illegible] телеви[illegible]ным и видеостандартом в США. Стандарт NTSC доставляет 525 строк в кадр[illegible]

ONVIF (Open Network Video Interface Forum) – отраслевой стандарт, определяющий протоколы взаимодействия таких устройств, как IP-камеры, видеорегист[illegible] и системы управления видео. Международный форум, создавший данны[illegible]нован компаниями Axis Communications, Bosch Security Systems и So[illegible] 2008 году [illegible]лью разработки и распространения открытого стандарта для систем [illegible]идеонабл[illegible]ия.

PAL (Phase Alternating Line / Телевизионный стандарт PA[illegible] [illegible]онный стандарт PAL является преобладающим телевизионным [illegible]м в стр[illegible] Европы. Телевизионный стандарт PAL доставляет 625 строк в ка[illegible]

PoE (Power over Ethernet / Питание через [illegible]et) – т[illegible] позволяющая передавать удалённому устройству вместе с данн[illegible]ую энергию через стандартную витую пару в сети Ethernet.

Port / Порт – идентифицируемый [illegible] системны[illegible]ресурс, выделяемый приложению, выполняемому на некоторо[illegible] связи с приложениями, выполняемыми на других сетевых хостах (в т[illegible]пе [illegible] приложениями на этом же хосте). В обычной клиент-серверной [illegible]дели пр[illegible]ни[illegible] либо ожидает входящих данных или запроса на соединение («сл[illegible]т»), [illegible]осылает данные или запрос на соединение на известный порт, открытый пр[illegible]ением [illegible]рвером.

PPP (Протокол дв[illegible]чечного сое[illegible]ения) – протокол, позволяющий использовать интерфейс по[illegible]ой пере[illegible]и для связи между двумя сетевыми устройствами. Например, подключе[illegible]средством телефонной линии.

PPPoE (Point-t[illegible]int Protocol / Пр[illegible]окол соединения «точка - точка») – протокол для подключения [illegible]ой сети [illegible]тандарта Ethernet к Интернету через широкополосное соединени[illegible]SL, беспроводное устройство или кабельный модем. С помо[illegible] и широкополосного модема пользователи локальной сети могут получать до[illegible]дуальной проверкой подлинности к высокоскоростным сетям данных. О[illegible]няя [illegible]ernet [illegible]протокол PPP (Point-to-Point Protocol), протокол PPPoE обеспечива[illegible]вный [illegible]б создания отдельных соединений с удаленным сервером для каждого [illegible]

[illegible]ressive [illegible] Прогрессивное сканирование – это технология представления [illegible]в [illegible]людении, при которой каждый кадр воспроизводится по одной линии в [illegible]ядке [illegible]ения каждую шестнадцатую долю секунды. То есть сначала [illegible]ется ли[illegible]1, затем 2, затем 3 и так далее. Таким образом, изображение не бьется на [illegible]укадры. В этом случае полностью исчезает эффект мерцания, поэтому качество [illegible]го видео получается более высоким.

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

Router / Маршрутизатор – это устройство, которое опред[illegible]йшей сети, в которую пакет данных должен быть направлен как в [illegible]окончатель[illegible]ункт назначения. Маршрутизатор создает и/или поддерживает [illegible]ьную [illegible]лицу маршрутизации, которая сохраняет информацию, как только она дост[illegible]енных пунктов назначения. Иногда маршрутизатор включен[illegible]стве ч[illegible]сетевого коммутатора.

RTP (Real-Time Transport Protocol / Транспо[illegible] прото[illegible]е реального времени) – это протокол IP для передачи данных (н[illegible]уд[illegible]и видео) в режиме реального времени. Протокол RTP переносит в своём загол[illegible]ые, необходимые для восстановления голоса или видеоизображен[illegible] приёмном узле[illegible]акже данные о типе кодирования информации (JPEG, MPEG и т[illegible]ного протокола, в частности, передаются временная метка и номер пакет[illegible]пара[illegible]воляют при минимальных задержках определить порядок и момент [illegible]ир[illegible]ния каждого пакета, а также интерполировать потерянные пакет[illegible]честве [illegible]ежащего протокола транспортного уровня, как правило, используется прот[illegible]

RTSP (Real Time Stre[illegible]ing Protocol / [illegible]отокол передачи потоков в режиме реального времени) – это п[illegible]равления, ко[illegible]рый служит основой для согласования транспортных протоколов, таких [illegible]ой или одноадресной передачи и для согласования используемых кодеков. RTS[illegible] рассматривать как пульт дистанционного управления потоками[illegible] предоставля[illegible]ыми сервером мультимедиа. Серверы RTSP обычно используют R[illegible]ртного протокола для передачи аудио- и видеоданных.

