



УДК 004.087

Н. А. Верзун, М. О. Колбанёв, Б. Я. Советов  
Санкт-Петербургский государственный электротехнический  
университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

А. М. Колбанёв  
АО «Эр-Телеком Холдинг» (Санкт-Петербург)

## Антиколлизсионные алгоритмы систем радиочастотной идентификации

*Представлен обзор современных технологий построения систем радиочастотной идентификации (RFID), являющихся неотъемлемой частью интернета вещей. Описаны особенности использования, достоинства и недостатки радиочастотной идентификации по сравнению с другими способами идентификации умных вещей. Приведена классификация радиочастотных меток по наиболее существенным для RFID-систем признакам. Рассматривается назначение антиколлизсионных алгоритмов в системах радиочастотной идентификации. Дается классификация алгоритмов антиколлизии, возможных к применению для организации взаимодействия радиочастотных меток со считывателем в RFID-системах различного назначения. Описаны и проанализированы возможности случайных, детерминированных, пространственных и корреляционных алгоритмов антиколлизии. Представлены временные диаграммы процедур опроса RFID-меток для случаев использования алгоритмов АЛОХА и тактированная АЛОХА, а также рассмотрены модификации указанных методов, позволяющие уменьшить вероятность возникновения коллизий и сократить время опроса. Развивается корреляционный подход к устранению (избеганию) коллизий применительно к RFID-меткам на поверхностных акустических волнах.*

### Интернет вещей, идентификация объектов, RFID система, RFID метка, множественный доступ, антиколлизсионные алгоритмы

Перспективы становления и продвижения в различные сферы деятельности концепции интернета вещей [1] связаны с развитием следующих технологий:

- технологий идентификации, которые позволяют отличить умную вещь от любой другой вещи;
- технологий всепроникающих сенсорных сетей, которые используют радиосигналы для организации взаимодействия между вещами [2]. Главными критериями выбора технологии являются энергетические и пространственные характеристики сенсорных полей, а не только битовая скорость передачи данных;
- технологий энергоснабжения умных вещей, которые обеспечивают их продолжительную автономную работу (использование миниатюрных источников энергии, тепла человеческого тела, кинетической энергии от ходьбы или нажатия на

клавиши, беспроводной подзарядки от электромагнитных сигналов и др.);

– сенсорных технологий для измерения характеристик вещей и их внешнего окружения, которые основаны на естественных законах физики (механика, колебания и волны, молекулярная физика и термодинамика, электродинамика, оптика, теория относительности, квантовая физика и др.), химии, биологии, географии, астрономии и геологии;

– технологий построения вычислителей разной степени интеграции, которые необходимы для реализации алгоритмов обработки данных (микропроцессоры, микроконтроллеры, микрочипы, устройства без аналого-цифрового преобразования и др.), и др.

В ряду упомянутых технологий центральное место занимают технологии идентификации ум-

ных вещей. Наиболее распространены системы идентификации, созданные на базе:

- штрихового кода;
- биометрических признаков, основанных на уникальности характеристик человеческого тела;
- радиометок, излучающих данные в форме радиосигналов.

Радиочастотная идентификация объектов (RFID – Radio Frequency IDentification) использует метку (транспондер, приемопередатчик, RFID-систему, RFID-тег) для дистанционного считывания или записи данных при помощи радиосигналов. По сравнению с другими подходами RFID обладает целым рядом преимуществ [3]: ускоряет процесс идентификации, не требует специального расположения маркера относительно устройства считывания, более надежна и долговечна. К недостаткам RFID-систем относят: зависимость от электромагнитных помех, взаимные коллизии в группе соседних меток, более высокую стоимость метки, подверженность кибератакам.

Область применения RFID-систем чрезвычайно широка [4]: системы контроля и управления доступом, сортировка, регистрация предметов (багаж, почтовые отправления, биоматериал и т. п.), логистика и цепочки поставок, профилактическое обслуживание и контроль целостности технических систем, идентификация беспилотных транспортных средств, управление складом, проведение инвентаризации, защита от подделок и многое др.

