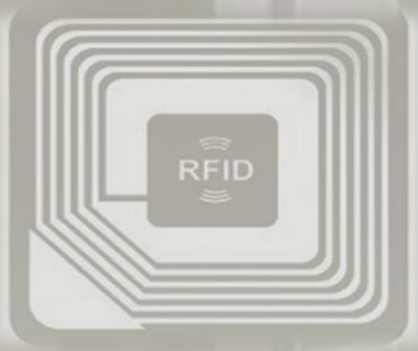
САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО
ЗОНАЛЬНАЯ НАУЧНАЯ БИБЛИОТЕКА ИМЕНИ В.А. АРТИСЕВИЧ

ПРЕДСТАВЛЯЮТ ВИРТУАЛЬНУЮ ВЫСТАВКУ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. СИСТЕМЫ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ



Саратов
2022

Выставка посвящена проблеме информационной безопасности при использовании RFID-систем (систем радиочастотной идентификации).

Развитие систем RFID и их быстрое распространение в различных сферах деятельности сопровождается значительным количеством инцидентов безопасности.

Существует несколько основных проблем: атаки на компоненты системы, утечка данных, недоверчивость пользователей.

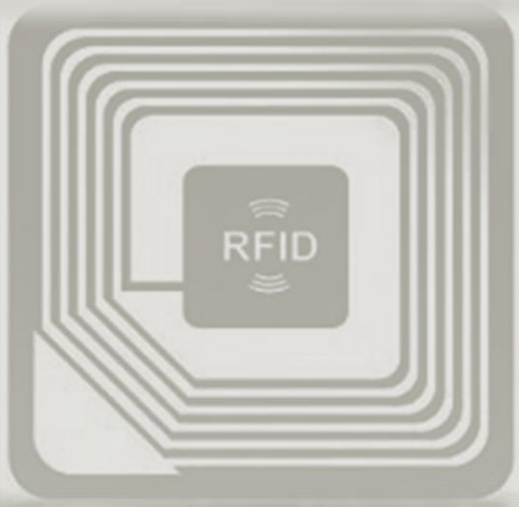
Особое развитие получают системы на основе недорогих пассивных меток – их можно широко применять в самых разных областях. В то же время конструктивные особенности этих меток не позволяют эффективно защититься от считывания данных, так как у них не хватает ресурсов на криптографические методы защиты.

Даже у тех устройств, где производится защита данных криптографией, алгоритмы могут быть ослабленными ввиду ограниченных вычислительных ресурсов.

Эти и другие проблемы рассматриваются в изданиях, представленных на выставке.

Выставка подготовлена по заказу кафедры микро- и наноэлектроники Института физики СГУ на базе АО «Контакт».

Литература представлена в обратной хронологии.



International Journal of Open Information Technologies ISSN: 2307-8162 vol. 9, no. 9, 2021

Безопасность RFID-систем

В. Бельский, Е. Грибоедова, К. Царегородцев, А. Чичаева

***Аннотация*—Радиочастотные метки (RFID-метки) широко используются во всем мире для идентификации и аутентификации объектов. В силу архитектурных особенностей и довольно низкой стоимости реализации RFID-метки часто характеризуются жесткими ограничениями на затрачиваемые ресурсы памяти и вычислительную мощность, что в свою очередь неминуемо отражается на требованиях к используемым криптографическим механизмам и протоколам. Существующих стандартизованных протокольных решений из других областей применения становится недостаточно, и требуется разработка специализированных алгоритмов именно для технологии RFID.**

В настоящей статье приводится классификация существующих RFID-систем, описываются типичные сценарии их использования. Основное внимание уделяется сравнительному анализу существующих криптографических механизмов защиты информации с учетом особенностей применения в средствах радиочастотной идентификации. Перечисляются эксплуатационные и криптографические свойства, которые необходимо учитывать при проектировании и сравнении RFID-систем. Приводится обзор известных на данный момент моделей противника, которые используются для анализа протоколов подобного типа.

***Ключевые слова*—RFID, аутентификация, ГОСТ**

I Введение

На протяжении двух десятилетий в мире активно развивается технология радиочастотной идентификации (RFID, Radio Frequency IDentification), позволяющая быстро и точно идентифицировать и/или аутентифицировать объект посредством использования радиоволн для считывания и передачи информации, хранящейся в RFID-метке.

