УДК 681.3.06

РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ И ЕЕ ПРИМЕНЕНИЕ

М.В. МАТЮШ
(Полоцкий государственный университет)

Исследуется основная задача системы радиочастотной идентификации – хранение информации об объекте в виде идентификационного кода с возможностью его удобного считывания. Анализ основных ограничений и настоящего уровня разработок аппаратуры RFID выявил большое число направлений будущих работ и исследований. Возможности применения технологии RFID очень широки. Новые применения и дополнительные возможности технологии RFID способны стимулировать большое число интересных и практически необходимых исследований. При этом автоматическая идентификация радиочастотных меток в сочетании с сетевыми базами данных обеспечит оперативное распознавание объектов информации и, соответственно, управление производственными технологическими процессами. На данный момент RFID в основном используется для управления сетью сбыта.

Введение. Технология радиочастотной идентификации (Radio Frequency IDentification) предоставляет возможности автоматической идентификации объектов посредством электромагнитного излучения. Современная система радиочастотной идентификации включает приемопередающую базовую станцию (называемую считыватель) с направленными антеннами и радиочастотную метку (транспондер), содержащую идентификационный код. Антенны приемопередающей базовой станции могут быть встроены в специальные сканеры, а также в ворота, турникеты, дверные проёмы и т.п. для получения информации от предметов или людей, проходящих через зону действия антенны. Конструктивно антенна и приемопередатчик с декодером могут находиться в одном корпусе. Сигнал, поступающий с антенны, демодулируется, расшифровывается и передается через стандартный интерфейс в компьютер для дальнейшей обработки.

Достижения информационных технологий в последние годы позволили совершить своеобразную информационную революцию. Повсеместное внедрение автоматизированных систем управления существенно изменило нашу жизнь.

Технологии бесконтактной идентификации наиболее полно соответствуют всем требованиям компьютерной системы управления (в том числе, управления подвижными объектами), где требуются распознавание и регистрация объектов и прав пользователей в реальном масштабе времени. Строятся они обычно на оптическом (всем известные штрих-коды) или радиочастотном принципе.

Радиочастотное распознавание осуществляется с помощью закрепленных за объектом специальных меток, несущих идентификационную и другую информацию. Этот метод, имеющий устоявшееся название RFID-технологии, уже стал основой построения современных бесконтактных информационных систем (БИС) [1]. RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) – метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. Любая RFID-система состоит из двух частей: считывающего устройства (ридера) и транспондера (он же RFID-метка).

Согласно стандартам информация передается при помощи PPM-модуляции. Большинство RFID-меток состоит из двух частей: первая – интегральная схема (ИС) для хранения и обработки информации, модулирования и демодулирования радиочастотного (RF) сигнала, а также других специфичных функций; вторая – антенна для приёма и передачи сигнала.

Существует технология безчипового RFID, позволяющая идентифицировать метку без использования ИС и тем самым снижающая стоимость. Размещается метка непосредственно на идентифицируемом объекте [2].

Физические основы RFID. Система радиочастотной идентификации состоит из метки, или тега (транспондера), которая несет информацию об объекте, считывающего устройства, которое получает информацию от объекта. Хост – устройство, которое производит непосредственно обработку данных, полученных путем считывания с метки. Связь между меткой и считывающим устройством и передача информации осуществляется посредством радиоволн [3]. Блок-схема такого устройства представлена на рисунке 1.

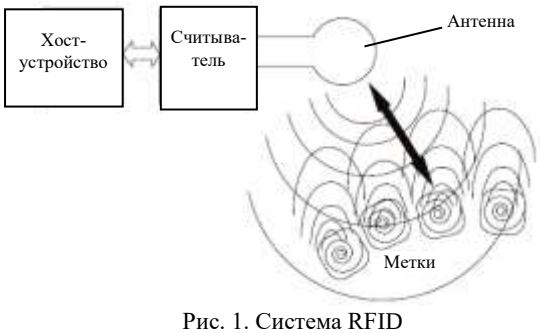


Рис. 1. Система RFID

Общий принцип работы любой RFID-системы достаточно прост (рис. 2). Считыватель излучает в окружающее пространство электромагнитную энергию. Идентификатор принимает сигнал от считывателя и формирует ответный сигнал, который принимается антенной считывателя, обрабатывается его электронным блоком и по интерфейсу направляется в компьютер [1].