Классификация RFID-меток строится по различным признакам:

- по исполнению: кремниевые, на поверхностных акустических волнах;
- по способу хранения данных: с чипом (кремниевая технология), без чипа (на поверхностных акустических волнах);
- по электропитанию: активные (с излучающим контуром), полуактивные (выделено питание для чипа), пассивные (резонирующие);
- по способу использования: только считывание идентификатора (RO – Read Only), однократная запись данных в память и их многократное считывание (WORM – Write Once Read Many), многократные запись/считывание из памяти (RW – Read and Write);
- по частоте: низкочастотные (LF) до 150 КГц, среднечастотные (HF) 13.56 МГц, высокочастотные (UHF) 850...950 МГц, 2.45...5 ГГц.

Метки с чипом (кремниевая технология) дают возможность интерактивного взаимодействия со

считывателем. Это самая важная их особенность. Чип используются для хранения и обработки данных, модуляции и демодуляции радиосигналов, для выполнения протоколов взаимодействия с другими устройствами системы при помощи команд типа «сообщи заводской номер», «передай (запиши) байт из (в) памяти с адресом А», «задержи передачу на время t», «перейди в (выйди из) режим(а) молчания» и т. п.

Пассивные RFID-метки с чипом получают энергию для функционирования от электрического тока, индуцируемого в антенне электромагнитным сигналом считывателя. Обработку входного и выработку ответного сигнала обеспечивает кремниевый КМОП-чип (КМОП – комплементарная структура металл-оксид-полупроводник). Они используются при создании самонаклеивающихся этикеток (стикеров), проездных бесконтактных карт, ключей для прохода в здания и др. В больших количествах изготавливаются в виде бумажных или пластиковых рулонов. Чип может содержать от сотен байт до нескольких килобайт памяти.

Выбор КМОП-технологии построения интегральных микросхем объясняется близким к нулю энергопотреблением в статическом состоянии. Энергия требуется только для переключения состояний транзисторов во время вычислений. Современное оборудование позволяет изготавливать миллионы таких чипов за час.

Активная RFID-метка содержит однокристалльный микроконтроллер с разнообразными цифровыми и аналоговыми портами ввода-вывода, радиоприемопередатчик, кварцевые генераторы для синтеза радиочастот и для часов реального времени, большой объем памяти, а также дополнительные компоненты, такие, как устройства управления, кнопки, датчики для измерения температуры, влажности, давления, вибраций и др. физических параметров помеченного объекта и окружающей его среды и т. п. Батарея электропитания должна служить в течение нескольких (до 10) лет.

Программное обеспечение, прошитое в микроконтроллер, способно реализовывать сложные протоколы взаимодействия и со считывателем, и с другими метками.

Радиоинтерфейс на физическом и канальном уровнях часто использует стандарт IEEE 802.15.4, который является базовым для многих сетевых технологий интернета вещей.

Собственный источник питания позволяет активным меткам генерировать выходной сигнал большого уровня для увеличения дальности уверенного считывания до сотен метров и использования метки в таких средах, как вода, тело животного или человека, или металл (например, в контейнерах).

Используют 2 частотных диапазона:

- среднечастотный (HF), который обеспечивает дальность действия от 1 см до 0.2 м и использует модуляцию нагрузки сигнала несущей частоты (Load Modulation – нагрузочная модуляция);

- высокочастотный (UHF), который может использоваться на расстояниях от 1 до 10 м и передает сигнал методом модуляции отраженного сигнала несущей частоты (Backscattering Modulation – модуляция обратного рассеяния).

Габариты метки зависят от размера антенны, а размер антенны – от длины волны несущей, для которой она создана.

Поскольку активная метка получает энергию, необходимую для обработки команд считывателя и формирования ответного сигнала, от встроенной батареи, а пассивная метка – по радиолинии от устройства считывания, между ними существуют значительные различия при производстве и эксплуатации (таблица).

Полупассивные метки, в отличие от активных, используют батарею питания для встроен-

ных датчиков и накопления данных в микрочипе при нахождении метки вне поля считывателя. Считывание и передача данных осуществляются так же, как и у пассивных меток с чипом.

Наряду с самими RFID-метками неотъемлемыми элементами RFID-систем являются считыватели, связанные с RFID-метками по радиоканалу, и информационные системы для управления всеми процессами.

