СКУД без проводов: идеи, примеры реализации, перспективы

Основной задачей данного обзора является ознакомление специалистов в области безопасности с новой, перспективной топологией организации полноценных беспроводных СКУД, базирующейся на протоколе беспроводной передачи данных IEEE 802.15.4, более известной как «технология ZigBee».

Правильнее было бы назвать эту статью «введением», а не обзором – так как из-за новизны предлагаемой концепции построения беспроводных СКУД, имеется реальная ограниченность предложения таких систем на рынке.

В последние несколько лет беспроводные технологии активно внедряются во многих системах безопасности – в частности, они весьма успешно используются в системах охранной и пожарной сигнализации. Беспроводные (зачастую – даже с питанием от обычных батарей) датчики, извещатели, сирены и другое оборудование, работающее по радиоканалу, предлагает большое число производителей, в том числе и отечественных. Причины такого успеха лежат на поверхности – вместе с отказом от проводов, эти системы приобретают ощутимые преимущества как для конечных пользователей так и для инсталляторов. Для первых повышается безопасность и надежность систем, независящих от перебитых или перегоревших проводов. Для вторых не только значительно упрощается установка систем – но и увеличиваются возможности по расширению и наращиванию систем на функционирующих объектах.

Тем не менее, в такой сфере обеспечения безопасности, как СКУД, ситуация на данный момент совсем иная: о беспроводных СКУД много говорят как в среде инсталляторов, так и разработчиков – но реально предлагает такие системы считанное число западных производителей. Да и внедрять такие системы у нас пока готовы далеко не все – на данный момент в странах СНГ установлено буквально несколько таких систем. И пока все они – на гостиничных объектах.

Попробуем разобраться в ситуации, а также убедить специалистов, что беспроводные СКУД – не миф или теоретические изыскания «на тему», а реальная альтернатива «классическим» проводным системам.

Для начала разберемся с самой идеей «беспроводности», т.е. определим:

а) о каких системах мы говорим

б) от каких именно проводов необходимо избавиться.

Итак:

а) Мы рассматриваем не автономные СКУД на 1-2 двери и сотню-другую пользователей, а универсальные системы 2-го, а лучше – 3-го класса, т.е. системы на большое количество пользователей и точек доступа (как минимум – несколько десятков), с управлением и контролем в реальном времени, с достаточным числом уровней доступа и временных расписаний доступа (256 и более) и т.д.

б) В идеале, «беспроводная СКУД» должна быть таковой в абсолютном выражении – т.е. без проводов вообще.

Существующие сегодня (и предлагаемые на нашем рынке) классические СКУД, подпадающие под ГОСТ-овское определение универсальных систем 2-го и 3-го классов, используют провода весьма широко, и причем с абсолютно разными целями. Разделим все эти провода на три категории: Во-первых, магистральные каналы связи (чаще всего используются стандарты передачи данных по протоколам RS485 или IP). В эту же категорию «оптом» запишем еще и всевозможные конвертеры и преобразователи интерфейсов (это хоть и не провода в чистом виде – но «довесок», от которого тоже не лишним будет избавиться). Во-вторых, провода для «обвязки» двери, т.е. шлейфы, соединяющие контроллер доступа со считывателями, исполнительными механизмами, датчиками, кнопками выхода и т.п. Ну и в-третьих, питающие лини как для контроллеров, так и периферии – считывателей, исполнительных устройств. Такое «классификационное» деление проводов сделано намеренно – поскольку перевод каждого из трех типов в беспроводное состояние решается по-разному.

1. **Магистрали.** По этим каналам осуществляется связь котроллеров доступа с базой данных СКУД (центральным сервером БД). Как правило, эти каналы передачи данных занимают львиную долю общего километража кабелей, и перевести их в беспроводный радиоканал проще всего (теоретически). Технологий для этого уже сейчас существует достаточно много – Wi-Fi, WiMAX, GSM, Bluetooth, ZigBee... Если в системе используются IP-контроллеры, то и выдумывать-то ничего не надо – достаточно просто поставить 2 точки доступа Wi-Fi «на концах провода». На самом деле, здесь не все так просто – но сначала рассмотрим следующие пункты.