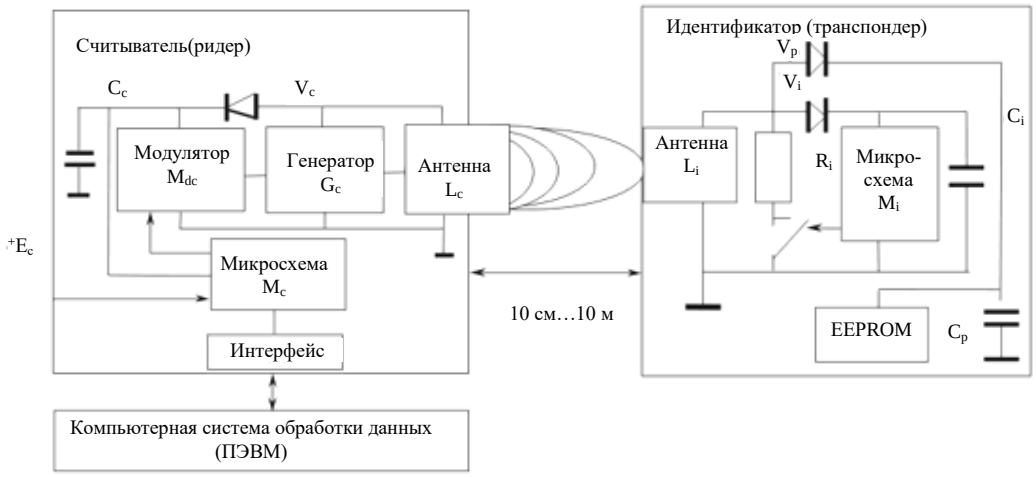


Рис. 2. Принцип работы RFID-системы

Ридер включает следующие устройства [3]:

- приемопередающее устройство и антенну – посылают сигнал к тегу и принимают ответный;
- микропроцессор – проверяет и декодирует данные;
- память – сохраняет данные для последующей передачи, если это необходимо.

Системы RFID можно условно разделить на две группы в зависимости от используемого типа метки: активные и пассивные [4].

В активных системах используют транспондеры с источником питания. Такая метка построена по схеме приемопередатчика и представлена на рисунке 3. Системы, построенные по такому принципу, имеют преимущество – в них возможно добиться хорошего соотношения сигнал/шум и, следовательно, большой дальности взаимодействия между меткой и считывающим устройством. Но как следствие применения на борту транспондера питающего элемента – высокая стоимость транспондера и ограниченный срок его службы. В пассивных системах применяется метка без питающего элемента и взаимодействие между считывателем и транспондером основано на принципе взаимной индукции.

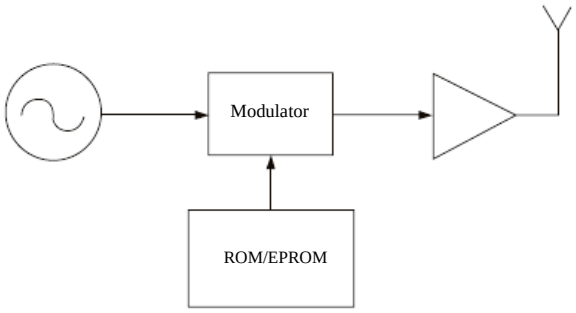


Рис. 3. Схема активной системы

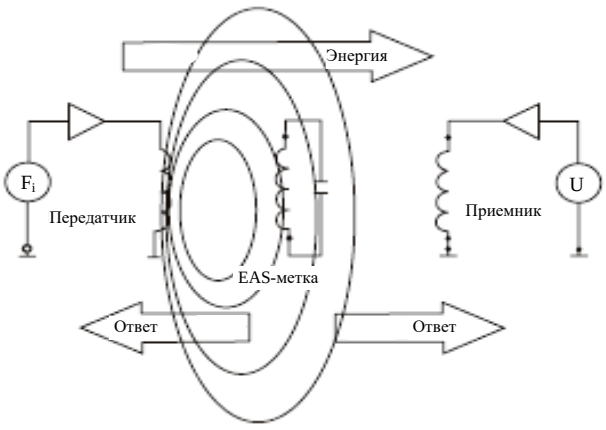
Антенна метки попадает в электромагнитное поле, создаваемое антенной считывателя. В ней посредством взаимной индукции наводится ток, затем полученная энергия переизлучается меткой и это излучение улавливается считывателем.