Как правило, при создании RFID-систем несколько меток оказываются в зоне действия одного считывателя и на выработанный им импульс опроса откликается одновременно группа меток [5]. Если не предпринять специальных мер, то такая ситуация приводит к коллизии (конфликту) меток, т. е. наложению друг на друга ответных сигналов нескольких меток, которое приводит к искажению данных, принимаемых считывателем [5]. Коллизии лишают RFID-систему ее самого важного свойства – способности дистанционного считывания уникальных идентификаторов меток.

Алгоритмы, которые позволяют считывать данные только с одной определенной метки, находящейся в непосредственном соседстве с другими метками, называются антиколлизийными алгоритмами. Они во многом схожи с алгоритмами множественного доступа, которые широко используются в сетях связи [6]. Классификация антиколлизийных алгоритмов приведена на рис. 1.

Пассивные метки	Активные метки
Для производства требуется стандартное технологическое оборудование микроэлектроники, низкая стоимость маркера	Достаточно сложные схемотехнические решения построения маркера, высокая стоимость
Источник питания не требуется	Источник питания ограничивает срок эксплуатации
Имеют малый размер, самый большой элемент – это антенна	Значительные габариты и масса, связанные с наличием источника питания
Дальность считывания обычно находится в пределах от десятков сантиметров до единиц метров	Дальность считывания определяется мощностью источника питания, может составлять несколько сотен метров
Ограниченные возможности для перезаписи или перезапись невозможна	Могут быть сделаны перезаписываемыми с сохранением дополнительных данных
Сохраняют работоспособность в широком температурном диапазоне, не подвержены воздействию радиации	Имеют ограниченный температурный диапазон, воздействие радиации приводит к отказу в работе
Некоторые типы маркеров обнаруживаются нелинейными локаторами	Могут быть легко обнаружены аппаратурой радиоконтроля

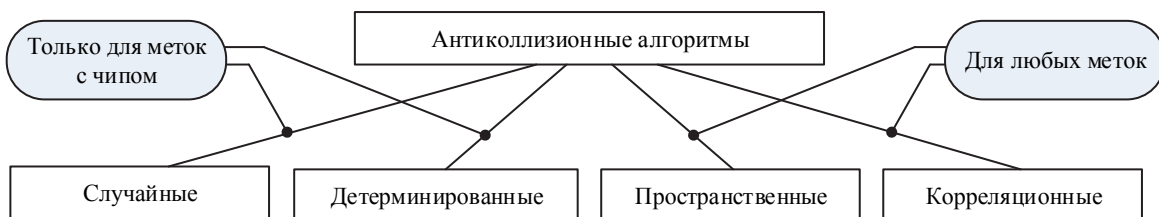


Рис. 1

Построение алгоритмов антиколлизий в RFID-системе существенно зависит:

- от функциональных возможностей меток. Выделение метки с чипом может быть организовано посредством ее диалога со считывателем по определенному протоколу, в то время как метки без чипа – только на основе излучаемых ею уникальных данных;

- предварительных знаний о свойствах меток, расположенных в зоне действия считывателя, таких, как серийные номера, расстояние до считывателя, место расположения и т. п.

**Случайные алгоритмы.** Многие случайные алгоритмы, разработанные для меток с чипом, так или иначе являются модификацией алгоритма АЛОХА, который предполагает способность метки зафиксировать факт коллизии и повторно выдать данные через некоторое случайное время задержки. Поскольку задержки вырабатываются метками независимо, то всегда наступает момент времени, при котором излучает только одна метка. Временная диаграмма процесса опроса RFID-меток при применении алгоритма АЛОХА приведена на рис. 2, а.

Стандарт ISO 15693 [7] вводит антиколлизционный алгоритм синхронная АЛОХА, в соответствии с которым передача данных осуществляется метками в начале временных интервалов, задаваемых считывателем. В случае возникновения коллизии меткой вычисляется случайное число интервалов задержки повторной передачи. Временная диаграмма процесса опроса RFID-меток при применении алгоритма синхронная АЛОХА приведена на рис. 2, б.

Дальнейшее развитие этого алгоритма использует способность метки выполнить команду считывателя, направленную именно к ней. В этом случае считыватель может:

- принудительно задержать передачу данных от некоторых меток;

- запретить вещание уже идентифицированным меткам.