2. **«Обвязка» точки доступа.** Термин достаточно условный, но все специалисты его прекрасно понимают. Несмотря на небольшой метраж таких кабелей в расчете на систему, именно возможность (точнее – невозможность) их прокладки на конкретном объекте в большинстве случаев ограничивает количество точек доступа, оборудуемых СКУД . А при развертывании СКУД на уже функционирующем объекте, именно прокладка этого «последнего метра кабеля» становится основной головной болью инсталляторов. Еще одна проблема – разнообразие типов протоколов, которые используются в «обвязке». В отличие от магистралей, где таких протоколов не наберется и пяти штук, здесь мы имеем полное разнообразие. Теоретически – все они также могут быть переведены на беспроводной радиоканал. Практически – стоимость всевозможных конвертеров абсолютно точно уничтожит весь смысл перевода системы в «беспроводное» состояние.

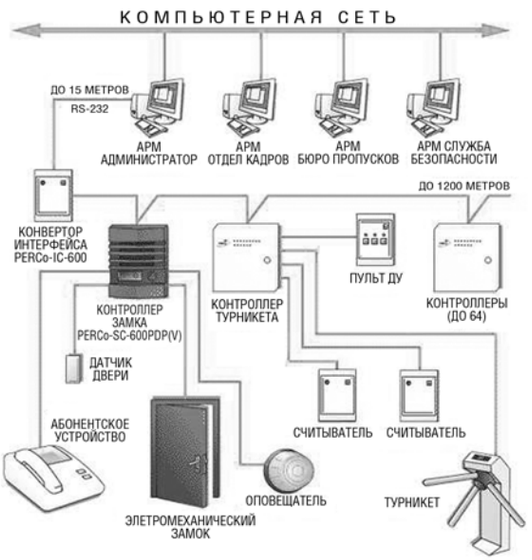
3. **Питающие линии.** Здесь также одна сплошная проблема... Технологий передачи питающего напряжения достаточной мощности без проводов практически нет (как минимум – нет промышленных образцов, пока только прототипы). Единственная альтернатива – использование батарей или аккумуляторов. Однако я с трудом могу себе представить размер (и стоимость) комплекта батарей, достаточный для работы так любимого нашими инсталляторами магнитного замка сроком хотя бы на год-два без перезарядки или замены (более частая смена батарей уничтожит перспективу применения такой системы для большинства пользователей из-за эксплуатационных расходов).

На первый взгляд – полный тупик... Да, у нас все еще остается реальная альтернатива перевода магистралей в беспроводное состояние, а кабели по 2-му и 3-му пунктам можно оставить как есть – и многие наши разработчики других вариантов даже и не рассматривали.

Но это будет уж никак не «беспроводная СКУД».

Тем не менее, все перечисленные проблемы имеют решение, причем известно оно достаточно давно.

Чтобы избавиться от проводов, нужно или применять сразу несколько беспроводных конвертеров (что – как было указано выше – сводит к нулю саму идею), или ... обнулить их длину. Т.е. комплект оборудования, куда входит контроллер, считыватель, датчик положения (если нужен), исполнительное устройство (замок) и т.д. должен превратиться в единое устройство – электронный замок. Провода «извне»



Пример классической проводной СКУД

к нему не подводятся, несколько сантиметров провода внутри самой конструкции замка мы учитывать не будем. Даже источником питания электронных замков служит не блок питания от сети 220 В, а обычные батарейки: от одного комплекта (как правило – от 1 до 6-ти стандартных батареек, которые можно купить в любом магазине) электронные замки работают по 2-4 года. Такие характеристики достигаются благодаря «хитрому» исполнительному механизму **электронного замка: двигатель (иногда – соленоид) в таких замках осуществляет только блокировку/разблокировку запирающего механизма, а дверь открывает сам пользователь, нажимая на ручку замка.** Благодаря такой схеме, в электронных замках применяются микродвигатели с экстремально низким потреблением энергии.

