сфератрэйд
сфера вашей безопасности

СКУД без проводов
от SALTO (Испания)

ОДО «Сфератрэйд»

Основной целью данной статьи является ознакомление специалистов отрасли с новой перспективной топологией организации полноценных беспроводных СКУД, базирующейся на протоколе беспроводной передачи данных IEEE 802.15.4, более известной как «технология ZigBee».

В последние несколько лет беспроводные технологии активно внедряются во многие системы безопасности — в частности, они весьма успешно используются в системах охранной и пожарной сигнализации. Причины — очевидны: беспроводные системы более предпочтительны как для конечных пользователей (повышается безопасность и надежность систем, не зависящих от перебитых или перегоревших проводов), так и для инсталляторов (установка систем не только значительно упрощается, но и увеличиваются возможности по расширению и наращиванию систем на функционирующих объектах).

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.

Существующие сегодня «классические» СКУД используют провода весьма широко, причем с абсолютно разными целями. Разделим все эти провода на три категории.

1. Магистральные каналы связи (чаще всего используются стандарты передачи данных по протоколам RS485 или IP). В эту же категорию отнесем еще и всевозможные конверторы и преобразователи интерфейсов (это хоть и не провода в чистом виде, но довесок, от которого тоже не лишним будет избавиться).

2. Провода для «обвязки» двери, т. е. шлейфы, соединяющие контроллер доступа со считывателями, исполнительными механизмами, датчиками, кнопками выхода и т. д.

3. Питающие линии считывателей, исполнительных устройств (как для контроллеров, так и периферии).

Такое классификационное деление проводов сделано намеренно, поскольку перевод каждого из трех типов в беспроводное состояние осуществляется 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 беспроводной радиоканал теоретически проще всего. Технологий для этого уже сейчас существует достаточно много — Wi-Fi, WiMAX, GSM, Bluetooth, ZigBee. Если в системе используются IP-контроллеры, то и выдумывать 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 невозможность их прокладки на конкретном объекте в большинстве случаев ограничивает количество помещений, оборудуемых СКУД (точек доступа). А при развертывании СКУД на уже функционирующем объекте именно прокладка этого «последнего метра кабеля» становится основной проблемой инсталляторов.

3. **Питающие линии.** Здесь также существует сложность. Единственная альтернатива — использование батарей или аккумуляторов. Однако с трудом можно себе представить размер (и стоимость) комплекта батарей, подходящий для работы магнитного замка сроком хотя бы на год-два без перезарядки или замены (частая смена батарей уничтожит перспективу применения такой системы для большинства пользователей из-за эксплуатационных расходов).

На первый взгляд нет никакой альтернативы. Однако у нас все еще остается возможность перевода магистралей в беспроводное состояние, а кабели по 2 и 3 пунктам можно оставить в таком же состоянии, без изменения. Но это будет уже не беспроводная СКУД.

Однако все перечисленные проблемы имеют решение, причем это известно достаточно давно.

Чтобы избавиться от проводов, нужно или применять сразу несколько беспроводных конверторов (что, как было указано выше, сводит на нет саму идею), или обнулить их длину. Т. е. комплект оборудования, куда входят контроллер, считыватель, датчик положения (если нужен), исполнительное устройство (замок) и т. д., должен превратиться в единое устройство — электронный замок. 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 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 поль-

зователь, нажимая на ручку замка. Благодаря такой схеме в электронных замках применяются микродвигатели с очень низким энергопотреблением.

Выбор технологии

Выбор технологии для организации беспроводного магистрального канала между электронными замками и сервером СКУД — принципиальная задача.

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, 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.

Этот стандарт описывает беспроводные персональные вычислительные сети (WPAN — Wireless Personal Area Network).

ZigBee — название набора протоколов высокого сетевого уровня, использующих радиопередатчики, 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). Скорость в этом канале — 250 кбит/с. Дальность передачи — от 10 до 100 м (в зависимости от отдаваемой мощности и окружающей среды).

> Благодаря технологии PoE (т. е. передаче питания прямо по витой паре) провода по обоим пунктам можно уместить в один кабель.