Для примера рассмотрим применение наиболее простых меток, которые получили название однобитных транспондеров (рис. 4). Такая метка представляет собой LC-контур. Считывающее устройство состоит из передатчика и приемника.

Транспондер, попадая в зону действия антенны передающего устройства считывателя, начинает излучать через антенну электромагнитные колебания, которые улавливаются приемной антенной, и система получает сообщение о присутствии объекта в поле считывателя [3].

Описанная выше система не позволяет различать объекты, она способна только извещать о факте ее попадания в зону действия считывателя.

Для того чтобы мы могли идентифицировать объект каждый в отдельности, применяются мультибитные транспондеры. Мультибитный транспондер представляет собой пассивный



приемопередатчик с элементом памяти (рис. 5).

Рис. 4. Система с однобитным транспондером

В самом простом варианте – это однократно программируемая память, в которую заносится на заводе-изготовителе уникальный серийный номер UID. Метка, попадая в поле считывателя, получает энергию, ток, наведенный в антенне транспондера, выпрямляется и поступает на схему метки, которая начинает излучать колебания, которые в свою очередь модулируются данными из памяти, и происходит передача уникального серийного номера от метки к считывателю.

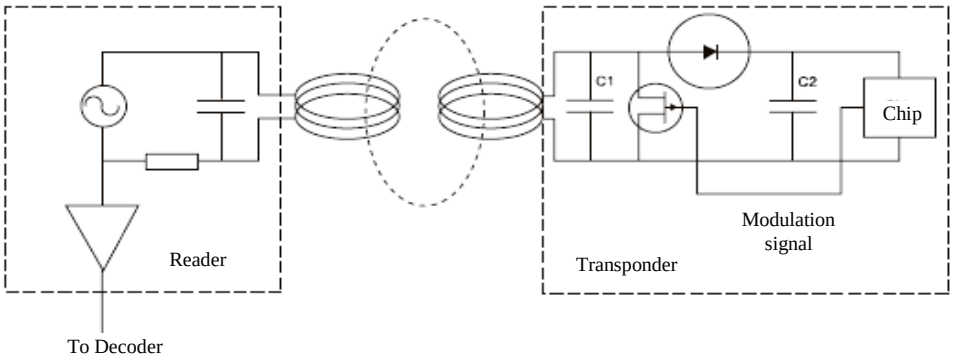


Рис. 5. Система с мультибитным транспондером

Существует большое разнообразие меток, различающихся по внутренней организации. Это метки с возможностью только считывания с них информации и более сложные, в которых возможно производить как чтение, так и оперативно через радиоинтерфейс заносить данные.

Метки различаются по объему памяти с различной организацией. Для приложений, где необходима повышенная защищенность передачи данных, применяются алгоритмы криптозащиты. В последних поколениях транспондеров применяются кристаллы, несущие на своем борту не только энергонезависимую память, но еще и микропроцессор, что дает возможность транспондеру самому производить необходимые вычисления и выполнение алгоритмов (JAVA CARD). Системы с такими метками применяются в банковских системах (кредитные карты), электронные паспорта и других приложениях, где необходима повышенная защищенность данных и вычислительные мощности. К тому же использование таких меток разгружает систему, что упрощает ее и, следовательно, удешевляет [4].

Связь Систем RFID. Связь между считывателем и меткой является неотъемлемой частью технологии RFID. Рассмотрим способы кодирования и модуляции, используемые в процессе связи в системе RFID.

При передаче информации нас интересует три основных параметра: 1) полоса пропускания; 2) вероятность ошибки; 3) сложность и издержки обнаружения ошибок.

Процесс связи состоит из передачи и приема информации. Для передачи по каналу связи с помехами информация преобразовывается накладывается на несущий сигнал и передается. После приема сигнала с помехами смесь демодулируется и обрабатывается для выделения первоначальной информации.

В технологии RFID информация включает команды управления и данные в двоичном виде. Обычно команды выделяются отдельными строками двоичных данных, но в отдельных случаях они представляют собой некоторую уникальную сигнатуру модуляции. В таких случаях необходима определенная обработка сигнала. Что касается данных, для них оказывается удобным использовать кодирующие устройства.