Подобные системы – системы электронных замков – изобретены более 20 лет назад, но они обладали рядом особенностей, достаточно серьезно ограничивающих область их применения:

1. До последнего времени, в таких системах магистральные каналы связи не использовались вообще. Электронные замки не имели связи с сервером системы в режиме реального времени. Время от времени оператор системы мог обеспечить связь замков с сервером благодаря переносу (в буквальном смысле) информации от БД к замку и обратно через специальный прибор – портативный программатор. То есть, для сбора протокола проходов через точку доступа или, наоборот, для внесения изменений в параметры точки доступа, он должен был подойти к замку с программатором, подключить его к замку для загрузки данных, и затем вернуться к компьютеру.

Управление же точкой доступа (электронным замком) в режиме реального времени (открывание или блокировка двери с рабо-чего места оператора системы) вообще не предусматривалась.

2. Для удобства управления правами доступа пользователей при отсутствии магистрали (точнее – для возможности назначения прав новым пользователям после того, как замки были запрограммированы), эти права в системах электронных замков записываются непосредственно на карту пользователя. Т.е. карта ВСЕГДА выступает не в роли идентификатора доступа, а в роли носителя прав доступа. Отсюда – следующая особенность:

3. Для управления пользователями, то есть для изменения или отмены прав доступа, оператор должен был получить физический доступ к карте (напомним – именно она является носителем информации о доступе) или к замку (чтобы внести в его память черный список с перечнем утерянных карт). Чтобы изменить права доступа – карту надо переписать. Чтобы отменить утерянный ключ – надо обойти все замки, где эта карта была действительна.

Назвать такую систему полноценной СКУД нельзя. До последнего времени они применялись в основном в отелях, где при большом количестве точек доступа (электронных замков) отсутствие необходимости в прокладке поводов с лихвой окупает все описанные недостатки.

Но времена меняются...

Идея создания беспроводной универсальной СКУД

Для эволюционного перехода от электронного замка к универсальной СКУД необходимо обеспечить связь между замками и сервером СКУД в режиме реального времени. Конечно, организовать такую связь можно и классическим методом, т.е. проложить кабели. Однако в таком случае мы теряем главное преимущество – простоту монтажа и возможность развертывания системы «по живому», в уже функционирующем офисе, к примеру. Да и цена такой системы будет достаточно высока. В классических СКУД можно (и нужно) использовать один контроллер на несколько дверей (4, 8, 16...), а поскольку контроллер является наиболее дорогостоящим элементом системы, цена «в расчете на одну дверь» будет не столь высока. С электронным замком, у которого контроллер «вживлен» внутрь, всегда выполняется равенство «один контроллер = одна дверь».

Однако, если к возможностям электронных замков добавить беспроводной радиомодуль, расклад сил может кардинальным образом измениться. Ведь в этом случае, в дополнение ко всем имеющимся преимуществам, мы получаем действительно **беспроводную**, универсальную и отвечающую всем требованиям СКУД.

Выбор технологии

Выбор технологии для организации беспроводного магистрального канала между электронными замками и сервером СКУД – весьма принципиальная задача. Упоминавшиеся ранее технологии Wi-Fi или Bluetooth, равно как и GSM-сети, для этих целей на самом деле не годятся. Как по причине высокого энергопотребления, так и из-за особенностей организации топологии сети. Любая из указанных технологий съедала бы весь заряд комплекта батарей автономного замка за несколько дней (в лучшем случае), а необходимость подвода внешнего питания (установка блоков питания и прокладка кабеля к замку) уничтожает сам смысл термина «беспроводная СКУД».

Поэтому в качестве транспорта был выбран протокол IEEE 802.15.4. – он предоставляет прекрасные возможности как по организации достаточно разветвленных многоуровневых сетей (со смешанной топологией «точка-точка», «звезда»), так и по параметрам энергопотребления передающих устройств.

Во врезке Вы сможете найти краткое описание истории возникновения и технических характеристик этого протокола. Мы же остановимся на нескольких нюансах, имеющих непосредственное отношение к тематике СКУД. Основным преимуществом этого стандарта как магистрального транспорта для беспроводных СКУД, основанных на применении электронных замков, является экстремально низкое потребление энергии самим радиомодулем.

