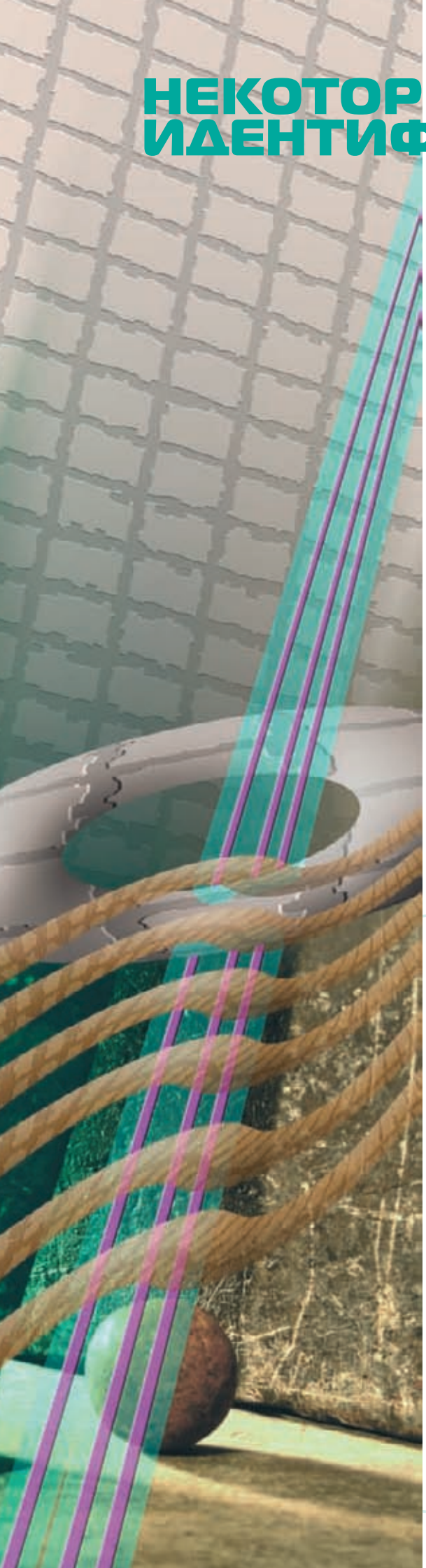


НЕКОТОРЫЕ ВОПРОСЫ ИДЕНТИФИКАЦИИ

Л. Стасенко
группа компаний «Релвест»

Любой театр начинается с вешалки, любая система контроля и управления доступом – с процесса идентификации пользователя. И процесс этот осуществляется с помощью считывателя и идентификатора (в случае применения биометрических технологий в роли идентификатора выступает сам пользователь). И хотя эти вопросы стары, как и применение СКУД, – начнем с основных определений и классификации.

Считыватель. Этим термином называют устройство, которое умеет получить код идентификатора и передать его контроллеру. В зависимости от принципов работы идентификатора меняется и технология считывания кода. Для «далласовской таблетки» это два электрических контакта, выполненных в виде «лузы», для proximity-карты – это уже достаточно сложное электронное устройство, а для считывания, например, рисунка радужной оболочки глаза в состав считывателя входит миниатюрная телевизионная камера.

Считыватель по определению должен быть доступен снаружи помещения, проход в которое необходимо получить. Отсюда и комплекс требований. Если считыватель устанавливается на улице (въездные ворота, наружная дверь здания), то, как минимум, он должен выдерживать суровые климатические нагрузки – жару и холод, снег и дождь. А если прилегающая территория не находится под присмотром, то еще потребуется и механическая прочность для устойчивости против любителей что-то поковырять гвоздем или подпалить зажигалкой.

Самыми вандалостойкими могут быть сделаны считыватели бесконтактных карт. Если сплошной корпус из нержавеющей стали кажется вам недостаточно защищенным, вы можете замуровать считыватель в бетонную стену или поместить его за слоем прочного пластика толщиной в пару сантиметров – при таком способе установки повредить считыватель без специального инструмента уже невозможно. А самому считывателю такая защита ничем не мешает – ведь он «видит» карту на расстоянии до 10 и более сантиметров.