После того как данные закодированы, они налагаются на несущий сигнал. Такой процесс называется модуляцией. Модуляция необходима как для передачи данных при помощи канала распространения сигнала, так и для согласования спектра частот с административными регламентными ограничениями.

Перед рассмотрением спектральных характеристик сигналов необходимо понять различные методы их описания во времени.

Кратко рассмотрим понятия усреднения по времени приведенной (нормализованной) мощности и среднеквадратического значения сигнала.

Усредненное по времени, или среднее значение (постоянная составляющая) сигнала, $\omega(t)$ определим по формуле (1):

$$\omega(t) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} \omega(t)dt. \quad (1)$$

Для периодического сигнала формула (2) упрощается:

$$\omega(t) = \frac{1}{T} \int_{-T_0/2}^{T_0/2} \omega(t)dt, \quad (2)$$

где T_0 – период сигнала.

Независимо от того, в каких единицах измерения описан сигнал $\omega(t)$: вольт, ампер, вольт/м или ампер/м, его возведение в квадрат дает приведенную мощность в ваттах (соответствующая резистивная компонента принимается равной единице). Приведенная средняя мощность сигнала представлена формулой (3):

$$P = \left\langle \omega^2(t) \right\rangle = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} \omega^2(t)dt. \quad (3)$$

Квадратный корень из приведенной средней мощности дает среднеквадратичное значение (СКВ) сигнала:

$$\sigma = \sqrt{\left\langle \omega^2(t) \right\rangle}. \quad (4)$$

Каждый сигнал может быть представлен в виде спектра частот. Эти частоты позволяют определить преобразование Фурье. Такое определение полезно не только для согласования с регламентами, но также и для согласования частотных характеристик компонентов системы. Антенны, например, имеют определенные частотные (спектральные) характеристики, в соответствии с которыми они могут эффективно излучать или принимать сигналы. Передача или прием компонентов частоты сигнала, находящихся вне этой спектральной характеристики, будут невозможны. Зачастую антенны используются в качестве элементов фильтрации.

Ширина полосы частот, которую занимает спектр, изменяется соответственно огибающей кривой непрерывного спектра. Видно, что с уменьшением длительности импульса, величина спектральных линий падает, но все они распределены в более широкой полосе частот. Это может привести к сложностям с приемом таких сигналов узкополосными антеннами, при этом может уменьшиться соотношение сигнал/шум. Также возможны проблемы, связанные с превышением допустимой регламентами ширины спектра излучения. Спектральная плотность мощности периодических импульсов может быть найдена при помощи возведения в квадрат модуля коэффициентов Фурье:

$$S(f) = \sum_{n=-\infty}^{n=\infty} |C_n|^2 \delta(f - nf_0). \quad (5)$$

Сумма спектральных линий от $n = -\infty$ до $n = +\infty$ соответствует средней мощности сигнала.

Представление о ширине спектра является особенно важным с точки зрения скорости передачи данных, соотношения мощности сигнала к мощности шума и удовлетворения нормам регламентов. Вообще, ширина спектра – это область положительных частот, которые занимает сигнал, однако однозначного определения не существует.

В цифровых системах связи символы двоичных данных должны быть преобразованы в форму, которая была бы удобной при их передаче. Обычно это делается при помощи передачи последовательности импульсов, которые форматированы для представления символов данных. Такое импульсное форматирование часто называется линейным кодированием.

Так как в системах RFID передаются узкополосные сигналы, закодированная последовательность импульсов модулирует несущую частоту. В зависимости от используемой схемы модуляции может быть необходимым преобразование сигнала биполярного к униполярному, как, например, в случае амплитудной манипуляции. Мы не будем подробно анализировать кодирование до тех пор, пока не рассмотрим процесс модуляции, поскольку и кодирование, и модуляция совместно определяют полосу пропускания, вероятность ошибки и сложность приемника.

Есть два важных фактора для оценки системы связи – полоса пропускания и характеристики приема сигнала в присутствии шума.