Такие команды сокращают общее время идентификации всей совокупности меток, поскольку количество активных меток в зоне опроса все время уменьшается.

Известны и другие модификации алгоритма АЛОХА, уменьшающие вероятность коллизий и сокращающие время опроса.

В стандарте Gen2 [8], [9] используется случайный алгоритм выбора метки с чипом, в котором метки из зоны опроса выделяются без использования их идентификаторов. Вначале считыватель тем или иным образом выбирает некоторое число  $Q$ . Затем:

**Шаг 1.** Считыватель просит все метки из зоны опроса сгенерировать 2 случайных числа в диапазонах, которые задает  $Q$ :

- первое число  $q_1$  в диапазоне от 0 до  $n = 2^Q - 1$ , например, если  $Q = 5$ , то  $q_1 = \{0, 1, \dots, 31\}$ ;

- второе число  $q_2$  в диапазоне от 0 до  $2^{n+1} - 1$ , например, если  $Q = 5$ , то  $q_2 = \{0, 1, \dots, 4\,294\,967\,295\}$ .

**Шаг 2.** Считыватель просит ответить ему только те метки, которые выбрали первое число  $q_1 = 0$ . Возможны 3 случая:

- если ответило несколько меток, то считыватель увеличивает значение  $Q$ , тем самым уменьшая вероятность генерации одинаковых чисел разными метками, и возвращается к шагу 1;

- если нет ответа ни от одной из меток, считыватель уменьшает значение  $Q$ , тем самым уве-

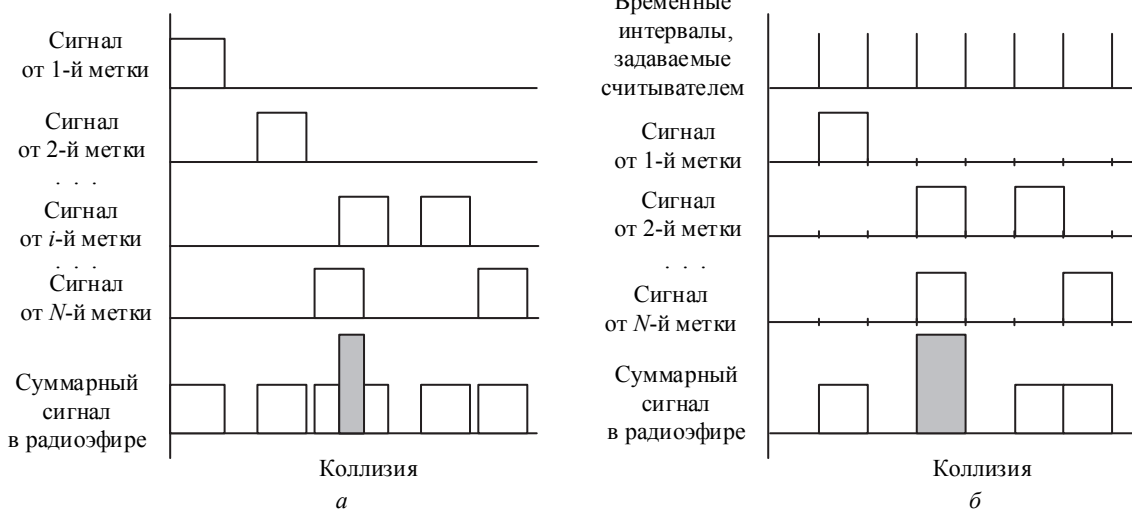


Рис. 2

личивая вероятность генерации числа 0 одной из меток, и возвращается к шагу 1;

– если отвечает одна метка, считыватель переходит к шагу 3.

**Шаг 3.** Считыватель запрашивает у ответившей (выбранной) метки второе случайное число  $q_2$  и далее использует его как временный идентификатор метки.

**Шаг 4.** Считыватель просит оставшиеся метки вычесть 1 из первого случайного числа  $q_1$  и переходит к шагу 2.

И так до тех пор, пока не будут определены все метки.

Алгоритм позволяет по сравнению с алгоритмом АЛОХА повысить:

– скорость поиска меток (до 1500 меток/с) и записи в них данных (до 16 меток/с);

– кибербезопасность RFID-системы, так как не требуется передавать через эфир уникальные идентификаторы меток.