Биометрические считыватели на сегодняшний день все еще сравнительно дороги, поэтому их применение должно быть обоснованным (либо реальной необходимостью, либо вашими амбициями). Кроме того, им свойственны еще некоторые недостатки:

- Сравнительно большое время идентификации – от десятых долей до единиц секунд. Для трафика на заводской проходной это может оказаться смертельным.
- Практически все они не рассчитаны на уличное применение.
- Считыватели отпечатков пальцев вызывают у людей некоторый дискомфорт, хотя, по правде сказать, ни один из современных дактилоскопических считывателей не хранит сами отпечатки пальцев, а только некую их математическую модель, по которой отпечаток не восстанавливается.
- Достоверность распознавания человека по биометрическим признакам долго еще будет отличаться от единицы, что также может создать определенные неудобства. Либо вы периодически будете получать отказ в доступе, либо порог «узнавания» придется снизить до величины, при которой вероятность пропуска «чужого» станет достаточно большой.

Отдельно можно упомянуть считыватели большой дальности (с расстоянием идентификации до нескольких метров и более). Такие системы удобны на автомобильных проходных, на въездах на стоянки. Идентификаторы для таких считывателей, как правило, активные (т.е. используют встроенную батарейку), поэтому немаловажной является возможность замены батарейки через 3-5 лет. К сожалению, многие импортные системы данного типа не предусматривают смену батарейки, а это значит, что по истечении срока ее работы вам придется снова за каждый новый идентификатор заплатить 20-30 долларов (для сравнения: новая литиевая батарейка стоит обычно не больше доллара).

Считыватели можно классифицировать по следующим основным параметрам:

- Технология считывания:
  - Контактные – магнитная полоса, wiegand, штриховой код
  - Бесконтактная (активная и пассивная) – инфракрасный оптический, proximity (включающий smart-карты), vicinity (средней дальности)
  - биометрические – по отпечаткам

пальца, по сетчатке, по радужной оболочке, по контуру руки, по изображению лица и т.д.

– Активные системы дальней идентификации.

- Выходной интерфейс (разновидности wiegand, RS-232 или RS-485, Ethernet – используется в биометрических считывателях и считывателях дальней идентификации, «фирменный» (или proprietary) протокол, I-Button – это однопроводный интерфейс от Dallass).
- Рабочая частота (стандартные значения 125 кГц, 13.56 МГц, 800-900 МГц, 2.45 Ггц для систем дальней активной идентификации). В США вместо 125 кГц используют 134 кГц.
- Дальность считывания. Актуально для бесконтактных считывателей и считывателей дальней идентификации.
- Поддерживаемые форматы карт (идентификаторов). Для бесконтактных наиболее популярны и известны (примерно в порядке убывания популярности) HID, Motorola, EM Marin, CheckPoint, есть и другие. Для smart-карт есть стандарт ISO14443-A или ISO14443-B, для средней дальности (vicinity) – ISO 15693, у HID есть свои карты I-Class, частично совместимые с другими smart-картами. Все другие форматы являются не массовыми, а скорее экзотикой, по крайней мере для нашего рынка.

Естественно, выше перечислены не все варианты, а в качестве примеров – наиболее ходовые.

Идентификатор. В любой СКУД имеется некий идентификатор (ключ), который служит для определения прав владеющего им человека. Это может быть «далласовская таблетка», широко используемая в подъездных домофонах, бесконтактная (или proximity) карточка или брелок, карта с магнитной полосой (сейчас практически не используется). Кроме того, в качестве идентификатора может использоваться код, набираемый на клавиатуре, а также ряд биометрических признаков человека – отпечаток пальца, рисунок сетчатки или радужной оболочки глаза, трехмерное изображение лица.

Карту или брелок можно передать, их могут украсть или скопировать. Код можно подсмотреть или просто сказать кому-то. Биометрические признаки передать или украсть невозможно (хотя Голливуд считает иначе), но некоторые из них все же подделываются без больших трудозатрат – в частности, те же отпечатки пальцев.

Тип используемого идентификатора во многом определяет защищенность системы от злоумышленников. Например, любой школьник-радиолюбитель по приводимым в Интернете описаниям может легко сделать имитатор «далласовской таблетки», а хранящийся в ней код всегда отштампован на обратной стороне.

Бесконтактные карты или брелоки, стандартно используемые в системах доступа, подделываются немного сложнее, но также не защищены от этого. Сегодня есть карточки с высоким уровнем защищенности (используются мощные схемы криптографирования, ключи для шифрования может назначать сам пользователь), но в нашей стране в стандартных СКУД эти решения, как ни странно, пока применяются мало.

