Современные ключи и идентификаторы систем кодового доступа

Андрей Кашкаров (Санкт-Петербург)

В статье описаны технические характеристики и варианты практического применения систем безопасности на основе смарт-карт. Использование карточных ключей – носителей информации – обеспечивает надёжную охрану зданий, помещений и автомобилей при минимальных затратах на установку систем.

Введение

Сегодня проблемы обеспечения безопасности граждан и государства, персональных и общественных секретов не потеряли свою актуальность: чем больше секретов, тем больше желания и возможностей их раскрыть. Подтверждением тому являются как разнообразные системы кодирования и передачи данных, так и устройства, перехватывающие и дистанционно декодирующие эту информацию. Простейший пример – подделки бесконтактных карт, в том числе с банковскими приложениями.

Строение смарт-карт, их возможности, технические характеристики и варианты практического применения различных систем безопасности на основе «меток» (ключей) и считывающих устройств (ридеров) описаны в предлагаемой статье.

Контактные, бесконтактные и комбинированные смарт-карты

Смарт-карта (smart-card, proximity, ProxCard, метки, транспондеры) – это, прежде всего, носитель информации. Электронные технологии, встроенные в смарт-карты (далее СК) и связанное с ними оборудование, ускорили процедуры аутентификации и, как следствие, последующие действия: проведение платежа, отказ от обслуживания, пропуск на объект или ограничение доступа и др.

Системы кодового доступа начали широко использоваться не так давно. Кодовые замки (механические и с применением электроники), «нагруженные» на электромагнитные замки (соленоиды, соединённые с дверной защёлкой) были весьма популярны в 1970–1990-х годах. Чтобы открыть такой замок требовалось ввести последовательность цифр. Очевидно, такие замки не являлись панацеей от несанкционированного проникновения. Кроме того, в эру ТТЛ- и КМОП-микросхем в DIP-корпусах электронные устройства нельзя было оперативно перепрограммировать.

С развитием микроэлектроники, микропроцессоров и персональных компьютеров (ПК) появились новые устройства кодового доступа. Они были весьма разнообразны – от набора кодовой комбинации (логина и пароля) посредством клавиатуры, до брелока – ключа с USB-разъёмом, который являлся идентификатором пользователя ПК или программного обеспечения. Разновидностью такого кодового устройства являлся считыватель (сканер) папиллярных линий с пальца пользователя.

Некоторые из описанных выше систем применяются до сих пор. Но наряду с ними появились устройства намного более эффективные и защищённые, а также приборы, которые могут копировать метки/ключи (что делает защиту весьма уязвимой).

Контактные кодовые устройства типа ibutton (см. рис. 1) широко применяются в бытовых приложениях, домофонах и других относительно простых системах доступа. «Таблетки» iButton имеют встроенную энергонезависимую память объёмом от 256 бит до 8 кбайт (см. табл. 1). Считыватели карт iButton оснащены 2 контактами из нержавеющей стали. Производство таких считывателей может быть организовано практически везде. Метки iButton не боятся прямого попадания влаги. Отдельные модели обладают дополнительными свойствами. Например, прибор DS1991 (объём памяти 1 кбит) имеет защиту памяти паролем, DS1963S (4 кбит) позволяет реализовать дополнительные методы активной аутентификации. Интерфейс карт iButton описан в литературе и позволяет соединять несколько считывателей в единую двухпроводную сеть.

Примерно в то же время появились новые носители информации в различном исполнении: на основе картона, пластика, пластиковых брелоков, полупроводниковых кристаллов, вживляемых в органическую ткань. В отличие от iButton, карты-метки (СК) на пластиковой и особенно бумажной основе боятся влажности. Карта со встроенным микроконтроллером, содержащим процессор, память и интерфейс ввода-вывода, работает под управлением встроенной операционной системы (ОС). Форма карты, контактов, их расположение и назначение регламентированы стандартами ISO/IEC 7816 и ISO/IEC 7810.

