УДК 621.397:625.42.

М.А Сайдахметов[1], М.В. Каракошкин[1]
[1]Казахская академия транспорта и коммуникаций им. М.Тынышпаева, г.Алматы, Казахстан

ПРИМЕНЕНИЕ WI-FI В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Аннотация. В этой статье мы рассмотрим технологию Wi-Fi. Дело в том, что потенциал данной технологии раскрыт недостаточно, и она редко используется при построении систем безопасности. Рассмотрены вопросы применения Wi-Fi в системах видеонаблюдения.

Аңдатпа. Осы мақалада біз Wi-Fi технологиясы қарастырамыз. Технология әлеуетті жеткілікті ашып, және ол сирек қауіпсіздік жүйелерін құрылыста пайдаланылатын фактісі. Бейнебақылау жүйелерінде Wi-Fi мәселелері.

Abstract. In this article we will consider the technology of Wi-Fi. The fact is that the potential of this technology is not sufficiently disclosed, and it is rarely used in the construction of security systems. Questions of application of Wi-Fi in video surveillance systems are considered.

Ключевые слова: видеонаблюдения, технология Wi-Fi, беспроводная связь, видеокамеры

Түйінді сөздер: бейнебақылау, Wi-Fi технологиясы, сымсыз байланыс, бейне камералар

Keywords: video surveillance, Wi-Fi technology, wireless communication, video cameras

Введение. Беспроводная связь – это передача информации на расстояние без использования электрических проводников. Беспроводная связь обычно рассматривается как отрасль телекоммуникаций. Беспроводная технология, которая стала заметна на мобильном рынке с появлением стандарта 802.11 или Wi-Fi.

Wi-Fi – это современная технология организации беспроводных сетей по радиоканалу. Обычно схема сети Wi-Fi содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме "точка-точка", в этом случае точка доступа не используется, а клиенты соединяются посредством беспроводных сетевых адаптеров напрямую.[1] Когда используется точка доступа, следует учитывать, что она представляет собой обычный концентратор. При нескольких подключениях видеокамер к одной точке полоса пропускания делится на количество подключенных пользователей. Теоретически ограничений на количество подключенных видеокамер нет, но на практике их число следует ограничивать, исходя из минимально необходимой скорости передачи данных для каждой камеры. Например, одна сетевая камера с разрешением VGA и скоростью 25 кадр/с при небольшом сжатии в самом популярном формате MPEG-4 занимает полосу в 2-2,5 Мбит/с. Это означает, что 10 камер отнимут максимум 25 Мбит/с. очка доступа с полосой пропускания 54 Мбит/с (а с реальной скоростью передачи данных 25 Мбит/с) позволит без проблем принять сигнал от 10 Wi-Fi-видеокамер, а если брать в расчет видеокамеры с более современным сжатием H.264, то поток от камеры с тем же качеством займет около 0,5-1 Мбит/с. К одной точке доступа можно подключить не больше 25 видеокамер.

Стандарт Wi-Fi не ограничивается малыми расстояниями в закрытых помещений, а в открытых помещениях в прямой видимости Wi-Fi может работать на расстоянии почти 500 м. Это уже приемлемая цифра для профессиональных систем видеонаблюдения, ведь при использовании современных потоковых алгоритмов сжатия скорости 0,5 Мбит/с может оказаться вполне достаточно для передачи 1 канала видео приличного качества. А

если учитывать, что это расстояние можно увеличивать с помощью направленных антенн и промежуточных точек доступа, то такое решение становится еще более интересным.

Рассмотрим немного подробнее к применению Wi-Fi в системах видеонаблюдения. Надежность соединения, правильный подбор оборудования, использование внешних узконаправленных антенн (которые, кстати, с помощью кабеля можно удалить от видеокамеры на расстояние до 30 м) и промежуточных точек доступа успешно решают эту проблему.

Защита видеоинформации в беспроводных IP-системах видеонаблюдения достигается несколькими способами. Ключевыми среди них являются: применение брандмауэров, использование паролей и шифрование. Брандмауэр работает как электронные "ворота", пропускающие зарегистрированных пользователей и запрещающие доступ неавторизованным лицам. Применение паролей позволяет не только ограничить доступ к системе видеонаблюдения, но и распределить права доступа персонала к определенным видеокамерам. А при шифровании попытки перехвата зашифрованных данных в IP-системе охранного видеонаблюдения становятся бессмысленными, если злоумышленник не знает уникального кода для расшифровки потока данных. Код, в свою очередь, устанавливается системным администратором.

Легитимность использования Wi-Fi. Использование Wi-Fi без разрешения на использование частот от Государственной комиссии по радиочастотам (ГКРЧ) возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий. Для легального создания вне офисной беспроводной сети Wi-Fi (например, радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот.

Глушение сигнала. Такая опасность, действительно, существует. Но, во-первых, для того, чтобы полностью заглушить сигнал, нужен достаточно мощный источник, и, во-вторых, этот источник должен находиться очень близко к радиотракту. Однако даже в этом случае можно попытаться решить проблему с помощью мощных узконаправленных антенн.

Вредность излучения. Мировая организация здравоохранения признала излучение Wi-Fi безвредным для здоровья человека Так, например, излучение от устройств Wi-Fi в среднем в 10-20 раз ниже, чем от обычного сотового телефона.

Выбор Wi-Fi-IP-видеокамеры. Рекомендуем выбирать те видеокамеры, которые поддерживают стандарт 802.11g.

Антенна желательно, чтобы она была съемной. Это при необходимости позволит заменить штатную антенну на более мощную и, следовательно, передавать сигнал на большие расстояния и с более высокой скоростью.

Поддерживаемые алгоритмы сжатия. Известно, чем больше расстояние от Wi-Fi-камеры до точки доступа и чем больше камер подключено к одной точке доступа, тем меньше ширина канала для каждой из них. Поэтому рекомендуем выбирать камеры, поддерживающие современные потоковые алгоритмы сжатия MPEG-4, H.264 и др., которые позволяют передать видео хорошего качества по "тонкому" каналу.

Защита данных. Так как Wi-Fi – это передача сигнала по радиоканалу, и "предполагаемый злоумышленник" может попытаться перехватить сигнал, рекомендуем выбирать те видеокамеры, которые имеют фильтрацию IP-адресов, шифрование сигнала.

Наличие обычного сетевого порта позволит при желании использовать Wi-Fi-видеокамеру как обычную проводную. Если потребуется аудиосвязь и подключение указанного оборудования, то лучше сразу приобретать видеокамеру с аудио входом и выходом, тревожными входами, чтобы в дальнейшем не пришлось тянуть провода для реализации дополнительных функций.

Технология Wi-Fi уже сегодня предоставляет уникальные возможности для построения систем видеонаблюдения, особенно в условиях, затруднительных для

прокладки кабелей, а также в тех случаях, когда необходимо оптимизировать сроки и затраты на монтаж, подключение и обслуживание систем IP-видеонаблюдения.

ЛИТЕРАТУРА

[1] Лиэри Дж, Рошан П.Основы построения беспроводных локальных сетей стандарта 802.11, М.: Издательский дом "Вильямс", 2004,

[2] www.secuteck.ru/articles2/ip.../pravda_i_mifi_o_wi_fi_v_ip_videonabludenii_page9..