Биометрические признаки подделать сложнее всего (а среди них отпечатки пальцев – проще всего). Вообще, там, где требуется высокий уровень защищенности от взлома, как правило, используют одновременно несколько идентификаторов – например, карточку и код, отпечаток пальца и карту или код.

Независимо от выбора идентификатора соблюдайте те же правила, что и для обычных механических ключей – берегите их от посторонних и старайтесь не терять. Правда, если вы потеряли механический ключ, то рекомендуется сменить замок или, как минимум, личину. В случае электронных идентификаторов утерянный «ключ» просто надо вычеркнуть из списка разрешенных, что намного проще и дешевле.

При выборе типа идентификатора имейте в виду следующее:

- В системе может быть единственная точка прохода (например, турникет на входе в здание), а пользователей может быть несколько сотен. В этом случае цена идентификатора, помноженная на количество, может превысить стоимость всего оборудования. А если учесть, что их теряют и ломают, то это запланированные затраты и на будущее.

В такой ситуации оптимальное решение – стандартная proximity-карта, цена которой сегодня уже менее 1 у.е., а с точки зрения удобства использования равной ей не найти.

- Желательно, чтобы выбранные вами идентификаторы были широко доступны на рынке (т.е. чтобы они производились не единственной в мире компанией, а имели бы клоны). Это залог того, что и через несколько лет вы сможете докупать нужное количество ключей.
- Если вы хотите использовать биометрический идентификатор, то не стоит использовать такую систему на точке прохода с большим трафиком (например, на проходной завода) – результатом будут очереди перед входом, а реальной пользы вы не получите. Хотя на хранилищах и других ответственных помещениях биометрический считыватель может оказаться уместным.

Идентификаторы можно классифицировать по следующим параметрам (часть из них совпадает со считывателями, поскольку они всегда работают в паре):

- Технология считывания.
- Рабочая частота.
- Формат (HID, …).
- Дальность считывания.
- Конструкция (карта, брелок, другое).

На сегодняшний день самой распространенной технологией идентификации является радиочастотная – RFID – Radio Frequency Identification, которая имеет уже примерно двадцатилетнюю историю. Основные типы идентификаторов, функционирующие в рамках данной технологии: карты, брелоки, таблетки, метки.

Именно в связи с подавляющим приоритетом RFID в СКУД остановимся на особенностях построения процесса радиочастотной идентификации.

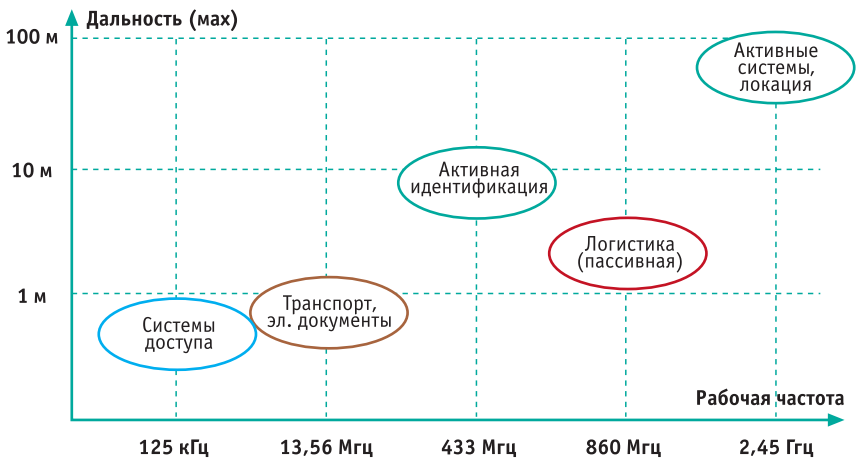
ТЕХНОЛОГИИ И СТАНДАРТЫ

Не вдаваясь в историю вопроса – этой теме посвящено огромное количество материалов как в печатных изданиях, так и в Интернете – посмотрим, каким арсеналом располагает технология RFID сегодня. Для этого дадим еще раз краткую классификацию по нескольким ключевым критериям, поскольку все многообразие имеющихся в мире решений никак не укладывается в линейной или одноранговой классификации. Иллюстрацией к нижеследующей классификации может служить *рисунок 1*.

Рабочие частоты

Существует пять основных частотных диапазонов, закрепленных различными стандартами за технологией RFID. Сразу заметим, что некоторые из частот, такие как

Рис. 1. Классификация систем RFID



13,56 МГц, 2,45 ГГЦ, едины для всех стран. В то же время в низкочастотном диапазоне в некоторых странах вместо 125 кГц используется частота 135 кГц. В СВЧ-диапазоне стандарты также различны для Европы и России (860 – 870 МГц), Америки (902 – 908 МГц) и Японии (950 – 956 МГц).