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 м при этом рассчитывать не стоит. Во-первых, эти параметры в большой степени зависят от конкретной реализации модуля и от состояния окружающей среды (толщина и тип стен, перекрытий и т. п.). Во-вторых, в заявленных 250 кбит/с немалую часть занимает 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 находятся несколько других технологий (те же Wi-Fi и Bluetooth). Из-за такого «соседства» в реальности вряд ли удастся спокойно использовать все 16 каналов, представленных протоколом.

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 совсем иная.

Во-первых, эти системы изначально создавались для использования в условиях отсутствия какой-либо магистрали, поэтому и в беспроводном варианте они выполняют весь базовый набор функций даже при условии полного «упадка» сети.

Во-вторых, сам принцип системы доступа здесь кардинально отличается от «классики». 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 в памяти контроллера, будучи ассоциированными с неким идентификатором, выданным на руки пользователю. Т. е. контроллеры электронных замков не должны хранить в своей памяти таблицу доступа со списком всех карт, которые надо «пускать», а только собственные параметры плюс реальные время и дата. 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. 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. 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.

Выше упоминалось, что радиомодули, работающие по стандарту IEEE 802.15.4, имеют ограничения по дальности. В реальных условиях это расстоя-

ния не более 20-40 м (мы, конечно, подразумеваем развертывание системы в помещении). Для организации нормальной СКУД в большинстве случаев такого расстояния 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 необязательно должна быть линейной — каждый шлюз (он, кстати, тоже совсем не обязательно должен быть только один на систему) может одновременно работать с 4 повторителями и 16 замками, каждый повторитель — еще с 4 другими повторителями и 16 замками. В итоге мы получаем древовидную топологию сети с множеством ответвлений.

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. Во-вторых, основная задача шлюза — производить стыковку беспроводной сети с обычной локальной сетью объекта. Т. е. шлюзы также используют провод, чтобы донести информацию до сервера.

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

Однако 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».

Система контроля и управления доступом SALTO RFID Wireless

Универсальная система. Допускает комбинацию в одной системе автономных и онлайн (IP) контроллеров с настенными считывателями, автономных и онлайн (беспроводных) электронных замков, электронных цилиндров.

Тип идентификаторов — бесконтактные перезаписываемые смарт-карты, отвечающие стандартам ISO 14.443A, ISO 14.443B и ISO 15.693 (Vicinity): MiFare, Desfire, ICODE, Legic, InsidePicoPass, HIDiClass, SKIDATA, совместимые с технологией NFC (Near Field Communication).

Тип оборудования точек доступа — контроллеры СКУД 3-х версий: автономные, онлайн (IP) и онлайн с функцией «виртуальная сеть SALTO». В системе применяются настенные считыватели для внутреннего и наружного применения, с клавиатурой или без нее.

Автономные и беспроводные онлайн-замки для любых дверей, в том числе для дверей эвакуационных выходов (с паник-баром).

Количество точек доступа — 64 000. Такое же количество возможных пользователей. Количество посетителей — неограниченно.

Глобальный (с записью отметки на ключ пользователя при входе и ее снятии при выходе или по истечении установленного времени) запрет двойного прохода. Возможность двойной идентификации. Возможность многоуровневой интеграции с другими системами. Виртуальная сеть SALTO: автономные замки могут записывать информацию на ключи пользователей (история проходов, состояние батарей и т. п.) — при проходе через онлайн-точку доступа (IP-контроллер) данные с ключа передаются в БД. Одновременно на ключ записывается обновление уровня доступа, срока действия ключа, черный список (метки утерянных ключей для внесения в память автономных замков) и т. д.

Андрей Катренко —
коммерческий директор компании
«Смарт Секьюрити»

Официальный дистрибьютор SALTO в Беларуси — ОДО «Сфератрэйд»
220035, Беларусь, г. Минск
ул. Тимирязева, 65А-516
+375 17 2269966
+375 29 6269966
+375 29 5269966
info@secur.by, www.secur.by

Александр Сушинский — инженер по системам контроля и управления доступом компании «Сфератрэйд»