Бесконтактные СК (БСК) более удобны, они могут срабатывать на расстоянии до 10 см от ридера (для надёжного взаимодействия между меткой и ридером достаточно воздушного зазора в 3...5 см). БСК содержат микроконтроллер и антенну, передача данных осуществляется (в зависимости от стандарта) на частоте 125 кГц или 13,56 МГц (в коммуникационных системах на основе технологий ближнего поля). Стандарты описаны в спецификациях ISO 18902, ISO 7816, ISO 14443 варианты A и B (реже ISO/IEC 15693), EMV (Europay, MasterCard, Visa), IPC/JEDEC J-STD-020C, ECMA 340, ETSI TS 102190 и др.

Автор рекомендует внимательно ознакомиться с описанием стандарта ISO 7816, в котором прописаны требования к конструкции и технологии обмена цифровыми данными для контактных СК (на основе контактных кристаллов) и ISO 14443A и 14443B – для бесконтактных карт. Дополнительная информация изложена на интернет-странице http://www.smart-park.ru/index.php/products/smartcards.htm. Там же приведены технические характеристики наиболее популярных микроконтроллеров, которые могут пригодиться разработчикам и пользователям систем безопасности и кодового доступа. Системы, работающие на основе технологии Java, регламентированы стандартами Java Card 2.1.1 и выше.

Если СК оснащены одновременно и контактным (кристалл), и бесконтактным интерфейсом, их называют дуальными. Комбинированные СК

Рис. 1. Метка-таблетка iButton

Рис. 2. Разобранная карта стандарта EM Marine

Рис. 3. Внешний вид меток в различном исполнении

(комби-карты) имеют два или несколько микроконтроллеров – встроенных микросхем. В бесконтактных смарт-картах применяется технология RFID (Radio Frequency IDentification, радиочастотная идентификация) – способ автоматической идентификации объектов, при котором посредством радиосигналов считываются или записываются данные, хранящиеся в метках. Основными направлениями развития технологий RFID с использованием бесконтактных пластиковых карт являются:

- контроль доступа и учёт рабочего времени на предприятиях;
- платный доступ на автомобильные парковки, подъёмники, аттракционы и т.д.;
- платежи за пользование общественным транспортом;
- замена или дополнение банковских и дисконтных карт с магнитной полосой.

Инициализация СК происходит с помощью системы контроля удалённого доступа (СКУД).

Карты на основе пластика и картона

Существуют три основных стандарта карт: Mifare, EM Marine и HID. Первый хорошо защищён, но главное его отличие от EM Marine, который разработан раньше, состоит в возможности записи на метку (носитель, карту, идентификатор, ключ) дополнительной информации. Карта EM Marine не имеет памяти для хранения информации, поэтому не перезаписывается. Стандарт носителя определяется микросхемой (микроконтроллером). На рисунке 2 представлен вид разобранной карты стандарта EM Marine.

Сегодня имеют хождение СК всех трёх стандартов в различных исполнениях (пластиковая карта, в том числе с прорезью для крепления, брелок, таблетка, в том числе прорезиненный «наручный» браслет с меткой – для эксплуатации в условиях водной среды и большой влажности). Карты всех стандартов можно визуально отличить друг от друга по некоторым признакам. Например, карта EM Marine имеет на поверхности набор цифр – уникальный номер (см. рис. 3 справа вверху), в то время как более защищённая карта (с теми же типоразмерами) Mifare не содержит никаких надписей.

При длительной эксплуатации цифры на пластике постепенно стираются. Карта стандарта HID (или ProxCard II) тоже может иметь на пластиковом носителе набор цифр, но отличается наклейкой на лицевой стороне «HID»; с обратной стороны пластика та же аббревиатура нанесена методом тиснения. Это – главное отличие одинаковых по внешнему виду карт с габаритными размерами стандарта Clamshell. Типоразмер СК и БСК определяется стандартом ISO/IES 7816-2.

С ключами в ином исполнении (браслеты, брелоки и др.) дело обстоит сложнее из-за меньших возможностей поместить и прочитать надписи. Карты (метки в других исполнениях) отличаются друг от друга и радиочастотой, на которой происходит взаимодействие с ридером. Рассмотрим некоторые примеры.