Также различны и максимальные разрешенные мощности излучения считывателей, что определяет максимальную дальность чтения меток, в первую очередь максимально дешевых пассивных.

Наименее распространенный частотный диапазон – это 433 МГц. Для него производятся системы активной идентификации всего несколькими компаниями в мире. Возможно, это связано с тем, что 400-мегагерцевый диапазон (также для разных стран имеющий разные стандарты в диапазоне от 430 до 460 МГц) настолько сильно «замусорен» беспроводными системами охранной сигнализации, переносными радиостанциями и автомобильной сигнализацией, что гарантировать нормальную работу систем RFID просто сложно. В России системы дальней идентификации в основном используют нелицензируемый диапазон 2,4 ГГц.

И замечание для наших читателей. Долгие годы все системы RFID формально были в России вне закона. И только в течение последнего года частотные диапазоны для RFID были в нашей стране узаконены (последние решения ГКРЧ по этому вопросу датированы 7 мая 2007 года). К сожалению, открытым пока так и остался вопрос разрешенных мощностей для ряда частотных диапазонов, что являет собой существенный пробел в законодательной базе.

Дальность идентификации

Дальность идентификации для пассивных систем зависит от нескольких основных факторов: частотного диапазона, мощности излучения считывателя и размеров антенн считывателя и метки.

Для активных систем зависимости несколько отличаются и приобретают дополнительные факторы, например, метод модуляции сигнала и ширина спектра.

Максимально достижимые дальности идентификации при реальных размерах антенн считывателей и меток (для меток это примерно размер стандартной кредитной карты) приведены *в таблице 1*.

Для систем активной идентификации, особенно в СВЧ-диапазоне, понятие размера антенны становится достаточно условным понятием, и приведено больше для оценки габаритов считывателя.

Активная или пассивная?

Как видно из таблицы, системы активной идентификации имеют на два порядка большие дальности чтения меток. Это и понятно – в пассивной системе считыватель должен «донести» до метки достаточное для работы микросхемы метки количество энергии, в то время как в активной системе метка имеет собственный источник питания, а дальность при этом определятся уже другими факторами.

Из принципов и конструкции активных и пассивных меток вытекает другое их различие – разница в стоимости, которая также составляет от одного до двух порядков. Как говорится, «за все надо платить»…

При использовании активных систем следует обращать внимание на конструкцию меток, ведь если не через год-два, то уже лет через пять батарейка в метке прикажет долго жить – и что тогда? Многие популярные в России системы активной идентификации зарубежного производства имеют неразборные конструкции, и при «погибшей» батарейке придется менять все метки на новые. Производителя таких меток понять можно – они готовят себе рынок на перспективу, потому что обещанные пять лет многим при покупке системы кажутся вечностью. Но, к сожалению, это время пролетает слишком быстро, и вы все равно оказываетесь перед необходимостью заплатить примерно по 25 у.е. за каждую метку…

Не так давно бывший Philips, а ныне NXP, разработал дешевый чип стандарта ISO-14443A для транспортных карт для использования в качестве билетов на одну или несколько поездок. Сегодня в московском метро можно спокойно набрать нужное количество «отработанных» билетов UltraLight и использовать их в системе доступа или других приложениях идентификации, поскольку они по-прежнему имеют уникальный серийный номер, который и требуется для процедуры идентификации. Невозможно использовать только их «электронный кошелек».

КЛАССИФИКАЦИЯ ПО ПРИКЛАДНЫМ ЗАДАЧАМ

Рассмотрим наиболее «тиражируемые» решения на основе технологии RFID (без расстановки приоритетов).

Идентификация в СКУД

В данных приложениях самыми популярными являются карты с рабочей частотой 125 кГц. Существует несколько распространенных и несовместимых друг с другом форматов, среди которых наиболее известны HID, Indala (Motorola) и EM Marin (сокращенно EM). Первые два формата лет 10 назад практически доминировали на рынке СКУД, однако сейчас самым массовым является формат EM Marin, поскольку он изначально был открытым, и сегодня карты данного формата производятся десятками компаний, а количество производителей считывателей вообще трудно поддается учету. При всех прочих равных условиях (да простят меня поставщики карточных брэндов) карты EM в несколько раз дешевле.