На заявленную же скорость передачи до 250 кбит/с и расстояния уверенного приема сигнала до 100 метров при этом рассчитывать не стоит. Во-первых, эти параметры сильно зависят от конкретной реализации модуля и от состояния окружающей среды (толщина и тип стен и перекрытий и т.п.). Во-вторых, в заявленных 250 кбит/с достаточно хорошую часть «отъедает» служебная информация самого протокола, обеспечивающая работоспособность устройств при достаточно больших допустимых потерях пакетов.

Еще один нюанс – «плата за использование» частотного диапазона 2,4 ГГц, в котором уже живут несколько других технологий (тот же Wi-Fi и Bluetooth). Из-за такого «соседства», в реальности вряд-ли удастся спокойно использовать все 16 представленных протоколом каналов.

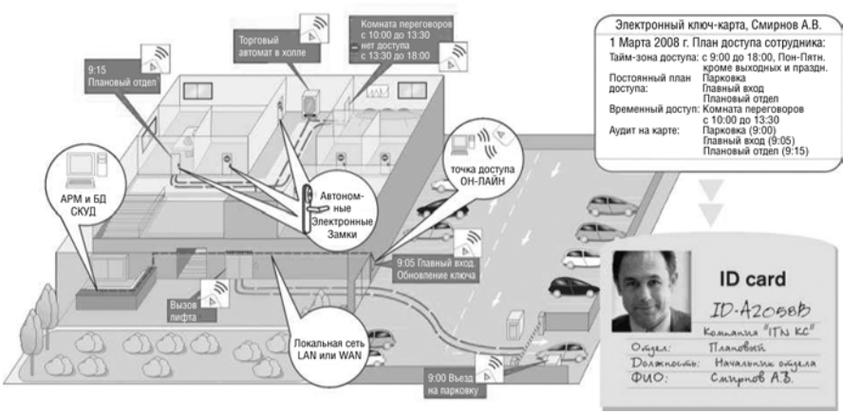
Возможно, именно эти проблемы пока тормозят использование протокола IEEE 802.15.4 в «классических» СКУД, так как зависимость их работоспособности от качества магистрали достаточно высока.

Однако с системами, построенными на электронных замках, ситуация принципиально другая.

Во-первых, эти системы изначально создавались для использования в условиях, когда никакой магистрали нет вообще – поэтому и в беспроводном варианте они спокойно выполняют весь базовый набор функций даже при полностью «упавшей» сети.

Во-вторых, сам принцип системы доступа здесь отличается от «классики» кардинально.

Платформа SALTO и ПО



Пример СКУД с использованием автономных электронных замков

Главное отличие – использование электронных «носителей информации о доступе» вместо «идентификаторов доступа». Права доступа записываются на саму карту в момент выдачи ключа пользователю – а не сохраняются «в недрах» БД СКУД и/или памяти контроллера, ассоциированные с неким «идентификатором», выданным на руки пользователю. То есть контроллеры электронных замков не должны хранить в своей памяти таблицу доступа со списком всех карт, которые надо «пускать» – а только собственные параметры плюс реальное время-дату. При предъявлении ключа происходит сравнение информации, считанной из памяти карты, с информацией из памяти контроллера (попадает ли данный контроллер в список зон, разрешенных на карте – с учетом реального времени-даты, текущего режима работы контроллера и т.п.). И решение «открывать-не открывать» контроллер принимает самостоятельно, без участия сервера системы.

Наличие беспроводной связи электронного замка с сервером не является обязательным условием функционирования системы – оно лишь снимает те ограничения, которые не позволяли ранее называть такие системы полноценной СКУД . Вместе с тем, все эти «дополнительные» функции не столь чувствительны ни к скорости прохождения сигнала от сервера к замку и обратно (конечно, речь не идет о минутах или даже о десятках секунд – но задержка в секунду-другую вполне возможна), ни к возможным пропаданиям связи и их длительности.

К этим возможностям относятся:

1. Мониторинг состояния системы и управление точками доступа в реальном времени.

2. Сбор аудита системы (кстати – электронные замки имеют свою собственную энергонезависимую память, куда все события обязательно записываются даже если беспроводная связь работает без сбоев).

3. Управление пользователями, т.е. возможность отмены, изменения прав доступа и отслеживания пользователя в реальном времени.