Метки стандарта Mifare

Брелок стандарта Mifare используется в дисконтных, платёжных и транспортных системах. Корпус обшит натуральной кожей, на брелок можно нанести логотип (см. рис. 3 слева). Метка допускает шифрование данных и обеспечивает до 100 000 циклов перезаписи. Она отличается от меток своего класса повышенной скоростью транзакции (быстродействием), измеряемой в миллисекундах. Объём внутренней памяти составляет 1024 байт. С данной метки невозможно сделать копию простым перезаписыванием информации (приложив к считывателю с запоминанием кода). Сохранение данных памяти до 10 лет – общая характеристика меток этого класса.

Технические характеристики ключа-метки модели IL-07MK фирмы IronLogic стандарта Mifare:

- микросхема Mifare S50;
- рабочая частота 13,56 МГц;
- тип карты – чтение/запись;
- время транзакции 164 мс;
- объём памяти 1024 байт;
- материал корпуса – натуральная кожа;
- цвет – чёрный;
- габаритные размеры 40,0 × 40,0 × × 5,5 мм;
- диапазон рабочих температур –30...+50°C.

Метки стандарта EM Marine

Карта IL-05ELR стандарта EM Marine (производитель IronLogic) с проре-

Таблица 1. Технические характеристики некоторых устройств iButton

Код прибора	Объём памяти, бит	Дополнительные возможности
DS1971	256+64, ЭППЗУ	
DS1973	4K, ЭППЗУ	
DS1991	1344, энергонезависимое ОЗУ	Защита памяти паролем
DS1992	1K, энергонезависимое ОЗУ	
DS1993	4K, энергонезависимое ОЗУ	
DS1994	4K, энергонезависимое ОЗУ	Часы
DS1995	16K, энергонезависимое ОЗУ	
DS1996	64K, энергонезависимое ОЗУ	
DS1963S	4K, энергонезависимое ОЗУ	Усиленная аутентификация, счётчик циклов записи
DS1963L	4K, энергонезависимое ОЗУ	Счётчик циклов записи

Все приборы имеют уникальный номер, 64 бита

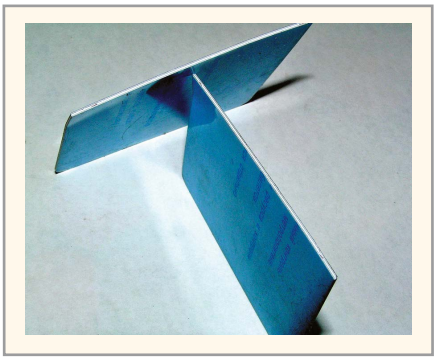

Рис. 4. Вид БСК с торца

зью для крепления имеет повышенную дальность считывания данных (на 50–70% относительно обычной карты данного стандарта). Эти сведения предоставлены разработчиками и подлежат проверке. На БСК нанесён её уникальный номер, что может упростить поиск в базе данных при отсутствии считывающего устройства. Для персонализации карты можно использовать наклейку (см. рис. 3).

Технические характеристики идентификатора IL-05ELR IronLogic стандарта EM Marine:

- микросхема EM Marine;
- рабочая частота 125 кГц;
- тип карты – только чтение;
- формат печати ID – xxx, xxxxx;
- материал корпуса – пластик ABS;
- цвет корпуса – белый, серый, зелёный, синий;
- габариты (Д × Ш × Т) 86,0 × 54,0× 1,6 мм;
- диапазон рабочих температур –30...+55°С.

Карта идентифицируется по системе Wiegand 26 с рабочей частотой 125 кГц в соответствии с протоколом DS1990A. Разумеется, существуют карты аналогичного типоразмера в стандарте Mifare, оснащённые функционалом чтение/запись, например, IL-05M фирмы IronLogic, которая имеет функции шифрования и антиколлизии, возможность перезаписи до 100 000 циклов и долговечность до 10 лет.

Метки стандарта Temic как аналог EM Marine

В качестве разновидности БСК стандарта EM Marine существуют метки стандарта Temic – RFID-карты для записи и копирования уникального номера. Они имитируют карты стандарта HID ProxII, EM Marine и других, но работают в диапазоне частот 100–150 кГц.