SD (Se[illegible]emory Card/ карта памяти типа SD) – формат карты флэш-памяти, ра[illegible]танн[illegible]для [illegible]пользования в основном в портативных устройствах. На сегодняшни[illegible]н[illegible]широк[illegible]пользуется в цифровых устройствах, например: в фотоаппара[illegible]елефонах, КПК, коммуникаторах и смартфонах, GPS-навиг[illegible]ах, ви[illegible]в некоторых игровых приставках.

[illegible]er / Электронный затвор – это элемент матрицы, который позволяет [illegible]лиро[illegible] накопления электрического заряда. Эта деталь отвечает за [illegible]ьность вы[illegible]ки и количество света, попавшего на матрицу перед формированием из[illegible]я.

SM[illegible]mple Mail Transfer Protocol / Простой протокол передачи почты) – протокол SMTP используется для отсылки и получения электронной почты. Однако поскольку он является «простым» по своей структуре, то он ограничен в своей возможности по вместимости сообщений на получающем конце, и он обычно испол[illegible] с одним из двух других протоколов, POP3 или протоколом интерактивного досту[illegible] почте (протокол IMAP). Эти протоколы позволяют пользователю сохраня[illegible]бщения [illegible]вом ящике сервера и периодически загружать их из сервера.

SSL/TSL (Secure Socket Layer / Transport Layer Security / Про[illegible]нных сокетов / Протокол транспортного уровня) – эти два пр[illegible]ротокол[illegible]вляется приемником протокола TSL) являются криптограф[illegible]токолами, которые обеспечивают безопасную связь в сети. В большинст[illegible]чаев пр[illegible]используется через протокол HTTP, чтобы сформировать прото[illegible]ён[illegible]дачи гипертекста (протокол HTTPS) в качестве использованного, например, [illegible]те для осуществления финансовых транзакций в электронном виде. Протокол SS[illegible]ьзует сертификаты открытого криптографического ключа, чтобы[illegible]ентичность сервера.

Subnet mask / Маска подсети – би[illegible] маск[illegible]еляющая, какая часть IP-адреса узла сети относится к адресу сети, а [illegible] – [illegible]дресу самого узла в этой сети. Например, узел с IP-адресом 192.16[illegible] маско[illegible]ети 255.255.255.0 находится в сети 192.168.0.0.

Switch / Коммутатор [illegible] коммутатором [illegible]вляется сетевое устройство, которое соединяет сегменты сети вм[illegible]рое выбира[illegible] маршрут для пересылки устройством данных к его ближайшему пол[illegible]мутатор является более простым и более быстрым механизмом, чем сетевой [illegible]изатор. Некоторые коммутаторы имеют функцию маршрутиза[illegible]

TCP (Transmissio[illegible]ротокол управления передачей) – один из основных сетев[illegible]колов [illegible], предназначенный для управления передачей данных в сет[illegible] TCP/IP. TCP - это транспортный механизм, предоставляющий поток данн[illegible]едв[illegible]ельн[illegible] установкой соединения, за счёт этого дающий уверенность в достовер[illegible] п[illegible]аемы[illegible]нных, осуществляет повторный запрос данных в случае потери дан[illegible]лирование при получении двух копий одного пакета (см. также T/TCP).