**Детерминированные алгоритмы.** Работа детерминированных алгоритмов не связана с выработкой каких-либо случайных величин. Определить номер произвольной метки  $(x_1, x_2, \dots, x_n)$ ,  $x_i = (0, 1)$ , находящейся в зоне опроса, позволяют бинарный алгоритм или его модификации:

**Шаг 1.** Сначала предположим, что среди меток, расположенных в зоне опроса, есть метка, номер которой начинается с цифры «0». Если это предположение подтвердилось, то продолжим работать с соответствующей половиной номеров, если нет – то с другой половиной.

**Шаг 2.** Затем предположим, что вторая цифра – «0». И так далее.

Реализация такого алгоритма в RFID-системе возможна при соблюдении следующих условий:

– идентификационные коды каждой метки представляют собой числа, которые заранее не известны считывателю;

– метка содержит чип и взаимодействует со считывателем в соответствии с некоторым стандартизированным протоколом;

– программное обеспечение метки по команде считывателя определяет совпадение или не совпадение некоторой цифры идентификатора с предыдущей цифрой и сообщает результат считывателю;

– для кодирования сигналов, излучаемых метками, используется линейный код, который позволяет считывателю принимать одновременно выработанные сигналы нескольких меток, если это одинаковые сигналы.

Недостатки такого подхода сводятся к следующему:

– алгоритм не работает, если в зоне опроса появляются новые метки;

– время поиска зависит в данном случае от сочетания кодов конкретных меток.

Следующий детерминированный побитовый алгоритм поиска двоичного идентификатора  $(x_1, x_2, \dots, x_n)$ ,  $x_i = (0, 1)$  произвольной метки, находящийся в зоне опроса считывателя, используется в Gen1:

**Шаг 1.** Считыватель устанавливает счетчики разрядов во всех метках в состояние 1. Пусть в начальном «нулевом» разряде хранится  $x_0 = 0$ .

Для всех разрядов идентификатора в порядке возрастания  $i = 1, 2, \dots, n - 1$  выполнить:

**Шаг  $i$ .** Определение цифры  $x_i$ . В соответствии с протоколом в ответ на сообщение считывателя: «Есть метки с  $x_i = x_{i-1}$ ?» отвечают только метки, у которых это условие выполняется.

Если ответ получен, тогда:

– считыватель сохраняет найденную цифру  $x_i$ ;

– метки, у которых  $x_i = x_{i-1}$ , устанавливают счетчик разрядов в положение  $i + 1$ ;

– метки, у которых  $x_i \neq x_{i-1}$ , не меняют состояние счетчика и блокируют вещание.

Если ответ не получен, тогда:

– считыватель сохраняет найденную цифру  $x_i = 1 - x_{i-1}$ ;

– метки, у которых  $x_i \neq x_{i-1}$ , устанавливают счетчик разрядов в положение  $i + 1$ ;

– метки, у которых  $x_i = x_{i-1}$ , не меняют состояние счетчика и блокируют вещание.

**Шаг  $n$ .** Определение цифры  $x_n$ . На сообщение считывателя: «Есть метки с  $x_n = x_{n-1}$ ?» отвечают только те метки, у которых это условие выполняется.

Если ответ получен, тогда  $x_n = x_{n-1}$ , если не получен, тогда  $x_n = 1 - x_{n-1}$ .

Считыватель нашел значение кода  $(x_1, x_2, \dots, x_n)$  одной из меток и блокирует дальнейшее взаимодействие с ней.

Затем аналогично определяются номера остальных меток из зоны опроса.

**Пространственные алгоритмы.** Главная идея пространственных алгоритмов антиколлизии заключается в выборе такого взаимного положения считывателя и группы меток в пространстве, которое позволит направить импульс опроса

только к одной определенной метке и не инициировать считывание данных с других меток этой группы. Дополнительными управляемыми параметрами при этом являются мощность и направленность импульса считывания, их настройка на локализацию определенной метки.