Карта IL-05T той же фирмы IronLogic оснащена кристаллом T5557 и работает на частоте 125 кГц. Реализуя стандарт EM Marine, метка Temic, однако, снабжена, функционалом чтение/запись и не имеет напечатанного на пластике набора символов. По внешнему виду отличить такую карту от Mifare практически невозможно. Именно поэтому нанесение идентификационного символьного кода на сам пластик является важным отличительным признаком. Например, карту IL-06E IronLogic с микросхемой EM Marine, функционирующую на частоте 125 кГц, также нельзя отличить от IL-05ELR по внешним признакам, хотя она содержит другой микроконтроллер.

Все карты внутри одного стандарта взаимозаменяемы: карта EM Marine ISO IL-06E можно заменить картой IL-05ELR, а карту IL-06M IronLogic Mifare ISO – IL-05M IronLogic.

Комбинированные метки

Особый (комбинированный) тип – это БСК того же типоразмера IL-06 E&M IronLogic ISO с 2 кристаллами EM Marine + Mifare 1K. Карта может работать с системами сразу двух стандартов, причём заготовка такой карты стоит всего на 20 рублей дороже. Комбинированная карта полезна в тех случаях, когда на одном объекте установлены считыватели разных стандартов.

Технические характеристики двухкристальной карты IL-06 E&M IronLogic ISO:

- микросхема EM Marine + Mifare1K;
- рабочая частота 125 кГц + 13,56 МГц;
- тип карты – только чтение + чтение/запись;
- материал корпуса – ПВХ.

Существуют различные по типу метки с «открытым» корпусом (для наполнения). Это означает, что в защищённый от влаги прорезиненный корпус можно установить любой из кристаллов серий EM4100, EM4102, MF1S50, MF1S70, MF Ultralight, T5557, I-Code I, I-Code II, чтобы использовать в устройствах соответствующего стандарта.

Бесконтактная СК представленного форм-фактора поддерживает несколько функций (карта доступа, банковская карта, идентификационная метка и др.).

Конструкция и элементная база карт

Антенна, как правило, выполнена металлизированными дорожками в виде нескольких спиральных кругов по периметру основы карты (иногда в центре) – пластика или картона. На рисунке 4 антенные дорожки видны на торце пластика.

Обратимся также к рисунку 2, на котором видно внутреннее устройство БСК. Карты, в которых кристалл выведен на поверхность и предназначен для электрического контакта с устройством считывания данных, имеют свои отличия. Кристалл представляет собой микропроцессор со встроенной операционной системой и памятью небольшого объёма (до сотен килобайт). В разное время выпускались 8-, 16- и 32-разрядные микропроцессоры, что определяет и объём внутренней памяти БСК. Самый популярный в своё время кристалл – AE55C1 производства компании Renesas Technology, был 32-разрядным. Память такого кристалла составляла десятки килобайт.

Другой популярный микропроцессор – ST19WR66 производства компании ST Microelectronics содержит ПЗУ объёмом 224 кбайт, что обеспечивает хранение операционной системы вместе с программой шифрования данных по стандарту ISO 14443B. Такой кристалл имеет энергонезависимую память, которая используется ОС для хранения персональной информации владельца, включая биометрическую. Именно на основе подобных микросхем (с большим объёмом памяти) реализованы «электронные» паспорта, срок действия которых ограничен 10 годами.

Более совершенное устройство, реализованное на основе микроконтроллера AE55C1 с масочным ПЗУ, имеет полезный объём памяти 240 кбайт и позволяет повысить плотность хранения кодов и данных по сравнению со «старыми» микросхемами Renesas Technology, ориентированными на БСК без банковского приложения.

Объём памяти и новые технологии

Относительно новая версия ОС для семейства микропроцессоров JCOP31 компании IBM поддерживает стандарты шифрования данных AES и ESS (последний обеспечивает повышенный уровень защиты с ключом малой длины). Увеличить объём памяти до 1 Мбайта удалось с помощью разработки кристаллов для БСК с флэш-памятью. Практически, можно сделать одну карту (один пластик) многофункциональным инструментом: электронным пропуском, корпоративным удостоверением и картой с банковским приложением. Возможности конфигурации различных приложений в карте с таким объёмом памяти весьма велики. Удобно и добавлять

новые функции в уже выпущенную карту. В качестве примеров можно упомянуть корпоративные «бейджики», «телефонные» карты или недавно выпущенную ФГУП «Почта России» совместно с ОАО КБ «Русский стандарт» почтовую/кредитную карту «Любимый клиент», на которую начисляются баллы за покупки на почте (ими можно рассчитываться вместо денег). В такие карты можно записывать и биометрические данные, если позволяют возможности кристалла.