Постепенно начинают отнимать свою долю рынка СКУД карты диапазона 13,56 МГц. Они несколько дороже карт EM и примерно равны по стоимости картам именитых производителей, однако имеют ряд преимуществ:

- Эти карты многофункциональны и в системах доступа могут использоваться «попутно», параллельно с использованием, например, в локальных платежных системах.
- Данные карты позволяют использовать различные криптоалгоритмы, что полностью защищает канал обмена «карта-считыватель» от любой попытки имитации (подделки), что бывает немаловажным для серьезных объектов.

Считыватели для диапазона 125 кГц обычно имеют дальность чтения 10-15 см (хотя доводилось видеть и такие, по которым надо буквально «тереть» картой, чтобы она прочиталась – слава нашим умельцам!). В небольшом количестве представлены считыватели, имеющие дальность чтения от 40 до 70-90 см.

Дальняя идентификация (например, автотранспорта на автомобильных проходных, парковках и т.д.) реализуется, как правило, на активных системах диапазона 2,45 ГГц.

Транспортные системы

В данной прикладной области (примером может служить Московский метрополитен) применяются карты диапазона 13,56 МГц стандарта ISO-14443A. Известно также другое название этих карт – Mifare®. Во всем мире используются уже сотни миллионов таких карт, при этом больше всего их в Юго-Восточной Азии (в основном Китай), а меньше всего – в США.

Идентификация животных

Это достаточно старое (как и системы доступа) применение RFID, не получившее, однако, пока распространения в нашей стране. Используется тот же низкочастотный диапазон 125 кГц, но для данной области существуют свои отдельные стандарты обмена меток со считывателями.

Технологические процессы

В последние годы технология RFID начинает интенсивно использоваться в производственных процессах для автоматического отслеживания прохождения изделий в технологических процессах.

Наиболее часто используются метки стандарта ISO-15693 (частота 13,56 МГц), а

Табл. 1

ДИАПАЗОН	РАЗМЕР АНТЕННЫ	МАКСИМАЛЬНАЯ ДАЛЬНОСТЬ	ПРИМЕЧАНИЕ
125 кГц	100 x 50 см	60–80 см	Пассивная
13,56 МГц	100 x 50 см	80–120 см	Пассивная
433 МГц	10 x 10 см	20–100 м	Активная
800–900 МГц	20 x 20 см	200–400 см	Пассивная
2,45 ГГц	10 x 10 см	10–150 м	Активная

в последнее время и метки EPC (частоты 800-900 МГц), которые обеспечивают большую дальность идентификации при меньших размерах считывателей.

Электронные документы

Это еще одно широкое поле для применения RFID. Появление смарт-карт с мощными встроенными микроконтроллерами, большими объемами памяти и аппаратными криптопроцессорами позволяет сегодня использовать их в различных электронных документах – визах, миграционных картах, водительских удостоверениях, паспортах граждан и т.д. В основе всех таких документов – карты (или чипы) стандарта ISO-14443.

Банковские системы

Еще одна область применения защищенных карт стандарта ISO-14443 – банковские или кредитные карты. С появлением бесконтактных смарт-карт безопасность такой формы оплаты выросла на порядки.

Несколько лет назад три крупнейшие платежные системы – EuroPay, MasterCard и Visa – выработали общую концепцию перехода на чиповые карты. По первым буквам имен членов альянса концепцию назвали «EMV – миграция». Процесс этот уже начался, количество эмитированных карт растет с каждым годом, однако окончательный переход на новые карты – пока еще дело будущего: слишком велики затраты в инфраструктуру (одна смена считывателей во всех банкоматах мира чего стоит!).

Несостоявшийся бум, или Маркировка грузов

Примерно 4-5 лет назад появились очень оптимистичные прогнозы в части развития рынка автоматической идентификации применительно к цепочкам поставок и системам оптовой и розничной торговли. Достаточно быстро был разработан и утвержден стандарт EPC (Electronic Product Code), который позволял использовать действительно максимально дешевые RFID-метки (в ущерб их функционалу). И именно усеченный функционал метки давал простор для деятельности лидеров информационных технологий (далеких, в общем-то, от RFID), поскольку в этом случае ставка делается на сетевую инфраструктуру и мощные сервера, необходимые для хранения баз данных товаров мирового масштаба с возможностями оперативного доступа из любой точки мира.