Числовой оценкой качества функционирования аналоговых систем является отношение мощности сигнала к мощности шума. В цифровых системах критерием качества является вероятность ошибки в одном двоичном разряде или вероятность появления ошибочных битов (bit error rate – BER). BER – это вероятность возникновения ошибки, когда система должна принять решение о приеме одного из двух возможных сигналов. В случае модуляции ASK это сигналы высокого или низкого уровня (в системах с OOK низкий уровень равен нулю). Приемник имеет порог принятия решения, выше которого сигналы считаются сигналами высокого уровня и ниже которого – низкого уровня. Полная вероятность ошибки (BER) является суммой вероятностей ошибки, связанной с обоими сигналами.

Когда детектирование когерентное, используется большее количество информации – информация об амплитуде и фазе. Когда детектирование некогерентное, используется информация только об амплитуде. При этом ошибки функционирования системы увеличиваются. Тем не менее из-за простоты и невысокой стоимости в аппаратуре RFID обычно используют некогерентное детектирование огибающей.

В сигналах, модулированных ASK и OOK, присутствуют только два уровня сигналов. Каким образом эти уровни представляют отдельный бит, зависит от используемого вида кодирования. Однако независимо от вида кодирования, если ошибки сделаны в процессе определения уровня сигнала, возникнет

битовая ошибка. Некоторые виды кодирования могут обнаружить такую ошибку, а другие – не могут. В таком случае могут быть использованы другие методы обнаружения и исправления ошибки.

В беспроводных каналах шумы могут иметь разнообразную природу. Обычно рассматривают два вида шума – это импульсные помехи и гауссовский шум. Гауссовский шум обычно является результатом фонового излучения, тепловых помех и дробового шума. В устройствах связи ближнего действия, особенно в пассивных системах RFID невысокой стоимости, обычно наиболее важны импульсные помехи, которые являются результатом интерференции многих других мешающих излучений. Для вычисления BER систем RFID рассмотрим как импульсные помехи, так и гауссовский шум [9].

Применение RFID

Транспортные приложения. В транспортных приложениях основное место (около 80 %) занимают карты Mifare® производства Philips Semiconductors. В частности, они используются в Московском метрополитене, в пригородных поездах и в ряде других приложений. Карты соответствуют третьему уровню ISO 14443 A и дополнены собственным механизмом криптозащиты, который исключает подделку транспортных карт. Эти же карты используются в сетях автозаправочных станций, в клубных системах и во множестве других приложений, где незаменима бесконтактная технология и требуется защита от несанкционированного использования.

Логистика и склад. В данных приложениях работают идентификаторы двух стандартов среднечастотного диапазона (ISO 15693 и EPC), а также идентификаторы высокочастотного диапазона по стандарту ISO 18000.

Необходимость появления стандарта EPC (electronic product code) вызвана следующими обстоятельствами: во-первых, перезаписываемые метки по ISO 15693 нерентабельны в тех приложениях, где требуется только пометить товар; во-вторых, при их использовании нарушается принцип приватности, что было причиной нескольких скандальных разбирательств. EPC аналогичен штриховому коду (по формату данных), а функция деактивации метки позволяет разрушать ее в момент, когда надобность в ней отпадает.

Метки высокочастотного диапазона (800 МГц…2,45 ГГц) обеспечивают максимальную дальность записи и чтения (до 8…10 м), что незаменимо при внедрении технологии RFID в процессы управления складскими запасами.

Электронные документы. Это совсем новое, но очень перспективное направление использования технологии RFID. Быстрота считывания и надежность, высокая защищенность от несанкционированного доступа позволила начать внедрение электронных меток в паспорта, водительские удостоверения, авиационные билеты и другие документы.

В частности, по имеющимся данным в 2006 году страны ЕЭС перейдут на паспорта с RFID метками, электронную «начинку» в недалеком будущем получат и въездные визы; примерно к 2010 году ИКАО (международная ассоциация авиаперевозчиков) планирует перейти на электронные авиабилеты.

В настоящее время во многих странах в работе находятся проекты по переводу внутренних паспортов на электронную основу. При этом в памяти имплантированной в паспорт метки будут заноситься не только обычные данные владельца (ФИО, год рождения и т.), но и биометрические признаки, а также цветная цифровая фотография.

Системы контроля и управления доступом (СКУД). Это исторически самое старое применение технологии RFID. Сейчас доступ в офис или на предприятие по бесконтактной пластиковой карте (proximity карта) стал обыденным явлением. Первые решения на основе технологии proximity были относительно дорогостоящими (если сравнивать с наиболее популярными тогда магнитными картами), однако удобство и надежность, обеспечиваемые RFID, позволили за несколько лет практически вытеснить с рынка профессиональных систем доступа все конкурирующие технологии.