Защита данных

Традиционные технологии шифрования данных не ограничиваются AES (Advaced Encryption Standard), SHA (Secure Hash Algorithm) и американской FIPS (Federal Informaion Processing Standards), описание которых не входит в задачи данной статьи. Однако следует упомянуть технологию NFC – связь в ближнем поле (Near Field Communication), которая весьма перспективна в настоящее время для экспериментов «продвинутых» пользователей и радиолюбителей, поскольку обеспечивает оперативную и защищённую передачу данных между устройством считывателя и метки на расстоянии до 10 см (заявленное производителем расстояние). Такая система практически не подвержена помехам из-за малого расстояния межу БСК и ридером.

Важной особенностью СК с возможностью перезаписи данных является их надёжность при сбоях любой природы. Данные в памяти сохраняются в том же виде, какими они были до начала незавершённой операции изменения и процесса записи. Это свойство называется «атомарностью» изменений данных в памяти.

В банковском секторе используются СК на основе операционных систем, перепрограммируемых с помощью языка Java. Эта технология регламентирована отраслевым стандартом VGP (Visa Global Platform), который сегодня весьма популярен в финансовой сфере.

Транспондеры (proximity-карты, СК, метки) реализованы в соответствии со стандартом ISO 14443A/B. Они работают (резонируют) на нелицензируемой частоте 125 кГц и 13,56 МГц и никому не мешают, т.к. не вызывают конфликтов с другим электронным оборудованием. Интегрирование в ту же карту (подложку) других электронных компонентов (в соответствии с данным стандартом) не увеличивает толщину носителя (картона).

Микросхемы для таких СК изготавливаются известными компаниями (Atmel, On Track, Inside Contactless и др.). Они работают на определяемой стандартом частоте (см. выше) и вместе с антеннами, встроенными в пластик или картон, превратились в полуфабрикат RFID-системы доступа, функционирующей в соответствии со стандартом ISO 15693-2.

Существуют различия между частотами и конструктивным исполнением метки (карты). Каждая метка-устройство RFID содержит кристалл и антенну – в частности, штампованную «катушку». Интересно, что на относительно низких частотах до 145 кГц катушка намотана на настроечный конденсатор, а на более высоких (13,56 МГц) представляет собой несколько токопроводящих дорожек спирали по периметру пластиковой карты.

Существуют многоразовые СК, на которые оператор (обычно в кассе метрополитена) с помощью специального устройства – программатора – записывает информацию о количестве поездок и сроке действия СК. Объём перезаписываемой информации в зависимости от технических параметров метки может составлять от нескольких десятков килобайт до нескольких Мбайт. Таким образом, на той же площади карты разработчики размещают разное количество композитных блоков.

Расширились и функциональные возможности смарт-карт. Считывание и запись данных в метку называют эмуляцией. Чтобы передать данные между NFC-устройствами (смарт-картой и системой считывания/записи данных) их надо сблизить на расстояние 4...5 см и менее или, если речь идёт о системах контактного доступа – таблетках для считывателей в старых системах домофонов, – привести в соприкосновение. Этот контакт инициирует работу интерфейса и конфигурирование сети равноправных узлов.

Важной особенностью протокола NFC является поддержание режима пассивного соединения (passive mode of communication), который позволяет обеспечить сеанс связи энергией, используя ресурсы только одного из устройств (считывателя, на который подано электропитание). Такая технология активно используется для передачи небольших объёмов данных, доступа на объекты, контроля посещаемости объектов с фиксацией времени прохода, контроля перемещений по большой территории сотрудников или грузов, проведения платежей, конфигурирования доступа к проводным и беспроводным сетям Wi-Fi и во многих других случаях.