4. Некоторые другие возможности, характерные для особых условий применения – например, в гостиничных системах стало возможным удаленное продление срока проживания или переселение из одного номера в другой без посещения гостем стойки размещения.

Несколько слов скажем о топологии беспроводной сети, построенной на основе протокола IEEE 802.15.4. Выше упоминалось, что радиомодули, работающие по этому стандарту, имеют ограничения по дальности «видимости» – в реальных условиях это расстояния не более 20-40 метров (мы, конечно, подразумеваем развертывание системы в помещении). Для организации нормальной СКУД в большинстве случаев этих расстояний недостаточно. Поэтому сетевая инфраструктура состоит не только из приемника и передатчика – но и промежуточных повторителей-ретрансляторов сигнала, а также шлюзов, соединяющих беспроводные сети с сегментом локальной сети. Например, путь прохождения сигнала может выглядеть как «точка доступа – повторитель – повторитель – ... – шлюз – локальная сеть – сервер». Количество повторителей между точкой доступа и шлюзом (это – обязательные элементы инфраструктуры) зависит как от «географии» объекта, так и от конкретной реализации системы. Например, в системах SALTO Wireless – которые мы будем рассматривать далее – максимальное количество повторителей между замком и шлюзом – 4. Но при этом инфраструктура сети не обязательно должна быть линейной – каждый шлюз (он, кстати, тоже совсем не обязательно должен быть только один на систему) может одновременно работать с 4-мя повторителями и 16-ю замками, каждый повторитель – еще с 4-мя другими повторителями и так же 16-ю замками. В итоге – мы получаем «древовидную» топологию сети со множеством ответвлений.

СИСТЕМНАЯ АРХИТЕКТУРА SALTO Wireless

Максимальная глубина – 4 повторителя

И последнее – вернемся еще раз к теме проводов... Шлюзы и повторители, которые создают сетевую инфраструктуру, на современном этапе нуждаются в проводах. Во-первых, им требуется внешнее питание – их перевод на питание от батарей теоретически возможен, но все-таки производители предпочитают пока использовать внешние источники питания. Во-вторых, основная задача шлюза, как видно из вышесказанного – производить стыковку беспроводной сети с обычной локальной сетью объекта. Т.е. шлюзы также используют провод, чтобы донести информацию до сервера. Конечно, и здесь можно обойтись Wi-Fi точкой доступа или же встроить шлюз прямо в компьютер – но удобнее разместить его в той точке пространства, где он наиболее оптимально будет выполнять свои обязанности.

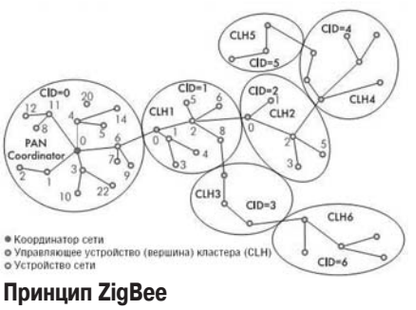
Разработчиком стандарта IEEE 802.15.4 выступил альянс компаний (Invensys, Honeywell, Mitsubishi Electric, Motorola, Philips и др.). Этот стандарт описывает беспроводные персональные вычислительные сети (WPAN – Wireless Personal Area Network). Стандарт IEEE 802.15.4 был принят достаточно давно (формирование спецификации IEEE 802.15.4 началось аж в конце 90-х гг. прошлого века, действующая сейчас спецификация протокола датирована 2006-м годом).

ZigBee – название набора протоколов высокого сетевого уровня, использующих радио-передатчики, основанные на стандарте IEEE 802.15.4. Название ZigBee появилось как комбинация от «Zig-zag» – зиг-заг и «Bee» – пчела, поскольку топология сети предполагает возможность передачи информации по траектории, подобной зигзагообразному полету пчелы от цветка к цветку.