[illegible]**Ti[illegible] to live)** – предельный период времени или число итераций или переходов, [illegible]котор[illegible]нных (пакет) может существовать до своего исчезновения. Значение [illegible]ж[illegible] расс[illegible]ваться как верхняя граница времени существования IP-дейтаграммы в се[illegible] TTL [illegible]анавливается отправителем дейтаграммы и уменьшается каждым узлом (наприм[illegible]ршрутизатором) на пути его следования, в соответствии со временем пребывания [illegible] данном устройстве или согласно протоколу обработки. Если поле TTL становится равным нулю до того, как дейтаграмма прибудет в пункт назначения, то такая дейтаграмма отбрасывается и отправителю отсылается ICMP-паке[illegible]ом 11 – «Превышение временного интервала».

UDP (User Datagram Protocol / Протокол дейтаграм[illegible]льзовател[illegible] это протокол обмена данными с ограничениями на пересыла[illegible]нные [illegible]ети, использующей протокол IP. Протокол UDP является альтернатив[illegible]ол[illegible] TCP. Преимущество протокола UDP состоит в том, что для не[illegible]тельна [illegible]вка всех данных и некоторые пакеты могут быть пропущены, ес[illegible]в [illegible]ужена. Это особенно удобно при передаче видеоматериалов в режиме ре[illegible]го врем[illegible]ку не имеет смысла повторно передавать устаревшую инфор[illegible]то[illegible]равно не будет отображена.

UPnP (Universal Plug and Play) [illegible]технология, поз[illegible]щая персональным компьютерам и интеллектуальным сетевым[illegible] охранному оборудованию, развлекательным устройствам или инт[illegible]шлюз[illegible]диняться между собой автоматически и работать совместно через е[illegible]с[illegible] Платформа UPnP строится на основе таких интернет-стандарто[illegible] TCP/[illegible]TP и XML. Технология UPnP поддерживает сетевые инфраструктур[illegible]ческ[illegible]ого типа - как проводные, так и беспроводные. В их число, в частности, входят [illegible]бельный Ethernet, беспроводные сети Wi-Fi, сети на основе телефо[illegible]иний, линий [illegible]ктропитания и пр. Поддержка UPnP реализована в операционных с[illegible]

URL (Uniform Resource Locato[illegible]диный указатель ресурсов) – это стандартизированный[illegible] записи адреса[illegible]сурса в сети Интернет.

WAP (Wireless Ap[illegible]спроводной протокол передачи данных) – протокол, созда[illegible]пециально [illegible]GSM-сетей, где нужно устанавливать связь портативных [illegible]етью Интернет. С помощью WAP пользователь мобильного устройства [illegible] заг[illegible]ть из[illegible]ети Интернет любые цифровые данные.

Web[illegible]/[illegible]еб-се[illegible] – это сервер, принимающий HTTP-запросы от клиентов, обычно веб-[illegible]ющий им HTTP-ответы, обычно вместе с HTML-страницей, изоб[illegible]ием, ф[illegible]диа-потоком или другими данными.

W[illegible]ss Fidelity, дословно – «беспроводная точность») – торговая марка [illegible]мыш[illegible]ы «Wi-Fi Alliance» для беспроводных сетей на базе стандарта IEEE [illegible]Любое [illegible]рудование, соответствующее стандарту IEEE 802.11, может быть про[illegible] Wi-Fi Alliance для получения соответствующего сертификата и права нанесени[illegible]ипа Wi-Fi.

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

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

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

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

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

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

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

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

Диафрагма (от греч. diáphragma – перегородка) – это отверстие в объективе камеры, которое регулирует количество света, попадающего на ма[illegible] Изменение размера диафрагмы позволяет контролировать целый ряд пока[illegible]х для получения качественного изображения.

Доменное имя – это определенная буквенная последова[illegible] обозн[illegible]щая имя сайта или используемая в именах электронных почтовых ящико[illegible]ные имена дают возможность адресации интернет-узлов и располож[illegible]них сет[illegible]ресурсов (веб-сайтов, серверов электронной почты, других служб) [illegible] человека форме.

ИК-подсветка (ИК-прожектор) – устройство [illegible]печива[illegible]етку объекта наблюдения с излучением в инфракрасном диапазоне.

Камера «день/ночь» – это видеокамера, предназначен[illegible]боты круглосуточно в разных условиях освещенности. В условия[illegible]вещенности [illegible]бражение цветное. В темное время суток, когда яркий свет п[illegible]я сумерки, изображение становится черно-белое, в результате чего по[illegible]тся [illegible]льность.