В системах безопасности используются новые решения, автоматизирующие контрольные процедуры и повышающие степень их надёжности. Аутентификация с помощью метки и системы кодового доступа – это предоставление, с одной стороны, и проверка, с другой, доказательств того, что предъявитель метки является именно тем, кому она принадлежит. При совершенствовании систем безошибочной аутентификации становится актуальным комплекс методов, например, сочетание кодового доступа с удостоверением личности, содержащим биометрию, дактилоскопию, особенности лица, голоса и других индивидуальных черт. Такие комплексные методы аутентификации, защиты информации и ограничения доступа обеспечат более надёжное взаимодействие людей и компьютеров. Примером того, что данные системы развиваются, является ввод в действие биометрических паспортов Федеральной миграционной службой России (и другими государствами мира).

Прогрессивная биометрия

Сегодня биометрический паспорт на основе одноимённых модулей – совершенно реальная вещь. Системы ограничения доступа, торговые точки, корпоративные пропуска (и учёт посещаемости сотрудников), электронные документы (заграничные биометрические паспорта) с появлением биометрического модуля AT77SM0101BCBO2VKE производства Atmel (и аналогов) были усовершенствованы. Такие модули являются законченной подсистемой и поставляются вместе с программным обеспечением для аутентификации, что облегчает работу пользователя. Модуль реализован на основе микроконтроллера той же фирмы AT91RM9200 с архитектурой ARM9 и оснащён несколькими интерфейсами, в том числе Ethernet, SPI и RS-232.

В конфигурацию биометрического модуля входит кристалл – датчик FingerChip (Atmel) с размерами 0,4 мм (толщина) и 14 мм (сторона). Он устойчив к ударным нагрузкам, загрязнениям и влажности; именно поэтому в нём удобно хранить дактилоскопирован-

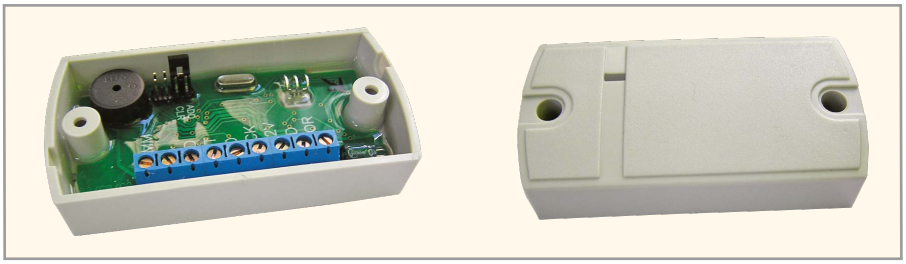

Рис. 5. Внешний вид считывателя Matrix II EH IronLogic

ные данные в цифровом виде. Существуют и другие датчики разных компаний-производителей. Общей тенденцией является миниатюризация датчиков. Например, ещё 3–4 года назад ИС сканирующего датчика фирмы Fingerprint Cards обладала разрешением 363 dpi и размерами 2,24 × 10,64 мм.

Вставка микросхемы с миниатюрной антенной в документ на бумажном носителе может производиться несколькими методами. Наиболее популярным по части надёжности является вставка/вклейка в напечатанный документ и последующее ламинирование. Именно так выполнены заграничные паспорта РФ нового поколения.

Считывающие устройства

Системы на основе СКУД позволяют легко и быстро собирать из нескольких модулей функциональные системы охраны и безопасности с кодовым доступом, требующие минимального количества внешних элементов. Кодовый доступ реализуется через дистанционное (до 10 см) считывание кода на метке, его инициализацию, декодирование и формирование сигнала управления для исполнительного устройства (например, электромагнитного замка двери или блокиратора на «вертушке»).

В качестве «запорного» устройства можно использовать не только сам замок (например, ЭМЗ-4 или ML-100), но и любую активную нагрузку, рассчитанную на соответствующее напряжение питания. Так, система кодового доступа, реализованная на модуле Matrix II EH IronLogic (см. ниже), рассчитана на подключение нагрузки с напряжением 12 В ±20% и током до 5 А. Если необходим больший ток, то коммутацию производят через дополнительное реле.

Пассивные системы RFID состоят из трёх частей: ридера, пассивной метки и ведущего компьютера. Ридер является шлюзом, с помощью которого цифровые данные вводятся в контроллеры на базе ПК и интегрированные системы. Считывающее устройство содержит микроконтроллер, передающую антенну, блок определения уровня сигнала радиоволны (peak detector), блок для передачи энергии метке и блок чтения информации с помощью детектирования изменения поля (backscatter modulation – отражённая модуляция). Ридеры выпускаются нескольких видов: встраиваемые, с клеммником для подключения (см. рис. 5), клавиатурные ридеры (с разъёмами USB/microUSB), ридеры в модулях PCMCIA в ПК и КПК и др.