Достигнуть нужного результата можно в тех случаях, когда есть возможность измерять расстояния до каждой из меток, находящихся в зоне опроса. Это дает возможность организовать последовательное чтение разных меток, однако задача усложняется по мере увеличения числа меток и уменьшения расстояния между соседними метками.

На практике пространственные алгоритмы работают в следующих случаях:

- считыватель имеет низкую мощность и считывает данные, находясь на малом расстоянии от метки;
- группа меток является статической системой, в которой точно известно положение каждой метки, так что можно заранее определить зону опроса при каждом положении считывателя.

В большинстве случаев достигнуть высоких антиколлизийных свойств пространственных алгоритмов удается при их сочетании с другими алгоритмами антиколлизии.

**Корреляционные алгоритмы.** Одна из перспективных технологий построения RFID-систем – создание меток на поверхностно-акустических волнах (ПАВ) [10]. В основе данной технологии лежат физические процессы прямого и обратного пьезоэлектрического эффекта:

– прямой пьезоэлектрический эффект – это возникновение поляризации диэлектрика под механическими воздействиями. Такой диэлектрик называется пьезоэлектриком;

– обратный пьезоэлектрический эффект – это возникновение механических деформаций под действием электрического поля.

По сути, пьезоэлектрик позволяет преобразовывать механическую энергию в электрическую и электрическую в механическую. Поверхностные акустические волны – это упругие волны, распространяющиеся вдоль поверхности твердого тела. В пьезоэлектрике их можно инициировать электрическим импульсом.

На рис. 3 поясняется принцип действия метки на ПАВ с электродами. Приложение излучателем импульса тока к пьезоэлектрической подложке преобразует электрическую энергию в механическую и генерирует ПАВ. Двигаясь по подложке, механическая волна преобразуется в электрический сигнал на каждом из пяти электродов, и в

шине приемника возникает импульсный сигнал. Параметры сигнала на каждом электроде зависят от способа их подключения. Для случая, показанного на рис. 3, в эфир будет выдан сигнал 00101.

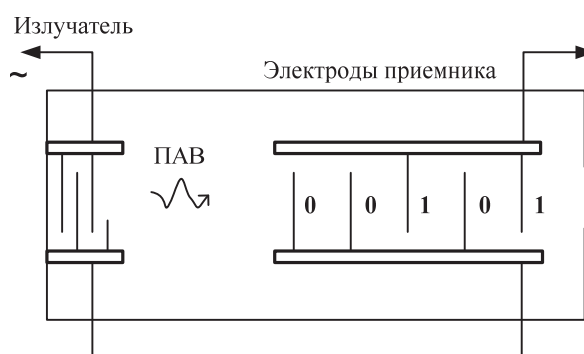


Рис. 3

RFID-метка на ПАВ с отражающими элементами показана на рис. 4. Она содержит:

- дипольную антенну, подключенную к встречно-штыревому преобразователю (ВШП), которая принимает сигнал опроса от считывателя и излучает ответный сигнал метки;
- ВШП – это 2 электрода, нанесенные на подложку методом фотолитографии. ВШП располагается в начале подложки и сначала преобразует электрические сигналы, поступающие от антенны, в ПАВ, а затем ПАВ, отраженную рефлекторами, – в электрические, передаваемые антенне. Длина электродов в 100 и более раз больше их ширины;
- рефлекторы, также создаваемые с помощью фотолитографии, расположены по длине подложки и моделируют акустическую волну, отражая некоторую часть ПАВ обратно по направлению к ВШП. Оставшаяся часть поверхностной волны продолжает двигаться к концу подложки и там гасится.

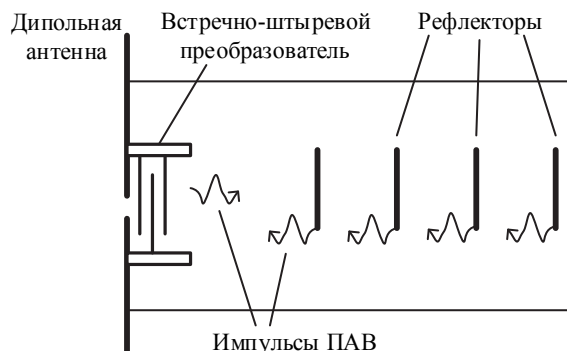


Рис. 4

Электрический сигнал, выработанный ВШП из отраженной волны, преобразуется антенной метки в высокочастотную последовательность электромагнитных импульсов, которые излучаются в эфир и могут быть приняты антенной считывателя.