Основная масса карт и считывателей для систем доступа работают в пассивном режиме в частотном диапазоне 125 кГц. Реально устоявшихся стандартов нет, но наиболее популярны и распространены форматы компаний EM Marin, HID и Motorola (Indala).

С недавнего времени в СКУД начали применяться и интеллектуальные карты стандарта ISO 14443 (13,56 МГц). Причин тому несколько: во-первых, количество таких карт на руках у пользователей в мире исчисляется уже сотнями миллионов, а во-вторых, применение таких карт обеспечивает ряд преимуществ [5].

Главные преимущества технологии радиочастотной идентификации, по сравнению с другими технологиями автоматической идентификации, использующими штриховое кодирование, инфракрасные лучи или технологию оптического считывания [6]:

- бесконтактное считывание идентификационных данных;
- отсутствие необходимости прямой видимости метки;
- возможность многократной записи данных;
- больший объем сохраняемых данных;
- возможность одновременного автоматического считывания до нескольких сотен меток;
- лучшая защита от воздействия окружающей среды и возможность

- использования в агрессивных средах;
- максимальная точность считывания данных.

Операционная система кристалла RFID

Кристалл и даже изготовленная карта не имеет ни малейшей ценности без программного обеспечения «зашитого» в блок масочного ПЗУ. Это программное обеспечение принято называть операционной системой (ОС). Именно ОС определяет функциональность микропроцессорной карты, уровень защищённости, возможность использования карты в той или иной информационной системе.

Основные задачи ОС интеллектуальной карты можно определить следующим образом:

1) управление обменом данных;
2) управление выполнением команд;
3) управление файловой системой;
4) выполнение алгоритмических механизмов защиты информации.

Структуру ОС можно представить в виде слоёного пирога (рис. 6), где каждый слой программного обеспечения всё более абстрагируется от реальных особенностей микроконтроллера карты.

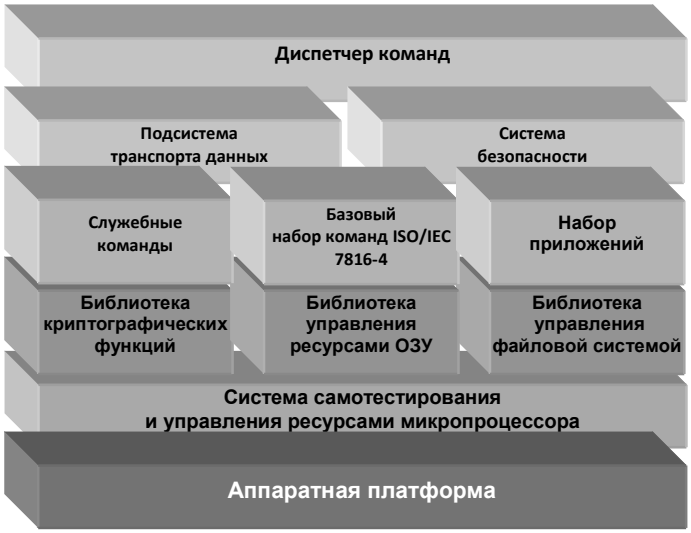


Рис. 6. Структура ОС

Система самотестирования и управления ресурсами микропроцессора состоит из библиотеки управления аппаратными ресурсами и встроенной системы самотестирования, обеспечивает программный доступ к периферийным устройствам микроконтроллера (ЭСППЗУ, устройства ввода/вывода и т.д.) и контроль работоспособности микроконтроллера.

Библиотека управления ресурсами ОЗУ обеспечивает доступ к области хранения и обмена данных ОЗУ микроконтроллера.

Область предназначена для обеспечения:

1) ввода/вывода данных;
2) временного хранения промежуточных данных;
3) для внутреннего обмена данными между командами.

Данный программный продукт обеспечивает реализацию процедур механизмов защиты.

Программы, входящие в состав библиотеки, выполняют выбор типа алгоритма, инициализацию переменных алгоритма, формирование/проверку криптографической подписи, шифрацию/дешифрацию данных.

Библиотека криптографических функций обеспечивает реализацию процедур механизмов защиты.