Радиочастотный синусоидальный сигнал генерируется ридером для передачи энергии метке и получения от неё данных. Наиболее распространёнными частотами являются 125 кГц и 13,56 МГц. На более высоких частотах функционируют другие системы RFID, и для них разработаны иные методы связи. Например, на частоте 2,45 ГГц между ридером и меткой используется радиосвязь, на частотах 125 кГц, 145 кГц и 13,56 МГц используется электромагнитная связь.

Периодические колебания напряжённости электромагнитного поля служат основой для передачи данных от метки к ридеру и обратно. В системе существует только один передатчик в полном смысле этого слова – ридер. Электромагнитное поле, создаваемое ридером, используется для:

- *питания* – метки не имеют внутренней батареи питания или другого источника энергии. Они питаются от электромагнитного поля, создаваемого ридером;
- *синхронизации* – большинство меток делят частоту связи для внутреннего тактирования различных модулей и счётчиков, хотя некоторые имеют встроенный генератор;
- *передачи данных от метки* – ридер следит за уровнем излучаемого поля, модуляцией которого передаются данные (форматом выходных данных может быть I^2C, SPI, RS2400, LEVEL+STROBE или PWM).

Популярный считыватель Matrix II EH 125 кГц (см. рис. 5) используется в системах контроля доступа. С помощью перемычек можно установить тип выходного интерфейса – Touch Memory или Wiegand. Считыватель с картами Proximity работает в стандарте HID и EM Marin.

Технические характеристики ридера Matrix II EH IronLogic:

- частота 125 кГц;
- чтение карт доступа EM Marine и HID ProxCard II;
- дальность уверенного обнаружения метки от 6 до 14 см;
- питание считывателя 8...18 В постоянного тока, ток потребления 50 мА;
- индикация: звуковой сигнал, светодиод (2 цвета – зелёный и красный – предполагают внешнюю индикацию светодиодом и звуком);
- температура эксплуатации –40...+50°С;
- материал – пластик ABS;
- цвет: от чёрного до светло-серого или даже «металлик»;
- выходной интерфейс: Dallas Touch Memory (эмуляция DS1990A), Wiegand 26;
- максимальное расстояние от считывателя до контроллера (система с ПК) – до 15 м (интерфейс DS1990A) и до 100 м (интерфейс Wiegand);
- габариты 85 × 44 × 18 мм.

Подключение ридера к контроллеру и нагрузке иллюстрирует рисунок 6.

Большинство ридеров описанного форм-фактора выпускаются в аналогичном исполнении, что упрощает их монтаж. Они устанавливаются в открытых для доступа местах, поэтому необходимо предъявлять повышенные требования к «вандалозащищённости».

Считыватели имеют и некоторые функциональные отличия. Например, существуют ридеры (различных стандартов), которые уже содержат источник питания и готовы к работе от сети 220 В, имеют на выходе транзистор с открытым коллектором, к которому подключают нагрузку (реле), или слаботочное электромагнитное реле с возможностью коммутации нагрузки до 6 А.

Главное отличие систем дистанционного кодового доступа примерно одного энергетического диапазона состоит в том, что одни системы могут только считывать с метки код, без возможности обратной записи информации на метку, а другие позволяют обмениваться информацией и записывать в память той же метки (в т.ч. БСК) новые данные.

Самый простой пример – общественный транспорт. В Санкт-Петербурге продаётся БСК с 10 фиксированными поездками – т.н. гостевой билет,

действующий в трамвае, троллейбусе, автобусе и метро. После того как 10 раз будет считан её код устройствами считывания, она становится бесполезной и подлежит утилизации. Записать (перезаписать) на карту новую информацию невозможно. Карта состоит из «запечатанной» в плотную бумагу (картон) микросхемы микроконтроллера вместе с антенной, идущей по периметру карты (см. рис. 2), и получила название Smart Paper ID. Кристалл находится ближе к левому краю (от центра), если смотреть спереди, положив СК перед собой.