Обратный импульс каждого рефлектора отражает особенности этого рефлектора и имеет определенные фазу, временную позицию и амплитуду, несущие информацию. Считываемый код закладывается при изготовлении метки. Кодирование основано на свойствах физического процесса распространения ПАВ:

– объем данных метки и скорость их передачи зависят от числа рефлекторов, т. е. от размера подложки и минимального допустимого расстояния между рефлекторами;

– скорость распространения ПАВ примерно в  $10^5$  раз меньше, чем скорость света, с которой распространяются радиоволны, поэтому все отражения от предметов, окружающих считыватель, успевают затухнуть до момента выработки меткой первого импульса;

– физический процесс формирования ответного сигнала характеризуется постоянными значениями фазы импульсов, отраженных от рефлекторов, и интервалом времени между импульсами, отраженными разными рефлекторами (интервал времени между импульсами линейно зависит от расстояния между соответствующими рефлекторами).

Определение идентификаторов меток без чипов, таких, как метки на ПАВ, возможно только на основе измерения корреляционных свойств излучаемых ею сигналов. Это позволяет выделить из эфира один определенный искомый сигнал или убедиться, что соответствующей метки нет в зоне опроса. Очевидно, что код искомого сигнала должен быть известен заранее.

Одно из свойств меток на ПАВ заключается в следующем. Если сигнал опроса построить как зеркальную последовательность кода метки, образованного рефлекторами, то за счет корреляции

отраженный импульс метки будет импульсом значительной амплитуды. Уменьшение взаимно-корреляционной функции (ВКФ) опросной последовательности с кодом метки приводит к уменьшению амплитуды отклика.

Это свойство дает возможность создать RFID-систему на маркерах без чипа, выбрав такие коды для меток, которые попарно имеют достаточно маленькую ВКФ.

Наилучший вариант системы кодов должен состоять только из ортогональных кодов, т. е. таких, для которых ВКФ любой пары кодов равна нулю. Такие свойства имеют коды Баркера, однако они содержат всего 3, 4, 5, 7, 11 и 13 символов.

Ортогональные коды можно получить при помощи функций Уолша, образуемых матрицей Адамара [11]. Это группа из  $2^n$  функций, которая формируется рекуррентно по следующей общей схеме:

$$H_{2^n} = \begin{bmatrix} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & -H_{2^{n-1}} \end{bmatrix}.$$

Свойства таких кодов сохраняются только при отсутствии временного сдвига. Их можно использовать только в синхронных системах, когда есть возможность определить момент времени начала вычисления ВКФ. Коды по строкам и по столбцам ортогональны. Корреляция строки с самой собой дает  $2^n$ , с другой – 0.

Таким образом, количество кодов, которое может быть получено при известных подходах, не позволяет создать RFID-систему с востребованным на практике числом меток, поэтому актуальной является задача разработки групп квазиортогональных кодов, образующих достаточно большую группу.

## СПИСОК ЛИТЕРАТУРЫ

1. Кучерявый А. Е. Интернет вещей // Электро-связь. 2013. № 1. С. 21–24.
2. Comparison Of Protocols For Ubiquitous Wireless Sensor Network / A. Muthanna, A. Paramonov, A. Kucheryavy, A. Prokopiev // 6th Intern. Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2014. St. Petersburg: IEEE Computer Society, 2015. P. 334–337.
3. Верзун Н. А., Колбанев М. О., Омелян А. В. RFID-технологии для эффективности и безопасности документооборота // Технологии информационно-экономической безопасности: сб. ст. сопр. каф. ИС и Т. СПб.: Изд-во СПбГЭУ «ЛЭТИ», 2016. С.44–51.
4. Radio Frequency IDentification (RFID). URL: [http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:RFID\\_%28Radio\\_Frequency\\_IDentification%2C\\_Радио\\_Частотная\\_Идентификация%29](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:RFID_%28Radio_Frequency_IDentification%2C_Радио_Частотная_Идентификация%29).
5. Шарфельд Т. Системы RFID низкой стоимости / под ред. С. Корнеева. М.: Москва, 2006. 197 с. URL: [http://www.alpha1.ru/recomend/rfid\\_lowcost.pdf](http://www.alpha1.ru/recomend/rfid_lowcost.pdf).
6. Верзун Н. А., Колбанёв М. О., Омелян А. В. Регулируемый множественный доступ в беспроводной сети умных вещей // Омский науч. вестн. Сер. Информатика, вычислительная техника и управление. 2016. № 4 (148). С. 147–151.