Кодек – в системах связи ко[illegible]о обы[illegible]ер/декодер. Кодеки используются в интегрированных цепях или мик[illegible]для [illegible]зования аналоговых видео- и аудиосигналов в цифровой формат для пос[illegible]щей [illegible]редачи. Кодек также преобразует принимаемые цифровые сиг[illegible] в аналоговый [illegible]ормат. Термин «Кодек» также может относиться к компрессии/деко[illegible] в этом с[illegible]ае он обычно означает алгоритм или компьютерную программу для умен[illegible]лов и программ.

Нормально за[illegible]тые контакты – [illegible]кая конструкция датчика, которая в пассивном состоянии имеет замк[illegible]ты, а в акт[illegible]ном — разомкнутые.

Нормально разомкну[illegible] – такая конструкция датчика, которая в пассивном сос[illegible]азомкнутые контакты, а в активном – замкнутые.

Объе[illegible] – эт[illegible]сть [illegible]тической системы видеонаблюдения, предназначенная для фокусировк[illegible]ока[illegible]та на [illegible]ице видеокамеры.

Отно[illegible] – численно определяет содержание паразитных шумов в сигн[illegible]змеря[illegible]цибелах (дБ). Чем больше значение отношения сигнал/шум для в[illegible] тем меньше помех и искажений имеет изображение.

П[illegible] одна из множества точек, составляющих цифровое изображение. Цвет [illegible]ивность[illegible]дого пикселя составляет крошечную область изображения.

[illegible]рвер (Proxy – представитель, уполномоченный) – служба в компьютер[illegible] сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресур[illegible]обственного кэша. Прокси-сервер позволяет защищать клиентский компьютер от [illegible]х атак и помогает сохранять анонимность клиента.

Протокол – стандарт, определяющий поведение функ[illegible]ых бл[illegible] при передаче данных. Формализованные правила, определяющие пос[illegible]ль[illegible]сть и формат сообщений, которыми обмениваются сетевые к[illegible], лежа[illegible]а одном уровне, но в разных узлах.

Разрешение изображения – это количество [illegible]лей (то[illegible]ницу площади изображения. Измеряется в мегапикселях или отображ[illegible]ле[illegible]величин – высоты и ширины изображения. Высота и ширина также в данном слу[illegible]ются в пикселях.

Ручная диафрагма – противоположн[illegible]тической ди[illegible]рагмы, т.е. настройка диафрагмы камеры должна выполняться [illegible]ровки количества света, достигающего чувствительного элемента.

Светосила объектива – это х[illegible]еристи[illegible]азывающая, какое количество света способен пропускать данный об[illegible] бол[illegible]ксимальный диаметр открытой диафрагмы (или, соответственно, чем мень[illegible]F-числ[illegible]), тем большее количество света может попасть сквозь объекти[illegible]фокальную пло[illegible]сть, и тем выше светосила объектива.

Симплекс – при сим[illegible]й кабель или канал связи может использоваться для передачи инфор[illegible]ом направлении.

Уличная вид[illegible]а – это каме[illegible] видеонаблюдения, которая обладает всеми необходимыми характе[illegible]яния внешней среды для работы на улице.

Цветная [illegible]мера – [illegible]ера, которая дает цветное изображение. По определению[illegible]окамер черно-белые, а для получения цветного изображения возле кажд[illegible]ейки [illegible]рицы формируются цветные фильтры. Первый фильтр привносит красную со[illegible]ю[illegible] цвет[illegible]рой зеленую, а третий синюю. Таким образом, три ячейки становятся [illegible]кой[illegible]овом формате RGB. Следовательно, вместо трех пикселей на результирую[illegible]нии мы получаем только один.

[illegible]тромеханический ИК-фильтр – представляет собой устройство, которое [illegible]собн[illegible]жиме подавлять инфракрасный диапазон при помощи инфракрасного [illegible]ль[illegible]а, а в[illegible]ом режиме ИК-фильтр убирается электромеханически, таким образом, де[illegible]ипн[illegible]есь спектр светоизлучения.