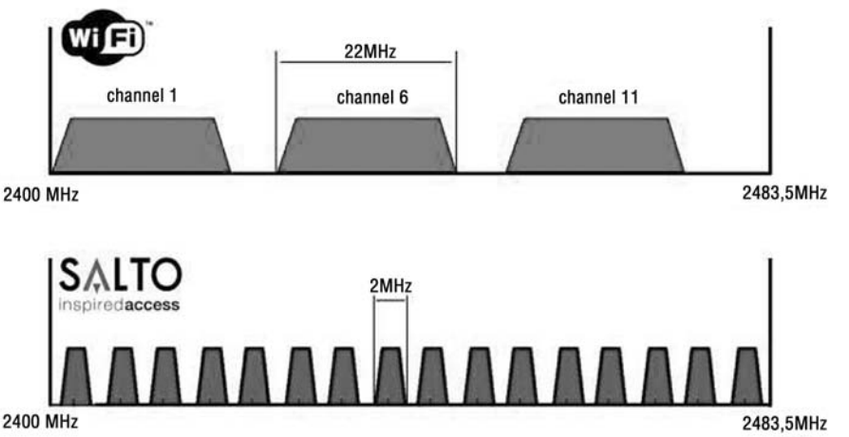
ZigBee нацелена на приложения, которым требуется большее время автономной работы от батарей и большая безопасность, при меньших скоростях передачи данных. Основная особенность технологии ZigBee заключается в том, что она при относительно невысоком энергопотреблении поддерживает не только простые топологии беспроводной связи («точка-точка» и «звезда»), но и сложные беспроводные сети с ячеистой топологией с ретрансляцией и маршрутизацией сообщений.

Стандарт IEEE 802.15.4 предусматривает работу в трех диапазонах, наиболее быстрый и емкий из которых – 16 каналов в диапазоне 2450 МГц (шаг центральных частот – 5 МГц, самая нижняя из них – 2405 МГц) – в Украине как раз попадает в спектр нелицензируемых частот. Скорость в этом канале – 250 кбит/с. Дальность передачи – от 10 до 100 м, в зависимости от отдаваемой мощности и окружающей среды.

По материалам статьи
И. Шахновича
«Персональные беспроводные сети стандартов IEEE 802.15.3 и 802.15.4»
http://www.electronics.ru/issue/2004/6/12



Принцип ZigBee



Работа в частотном диапазоне WiFi без помех

Кстати – благодаря технологии PoE (т.е. передаче питания прямо по витой паре), провода по обеим пунктам можно «уместить» в один кабель.

Однако как нам кажется, наличие в системе нескольких метров проводов для подключения и питания шлюзов и повторителей точно не может лишить системы, построенные на этой технологии, честно заработанного звания «Беспроводная СКУД».

Реализация и примеры инсталляций

На сегодняшний день существует всего несколько реализаций подобных беспроводных СКУД – что объясняется, прежде всего, новизной технологии. Промышленные (не экспериментальные) образцы оборудования появились в основном во второй половине прошлого года, когда сразу несколько производителей представили свои беспроводные решения с интервалом буквально два-три месяца. Одну из этих систем приведем в качестве примера реализации описанной идеи беспроводной СКУД.

Речь пойдет о системе SALTO RFID Wireless (Испания).

Как видно из названия, речь идет о системе, использующей бесконтактные (но обязательно – перезаписываемые) электронные ключи и электронные замки, использующие беспроводной протокол IEEE 802.15.4.

Главной особенностью такой системы является возможность комбинации (в любой пропорции) беспроводных он-лайн замков как с «классическими» проводными IP-контроллерами и считывателями, так и полностью автономными электронными замками, не имеющими связи с сервером в реальном времени. Это позволяет, в зависимости от конкретного объекта, создавать любые системы, с любым набором функционала и адекватной этому функционалу ценой. Например – часть точек доступа, наиболее важных с точки зрения надежности управления и контроля в реальном времени, можно оборудовать проводными IP-контроллерами. Другая часть помещений, где управление в реальном времени просто не нужно (часть кабинетов, переговорные и т.д.) оборудуются обычными электронными замками. А основная часть точек доступа оборудуется беспроводными он-лайн замками. То есть заказчику системы или инсталлятору совсем не обязательно выбирать между полностью проводной, автономной или беспроводной системой – по каждой конкретной точке доступа можно спокойно решать, какой из типов оборудования наиболее приемлем как по возможностям, так и по стоимости. Более того – автономные замки могут быть легко обновлены до версии «беспроводной онлайн» спустя какое-то время после развертывания системы – для этого достаточно просто вставить в замок радиомодуль, приобретенный отдельно.