Поставщики крупнейших торговых сетей были обязаны уже с 2005 года поставлять товары с маркировкой метками EPC, производство меток в массовых количествах были развернуты в Юго-Восточной Азии.

Но опять жизнь внесла свои коррективы: все, что хорошо работало в лабораторных условиях, не всегда обеспечивало достоверные результаты в реальной жизни. Для решения возникших проблем стандарт существенно доработали, новый стандарт получил название EPC Gen2 (вторая генерация), но метки с доработками опять несколько поднялись в цене.

Таким образом, система глобальной логистики существенно замедлила темпы своего роста и обещанный бум с приростом объемов в данной сфере по 25…30% в год пока не состоялся.

НОВЫЕ НАПРАВЛЕНИЯ

Решения в области активной идентификации

Из замеченных в последнее время тенденций можно отметить рост количества новых продуктов в области дальней активной идентификации в диапазоне 2,45 ГГц. Объясняется это достаточно просто – развитие внутриофисных и домашних беспроводных коммуникаций привело к появлению в больших количествах новой элементной базы, причем с разумными ценами. Ряд компаний быстро выпустили на рынок считыватели и метки на базе трансиверов, разработанных для wireless технологий связи, однако эти решения не всегда применимы в реальной жизни. Дальняя идентификация всегда привносила свои проблемы в СКУД, поскольку с ростом дальности размывается граница зоны чтения, и еще большая проблема возникает при попытке определить направление прохода или проезда.

Вместе с тем адекватные решения в этой области уже появились на российском рынке, и считыватели СКУД с дальностями до 30-50 м – это уже серийный продукт.

Системы позиционирования

Необходимость повышения уровня автоматизации во всех сферах привела к появлению новых решений в области активной дальней идентификации. Как для офисных приложений (СКУД, системы управления персоналом), так и для многих других задач (мониторинг контейнеров на площадках хранения, автомобилей на стоянках) возникает потребность в определении местоположения маркированных объектов в реальном времени. И эта задача уже имеет несколько решений.

Базируются такие решения на оборудовании для частотного диапазона 2,45 ГГЦ, который в последние годы стал наиболее популярным во всех областях – от коммуникаций до беспроводных охранных систем.

Точность позиционирования составляет около метра на открытых пространствах и примерно не хуже 3 м в помещениях – результат, который для многих реальных задач вполне приемлем.

Охранные системы и домашняя автоматика

Здесь мы уже плавно уходим от темы RFID в сторону беспроводных коммуникаций, но это вполне закономерно, поскольку четкой границы нельзя провести уже сегодня. Просто нельзя не упомянуть еще одну сравнительно новую технологию (или, точнее, стандарт беспроводных коммуникаций) – это ZigBee. Родившись в недрах Freescale, подразделении Motorola, эта технология получила всеобщее признание, и некоммерческий альянс ZigBee сегодня поддерживается практически всеми крупными производителями как элементной базы (трансиверы и микроконтроллеры), так и производителями конечного оборудования.

Стандарт разрабатывался для беспроводных локальных сетей разного рода датчиков и простых исполнительных устройств с небольшим информационным трафиком и минимальным энергопотреблением для обеспечения работы от батареек. Естественно, датчики могут быть и охранными или пожарными, поэтому следует ожидать миграции беспроводных охранных систем из диапазона 430-460 МГц в более высокочастотный диапазон 2,45 ГГц.

Конечно, частные решения в этом же диапазоне могут оказаться более оптимальными по ряду параметров (например, по энергопотреблению), но наличие данного стандарта и его повсеместная поддержка открывают широкую дорогу именно решениям на основе стандарта, обеспечивая совместимость оборудования множества производителей, что очень важно в конечном итоге и для потребителей.

Премия компании «Тензор»

Редакция журнала «Алгоритм безопасности» поздравляет компанию «Тензор» с получением одной из престижных премий в области безопасности «За укрепление безопасности России (ЗУБР) 2008» в категории «Пожарная безопасность», номинация «Новинка года» за грамотное, оригинальное и простое решение, реализованное в устройстве для самотушения горящих жидкостей УСП-01Ф. Устройство разработано специалистами «Тензора» совместно с ФГУ ВНИИПО МЧС РФ на основе результатов экспериментальных и теоретических исследований проблемы тушения пожаров, связанных с горением легковоспламеняющихся и горючих жидкостей. УСП-01Ф имеет опыт применения на зарубежных и российских атомных станциях.

НОВОСТИ