Программы, входящие в состав библиотеки, выполняют выбор типа алгоритма, инициализацию переменных алгоритма, формирование/проверку криптографической подписи, шифрацию/дешифрацию данных.

Библиотека программ управления протоколом приложения обеспечивает прием/передачу модулей данных команды и ответа в соответствии с протоколом передачи.

Программы осуществляют прием заголовка команды и данных, если они есть, а также формирование и выдачу ответного сообщения.

Библиотека файловой системы обеспечивает структурированный доступ к информации, хранящейся в энергонезависимой памяти карты.

Библиотека файловой системы состоит из системных процедур, осуществляющих создание, тестирование и управление файловой системой.

Библиотека команд ОС функционально разделена на три части:

1) служебные команды;
2) базовый набор команд;
3) набор приложений.

Служебные команды используются на этапе производства и персонализации карты для ее тестирования, идентификации и инициализации.

Базовый набор команд состоит из стандартных команд в соответствии с ISO и дополнительных команд, обеспечивающих идентификацию пользователя и другие функции.

В ОС предусмотрена возможность включения приложений, расширяющих возможности использования карт: электронный кошелек; EMV приложение.

Электронный кошелек представляет собой платежное приложение, разработанное на основе спецификации MPCOS-EMV для платежных приложений (дебетовые/кредитовые приложения) E-Purse.

EMV приложение представляет собой платежное приложение, функционально соответствующее приложению M/Chip Lite компании MasterCard, реализованное на базе данной операционной системы.

Подсистема транспорта данных обеспечивает обмен сообщениями между внешним устройством и картой в соответствии с действующими протоколами передачи и приложения.

Система безопасности обеспечивает защиту от несанкционированного доступа, достоверность и конфиденциальность информации.

Диспетчер команд ОС осуществляет общее управление подсистемой транспорта данных, системой безопасности и исполнением команд ОС.

Работа диспетчера начинается с инициализации переменных системы. Далее диспетчер идентифицирует фазу жизни карты, осуществляет проверку результатов самотестирования и в соответствии с полученным результатом обеспечивает выдачу последовательности байтов ATR.

Если внешнее устройство инициирует процедуру выбора параметров протокола (PPS), диспетчер обеспечивает прием запроса и выдачу ответа PPS.

В случае успешного завершения стартовых процедур диспетчер приступает к управлению исполнением команды. Диспетчер обеспечивает:

1) прием сообщения команды;
2) идентификацию команды или приложения;
3) проверку прав доступа и блокировку возможности прямой выдачи из команды;
4) реализацию механизма безопасной передачи сообщений;
5) передачу управления процедуре, реализующей соответствующую функцию;
6) формирование и выдачу ответа команды.

Перед началом исполнения команды диспетчер осуществляет контроль за минимально допустимым объёмом свободной области памяти.

После завершения исполнения команды диспетчер анализирует результаты выполнения команды и обеспечивает выдачу байтов слова состояния [7].

E-PURSE приложение

Электронный кошелек E-Purse представляет собой платежное приложение для операционной системы микропроцессорных карт МинОС.

Данное приложение обеспечивает:

1) работу карты с терминалами, поддерживающими платежные приложения, разработанные в соответствии со спецификацией E-Purse;
2) защиту денежных средств картодержателя;
3) проверку подлинности картодержателя, карты и терминала;
4) выполнение платежных функций:
5) защита данных и проверка их целостности с использованием криптографического алгоритма 2DES;
6) возможность получения подписи последней транзакции;
7) обмен информацией между картой и терминальным оборудованием в соответствии с требованиями стандарта ISO 7816 3-4.

Файлы электронного кошелька размещаются в директории приложения. Как правило, приложение содержит три типа элементарных файлов:

1) файл PIN-кодов (EF_{PIN});
2) файл ключей (EF_{KEY});
3) файл кошелька (EF_{PURSE}).

В файле кошелька содержится следующая информация:

1) максимальный баланс (максимальное количество денег, которое может хранить кошелек);
2) максимальная сумма дебета без предъявления PIN;
3) текущий баланс;
4) резервная копия баланса;
5) накопительный баланс операций без предъявления PIN;
6) счетчик транзакций терминала и счетчик транзакций карты.

Так как приложение подразумевает под собой не только набор данных, хранимых на карте, но и способы их обработки, в соответствии со стандартом ISO 7816-4 разработан набор команд для электронного кошелька.