Сегодня СК (она же транспондер, метка или ключ) могут выглядеть как брелоки, браслеты и таблетки (см. рис. 3), и могут функционировать в составе компьютерных систем, мобильных телефонов, автомобилей и любого другого оборудования, – сфера их применения практически не ограничена. Можно предположить, что более миниатюрную метку, но с тем же принципом работы и функционалом, можно вживлять под кожу человеку и/или животному с помощью медицинских технологий, что позволяет не только его идентифицировать, но и контролировать перемещение. Такие технологии давно апробированы и сегодня уже никого не удивляют, хотя ещё десятилетие назад описывались писателями-фантастами.

Читатель может самостоятельно провести такой эксперимент. Поднесите БСК HID (например, карту доступа в номер отеля «Космос», г. Москва) к любому сотовому телефону выпуска 2010 года и новее – на дисплее появится информация о том, что карта не считана. Таким образом, электронная система современного мобильного телефона уже настроена на то, чтобы считывать подобные метки (стандарт ISO 14443 и др.).

По тому же принципу (спецификации для банковских карт Master Card Pay Pass на основе технологии RFID) работают «электронные» шкафчики в бассейнах, фитнес-клубах и аквапарках, где меткой является выдаваемый клиенту браслет.

Выводы

Все описанные технологии, как вчера, так и сегодня, применяются в широком спектре задач. В магазинах, в комплексе противокражных систем (устройств), метки используются уже двадцать лет. Широко распространены метки для противоугонных систем автомобилей (двигатель заглохнет через 10...60 с, если владелец не приложит метку к определённому месту). Ключи дорогих и престижных автомобилей также снабжены встроенной «меткой», которая считывается ридером, установленным в головке замка зажигания. Похожая система применяется в составе устройств типа Аркан Сателлит, отслеживающих автомобили, снабжённые определителем местонахождения по GPS. Метки стали применять и в системе учреждений Федеральной службы исполнения наказаний РФ для контроля перемещения заключённых и их идентификации, а также домашнего ареста (в этом случае человек носит браслет с меткой).

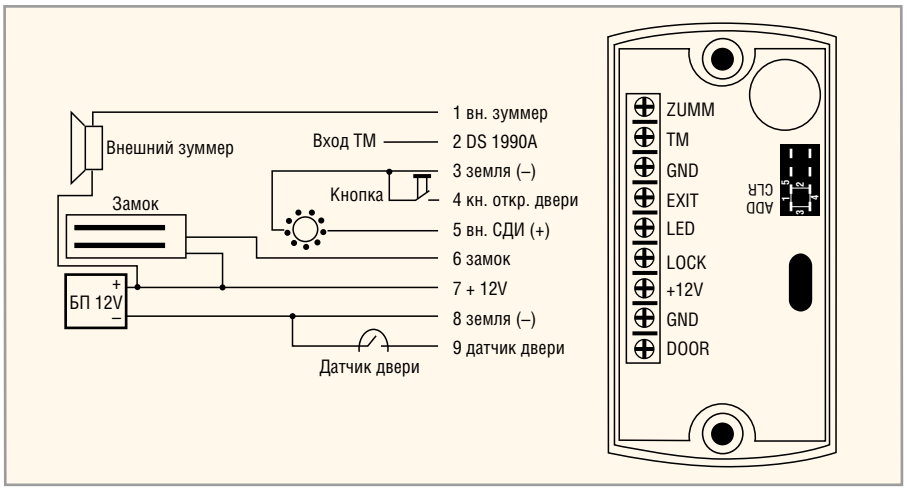

Рис. 6. Схема подключения цепей питания и коммутации считывателя Matrix II EH IronLogic

Метки применяются довольно широко в оборонной промышленности: для контроля доступа – смарт-карты, для идентификации человека при доступе к секретным сведениям – специальные кристаллы, вживляемые под кожу. И если ранее отследить перемещение объекта можно было только с помощью изотопов, то сегодня электроника справляется с этим без особых затруднений.

Весь спектр использования бесконтактных устройств нового поколения практически невозможно описать. Бесконтактные устройства контроля будут совершенствоваться, а микроконтроллеры в системах идентификации – развиваться, пополняясь новыми функциями для комплексной защиты объектов и секретной информации.