7. Радиочастотная идентификация. Технологии, стандарты, компоненты. URL: [http://www.vital-ic.com/files/Catalog\\_RFID\\_light.pdf](http://www.vital-ic.com/files/Catalog_RFID_light.pdf).

8. Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9. URL: [http://www.keytex.ru/files/Class\\_1\\_Generation\\_2\\_UHF\\_Air\\_Interface\\_Protocol\\_Standard\\_Version\\_1.0.9.pdf](http://www.keytex.ru/files/Class_1_Generation_2_UHF_Air_Interface_Protocol_Standard_Version_1.0.9.pdf).

9. TI UHF Gen2 Protocol Reference Guide. URL: <http://www.keytex.ru/files/UHF-ProtocolRefGuide.pdf>.

10. Дмитриев В. Ф. Исследование корреляционного метода для решения задачи антиколлизии для систем радиочастотной идентификации на ПАВ // Информационно-управляющие системы. 2009. № 5. С. 48–53.

11. Беспалов М. С., Скляренко В. А. Дискретные функции Уолша и их приложения: учеб. пособие. Владимир: Изд-во ВлГУ, 2014. 68 с.

N. A. Verzun, M. O. Kolbanev, B. Ya. Sovetov  
Saint Petersburg Electrotechnical University «LETI»

A. M. Kolbanev  
SC «Er-Telecom Holding» (Saint Petersburg)

## ANTI-COLLISION ALGORITHMS OF RADIO-FREQUENCY IDENTIFICATION SYSTEMS

*The review of modern technologies of construction of radio-frequency identification (RFID) systems, which are an integral part of the Internet of things, is presented. The advantages and disadvantages of radio-frequency identification compared to the other methods of identification of smart things are described. The classification of radio-frequency labels by the most essential for RFID systems features is given. The purpose of anti-collision algorithms in radio-frequency identification systems is considered. The classification of anti-collision algorithms that may be used for the organization of interaction of radio-frequency labels with the reader in different-purpose RFID systems is presented. The possibilities of random, deterministic, spatial and correlation algorithms of anti-collision are described and analyzed. A correlation approach to the elimination (avoidance) of collisions in relation to RFID tags on surface acoustic waves is developed.*

**Internet of things, object identification, RFID system, RFID tag, multiple access, anti-collision algorithms**

УДК 519.65

О. В. Мандрикова, Н. В. Фетисова

*Институт космических исследований и распространения радиоволн Дальневосточного отделения Российской академии*

В. В. Геппенер

*Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)*

## Обобщенная многокомпонентная модель временного ряда параметров ионосферы

*Предложена обобщенная многокомпонентная модель временного ряда параметров ионосферы (ОМКМ), позволяющая описать регулярный временной ход параметров и выделить периоды аномальных изменений в данных. Идентификация модели основана на совместном применении вейвлет-преобразования и моделей авторегрессии-проинтегрированного скользящего среднего (АРПСС). На примере часовых данных критической частоты ионосферы (foF2) станции «Паратунка» (ИКИР ДВО РАН, Камчатка) описан процесс идентификации ОМКМ-моделей для различных сезонов и различных уровней солнечной активности. Сравнение полученных ОМКМ-моделей с эмпирической Международной справочной моделью ИРИ для анализируемой станции показало эффективность применения предлагаемой авторами модели. Результаты моделирования показали высокую эффективность модели в задачах выделения ионосферных аномалий, возникающих накануне и в периоды магнитных бурь.*

**Вейвлет-преобразование, авторегрессионные модели, параметры ионосферы, аномалии**

**Введение и постановка задачи.** Цель – разработать математические модели для аналитического

описания временных рядов сложной структуры и построения автоматизированных систем модели-