Системные команды:

- Команда OPEN ADMINISTRATION SESSION – используется для открытия административной сессии и для инициализации механизма защищенного обмена сообщениями между терминалом и картой с использованием уникального сеансового ключа.
- Команда OPEN PAYMENT SESSION – используется для открытия платежной сессии, предшествующей платежным операциям над кошельком.
- Команда GET INFO – требует выдачи информации, понятной терминалу, о ключах, PIN-кодах или о файле кошелька.
- Команда – SELECT FILE осуществляет выбор файлов (селектирование на файл).
- Команда VERIFY CHV – осуществляет проверку введенного PIN-кода.
- Команда READ RECORD – осуществляет чтение записи из файла.
- Команда UPDATE RECORD – обновляет запись в файле.

Команды платежной сессии:

- Команда DEBIT – используется для операции дебетования кошелька (снятие денег со счета).
- Команда CREDIT – используется для операции кредитования кошелька – пополнение счета.
- Команда CANCEL DEBIT – используется для отмены последней операции дебетования кошелька.
- Команда READ BALANCE – используется для выдачи картой текущего баланса кошелька.
- Команда SIGN – используется для выдачи картой подписи последней транзакции кошелька [8].

Выводы

При анализе основных ограничений и настоящего уровня разработок аппаратуры RFID выявилось большое число направлений будущих работ и исследований.

Должны быть исследованы возможности реализации бесчиповых меток, созданию которых в настоящее время уделяется большое внимание. Особый интерес вызывают исследования, касающиеся дальности, памяти и антиколлизионных возможностей таких меток.

Возможности применения технологии RFID очень широки. На данный момент RFID в основном используется для управления сетью сбыта.

Прибыль от радиочастотной идентификации не всегда очевидна. Учитывая то, что в рамках технологии возможно существование сильно различающихся систем, оптимально подходящих всем решений просто не существует. Однако, при грамотном подходе, технология способна не только вернуть все вложенные в нее инвестиции, но и начать приносить прибыль. Отсутствие готовых систем способствует тому, что внедренная RFID-система будет решать заданные проблемы конкретного предприятия, при этом компания не будет доплачивать за неиспользуемые стандартные приложения.

Таким образом, новые применения и дополнительные возможности технологии RFID способны стимулировать большое число интересных и практически необходимых исследований. При этом автоматическая идентификация радиочастотных меток в сочетании с сетевыми базами данных обеспечит оперативное распознавание объектов информации и, соответственно, управление производственными технологическими процессами.

ЛИТЕРАТУРА

1. RFID или не RFID? ВОТ В ЧЕМ ВОПРОС // Специальная техника [Электронный ресурс]. – 2005. – № 6. – Режим доступа: http://st.ess.ru/publications/6_2005/barsukov/barsukov.htm. – Дата доступа: 10.09.2007.
2. RFID // Материал из Википедии – свободной энциклопедии [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/RFID. – Дата доступа: 10.09.2007.
3. Обзор систем компонентов радиочастотной аутентификации и их применение [Электронный ресурс]. – Режим доступа: http://www.rfidsolutions.ru/ files/Articles/Article1.pdf. – Дата доступа: 14.09.2007.
4. Приложения и RFID технологии [Электронный ресурс]. – Режим доступа: http://www.symmetron.ru/suppliers/rfid/rfid-philips.pdf. – Дата доступа: 14.09.2007.
5. Применение RFID [Электронный ресурс]. – Режим доступа: http://www.rfid.com.ru/application.htm.
6. Технологии радиочастотной идентификации [Электронный ресурс]. – Режим доступа: http://www.rfid-team.ru/information.html. – Дата доступа: 15.09.2007.
7. Операционная система микропроцессорных карт МинОС. Техническое описание: утв. 58191855.00011-01 99 01 ЛУ. – Минск: Литера О, 2004. – 193 с.
8. E-purse приложение для смарт-карт на базе кристалла К5004ВЕ2. Спецификация: утв. 58191855.00013-01 99 01. – Минск: Литера О, 2004. – 48 с.

9. Шарфельд, Т. Системы RFID низкой стоимости / Т. Шарфельд; прилож. И. Девиля [и др.]; пер. с англ. и науч. ред. С. Корнеева. – М., 2006. – 197 с.

Поступила 31.08.2007