IP-технологии в ОПС

Сергей ЛЁВИН,
главный конструктор «СИГМА-ИС»

Сегодня можно смело утверждать: IP-технологии правят миром. Шутка про чайник с выходом в интернет уже и не шутка даже вроде, а вполне себе реальность. А ведь не так уж и давно все начиналось.

В середине 1970-х гг. Агентство по внедрению научно-исследовательских проектов передовой технологии при министерстве обороны (DARPA) заинтересовалось организацией сети с коммутацией пакетов для обеспечения связи между научно-исследовательскими институтами в США. DARPA и другие правительственные организации понимали, какие потенциальные возможности скрыты в технологии сети с коммутацией пакетов; они только что начали сталкиваться с проблемой, с которой сейчас приходится иметь дело практически всем компаниям, а именно с проблемой связи между различными компьютерными системами.

Поставив задачу добиться связности гетерогенных систем, DARPA финансировала исследования, проводимые Стэнфордским университетом и компаниями Bolt, Beranek и Newman (BBN) с целью создания ряда протоколов связи. Результатом этих работ по разработке, завершенных в конце 1970 гг., был комплект протоколов Internet, из которых наиболее известными являются Transmission Control Protocol (TCP) и Internet Protocol (IP).

В отчете Cisco Visual Networking Index Forecast 2012–2017 («Индекс развития визуальных сетевых технологий за период с 2012 по 2017 г.») компания Cisco спрогнозировала трехкратное увеличение интернет-трафика. Ожидается, что в период до 2017 г. объем глобального фиксированного и мобильного IP-трафика будет ежегодно расти со скоростью 1,4 зеттабайта, т. е. более 1 трлн Гбайт. В результате к 2017 г. ежемесячный объем глобального IP-трафика составит почти 121 экзабайт. Для сравнения: в 2012 г. аналогичный показатель составил 44 экзабайта. К 2017 г. в мире будет осуществлено более 19 млрд сетевых соединений (для фиксированных и мобильных персональных устройств, для связи типа «машина-машина»). Для сравнения: в 2012 г. таких соединений было около 12 млрд.

В 2012 г. 26% интернет-трафика генерировалось не ПК, а иными устройствами. К 2017 г. доля таких устройств в интернет-трафике возрастет до 49%. Объем трафика, сгенерированного на персональных компьютерах, будет ежегодно увеличиваться на 14%, но объемы, сгенерированные на других устройствах, будут расти еще быстрее: ежемесячный рост трафика, сгенерированного на телевизионных приемниках, составит 24%, на планшетных компьютерах – 104%, на смартфонах – 79%, на модулях «машина-машина» – 82%.

В системах безопасности, безусловно, ведущее положение в применении IP-решений занимают системы видеонаблюдения. Это касается как степени проникновения сетевых технологий в технические решения, так и объема передаваемой информации. Причем первое утверждение вытекает из второго: так как поток информации от любого компонента системы видеонаблюдения достаточно большой (это касается как видеокамер, так и видеосерверов), то логично, что все они непосредственно напрямую подключаются к сети. Для видеонаблюдения IP-решения предоставляют принципиально новые возможности – это и использование камер высокого разрешения, простое масштабирование системы, резервирование и возможности по организации доступа к видеоинформации в независимости от географической удаленности видеокамер от наблюдателя.

Что же может дать внедрение IP-технологий в охранно-пожарные сигнализации? Рассмотрим по порядку возможные преимущества таких решений. Основными компонентами системы охранно-пожарной сигнализации являются охранные и пожарные извещатели, а также приемно-контрольный прибор (ППК). В больших системах применяются промежуточные контроллеры-расширители. В этом случае извещатели подключаются к центральному прибору через расширитель. В состав системы может входить автоматизированное рабочее место (АРМ) на базе компьютера, где в графическом виде показывается состояние объекта охраны, а также выдаются тревожные извещения. Приемно-контрольный прибор подключается к компьютеру, передает информацию о своем состоянии и принимает команды управления. Все эти компоненты системы подключаются между собой, используя некие интерфейсы. И, в общем то, в каждом случае это может быть IP-соединение, что, как правило, предполагает подключение через Ethernet.