Такой подход к построению СКУД выгодно отличает системы SALTO от классических проводных систем прежде всего по возможностям развертывания и расширения систем. И если для «классических» СКУД среднее количество точек доступа на объект зачастую колеблется где-то около десяти, а еще чаще вообще ограничивается буквально несколькими «турникетами на входе в здание», то для систем SALTO среднее количество точек доступа на объекте приближается к 50. Потому как Вы можете спокойно установить такую систему как на турникет, так и на основную массу всех дверей в офисе, банке, или университете – не попадая в зависимость от возможности прокладки проводов до определенного помещения или двери.

Несколько слов о примерах инсталляций таких систем – у нас, и в мире.

Поскольку на данный момент локомотивом описанной беспроводной технологии являются исключительно производители электронных замков – а их вотчиной в России и Украине до последнего времени были исключительно отели – то и первые установки таких систем у нас в стране также случились именно в отельном бизнесе.

Если же говорить о внедрении подобных систем на западе – то там ситуация несколько иная. Прежде всего это связано с тем, что там нет такого доминирования исключительно проводных систем – и СКУД на основе автономных замков там используются достаточно широко, отнюдь не ограничиваясь отельным сектором. У уже упомянутого производителя – SALTO Systems (Испания) – количество установленных беспроводных замков на начало 2010 года составляло уже более 1500. Учитывая, что технологии «от роду» буквально несколько лет. Среди реализованных проектов можно упомянуть Бристольский университет (более 200 точек доступа), Офисный центр Компас в Гон-Конге и отель Мандарин в Барселоне.

Перспективы

На данный момент никто не рискнет гарантировать технологии, которую мы описали, светлое будущее – хотя все предпосылки для этого есть. Достаточно, например, посмотреть на более чем солидный список имен компаний – основателей альянса ZigBee. Применение этой технологии на узком участке фронта – СКУД – лишь малая часть процесса по глобальному и стремительному внедрению беспроводных технологий во все, что нас окружает.

Возможно, через какое-то время от беспроводных СКУД откажутся совсем – но нам почему-то кажется, что такое вряд ли случится. Как не произойдет и полного погружения в беспроводность – СКУД, работающие «по воздуху» найдет свою нишу, где с ними не смогут конкурировать другие технологии. И как только это случится – появится достаточно большое предложение и на этом рынке. Еще один более чем реальный сценарий – появление беспроводных интегрированных систем безопасности. Конечно, видео по технологии ZigBee не будет передаваться никогда – зато беспроводная магистраль, развернутая для СКУД, вполне пригодна для систем охранно-пожарной сигнализации, учета рабочего времени, и для некоторых других.

Сегодня беспроводных СКУД существует всего несколько, и все они «импортного» происхождения. Отечественные разработчики пока не предлагают готовых решений, основанных на подобных идеях. Многие компании проводили оценку эффективности внедрения беспроводных технологий в существующие системы – поэтому ими рассматривался вопрос перевода в «беспроводное» состояние исключительно магистральных линий, а не всей СКУД.

Во многом – это особенность именно нашего рынка. Причем она лежит скорее в сфере особенностей менталитета инсталляторов и разработчиков, чем экономических или иных условий.

Все монтажные организации, с которыми мы сотрудничаем, любят провода,т.к. зарабатывают в основном именно на их прокладке. Соответственно, они очень осторожно настроены к любым решениям, которые лишают их этого заработка. Есть исключения, но они редки. Zigbee – технология, которая стала быстро известна разработчикам, но не потребителям или монтажным организациям. Люди живут своими старыми представлениями о радиоканале, им зачастую достаточно трудно объяснить преимущества Zigbee.

Но нам не привыкать действовать по принципу «догнать и перегнать» – ведь, как известно, у нас очень медленно запрягают...

ООО «Смарт Секьюрити Украина»
г.Киев
пер.Лабораторный, 1 оф. 271
тел.: (044) 592-92-25
тел./факс: (044) 529-33-99
e-mail: dm@smartsec.com.ua
www.salto.com.ua