ПОДКЛЮЧЕНИЕ ППК К ВЕРХНЕМУ УРОВНЮ СИСТЕМЫ БЕЗОПАСНОСТИ

Подключение ППК к компьютеру через сеть выглядит сегодня наиболее оправданным. Лет 10–15 назад стандартный интерфейс подключения в подобных случаях был RS-232. Однако сейчас этого интерфейса в компьютерах уже не найти. USB для подключения ППК не совсем подходит – дальность связи маловата, да и надежностью этот тип соединения похвастаться не может. Из стандартных интерфейсов современного компьютера остается Ethernet. Использование сетевого подключения дает неоспоримые преимущества и даже создает новые возможности, ранее не доступные. Во-первых, может использоваться существующая сетевая инфраструктура предприятия. Одновременно к одному прибору может быть подключено несколько АРМ, по крайней мере, сетевой интерфейс это позволяет. Появляется возможность построения распределенной системы, когда ППК размещаются непосредственно на объекте охраны, в непосредственной близости от мест установки извещателей. И самое главное – достаточно просто может быть реализован механизм резервирования подключения и дублирования компьютеров верхнего уровня.

ЦЕНТРАЛИЗОВАННАЯ ОХРАНА

До недавнего времени в централизованной охране объектов в качестве интерфейса систем передачи извещений (СПИ) использовались в основном каналы телефонной сети общего пользования (ТФОП) или специализированный радиоканал. Сегодня все чаще применяются решения на базе GSM и интернет. Здесь сетевое подключение объектов охраны к пульту централизованной охраны (ПЦО) дает возможность использования уже существующей инфраструктуры передачи данных, что значительно упрощает и удешевляет внедрение и развертывание системы. Также появляется возможность доступа к системе безопасности через web-интерфейс, что может быть интересно конечным пользователям системы.

ОБЪЕДИНЕНИЕ ППК В СЕТЬ

Если объект охраны достаточно большой, то, скорее всего, в системе используется несколько приборов. В этом случае бывает необходимо обеспечить обмен информацией между приборами, чаще всего это выполнение каких-либо действий в одном приборе в ответ на события в другом. Например, при срабатывании пожарного извещателя, подключенного к ППК № 1, включить управление оповещением об эвакуации через исполнительное устройство, подключенное к ППК № 2. Лучшим способом организации взаимодействия ППК в этом случае будет IP-подключение через Ethernet. При этом достаточно просто может быть реализована одноранговая сеть ППК, что позволит напрямую передавать данные с прибора на прибор.

ПОДКЛЮЧЕНИЕ РАСШИРИТЕЛЕЙ И ИЗВЕЩАТЕЛЕЙ К ППК

Чаще всего для связи расширителей и ППК применяются интерфейсы и протоколы полевых шин, например RS-485. Применение RS-485 здесь в общем и целом оправданно, однако и здесь вполне возможно использование сетевого подключения. Это прежде всего удобно с точки зрения использования существующей кабельной системы объекта. Что касается извещателей, то сейчас пока большинство все еще за неадресными вариантами подключения, когда каждый извещатель подключается к индивидуальному входу ППК или расширителя. Если же к одному входу подключено несколько извещателей, определить, какой конкретно сработал, становится уже невозможно. Более современный способ предусматривает наличие адреса у каждого извещателя, что позволяет однозначно идентифицировать его в системе и подключать на один интерфейсный вход несколько извещателей (до нескольких десятков или даже сотен датчиков). Для адресного извещателя теоретически уже возможно применение IP-подключения. Однако на практике пока это оказывается слишком дорогим решением. Если говорить о пожарной сигнализации, то применение IP-подключений несколько ограничено нашими нормативными документами, требующими применения специализированных кабелей, не поддерживающих горение. Но в целом IP-технологии в охранно-пожарных системах уже прочно заняли свое место. Так что в ближайшем будущем наличие у каждого охранного или пожарного датчика собственного IP-адреса будет восприниматься как должное.