RFID-системы успешно применяются в самых различных областях, таких как розничная торговля, логистика, платежные системы, системы контроля и управления доступом (СКУД), системы учета животных и анализа их поведения и многих других. При этом рынок RFID-меток продолжает расти с каждым годом [1]. Технология RFID имеет существенные преимущества. Так, например, некоторые классы RFID-меток не нуждаются во внутреннем источнике питания и в силу относительной простоты реализации обладают низкой стоимостью. Малые размеры меток позволяют легко прикреплять их к различным объектам и считывать с расстояния нескольких десятков метров. Указанными преимуществами обусловлен стремительный рост популярности данной технологии на протяжении последних лет [1, 2].

Однако, как это часто бывает с любыми новыми и стремительно развивающимися технологиями, процесс разработки необходимых открытых международных стандартов далек от завершения. В настоящий момент многие функционирующие RFID-системы не в полной мере отвечают необходимым требованиям безопасности, более того, в большинстве RFID-меток просто отсутствуют какие-либо криптографические механизмы, что делает эти системы уязвимыми ко множеству атак.

Российский рынок занимает незначительную долю в мировом рынке технологий RFID [2] и находится на этапе становления. Исследования безопасности протоколов аутентификации в RFID-системах недостаточно представлены в русскоязычной специальной литературе, а стандартизованные решения на базе российских криптографических алгоритмов отсутствуют. Поэтому разработка указанных протоколов является крайне актуальной задачей.

Настоящая статья посвящена первому этапу, который должен быть проведен при разработке любого криптографического протокола: классификации и сравнительному анализу существующих RFID-систем с учетом обеспечиваемых свойств безопасности, а также технических и эксплуатационных характеристик, с целью выбора наиболее релевантной модели противника, в рамках которой в дальнейшем будут проводиться исследования стойкости протоколов.

Статья построена следующим образом. В Разделе II выделены основные компоненты RFID-системы и описаны принципы работы технологии RFID. В Разделе III рассматриваются основные характеристики RFID-систем и обсуждаются различные классификации RFID-меток. Раздел IV посвящен рассмотрению основных атак и моделей угроз, наличие которых необходимо учитывать при выборе модели противника. В Разделах V, VI и VII более подробно обсуждаются свойства аутентификации, конфиденциальности и целостности данных, а также приватности (конфиденциальности источника) соответственно. В заключении в Разделе VIII приводятся ключевые требования, которые могут браться за основу при проектировании RFID-систем, удовлетворяющих различным требованиям безопасности.

Систематизированный и подробный обзор существующих механизмов, а также наличие сравнительного анализа используемых подходов позволит, с точки зрения авторов, существенно упростить процесс изучения современной научной литературы по данному вопросу, а также поможет при выборе и разработке конкретного протокольного решения.

Статья получена 12 июля 2021.

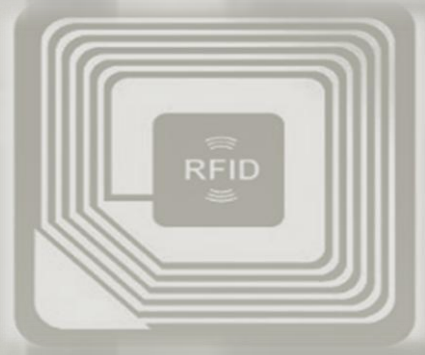
Владимир Сергеевич Бельский, Лаборатория Криптографии АО НПК «Криптонит», (email: v.belsky@kryptonite.ru).

Екатерина Сергеевна Грибоедова, Лаборатория Криптографии АО НПК «Криптонит», (email: e.griboedova@kryptonite.ru).

Кирилл Денисович Царегородцев, Лаборатория Криптографии АО НПК «Криптонит», (email: k.tsaregorodtsev@kryptonite.ru).

Анастасия Александровна Чичаева, Лаборатория Криптографии АО НПК «Криптонит», (email: a.chichaeva@kryptonite.ru).

Безопасность RFID-систем / В. Бельский, Е. Грибоедова, К. Царегородцев, А. Чичаева. - Текст : непосредственный // International Journal of Open Information Technologies. - 2021. - № 9. - С. 1-20. - ISSN 2307-8162.



В статье приводится классификация существующих RFID-систем, описываются типичные сценарии их использования. Основное внимание уделяется сравнительному анализу существующих криптографических механизмов защиты информации с учетом особенностей применения в средствах радиочастотной идентификации. Перечисляются эксплуатационные и криптографические свойства, которые необходимо учитывать при проектировании и сравнении RFID-систем.

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ

RFID

Специальный проект журнала «Современная электроника» и ГК «СИЛТЭК»

Разработка RFID-меток: что нового?

Максим Селиванов (smv@siltech.ru)

В прошлых номерах автор рассказывал о технологии RFID, видах радиометок, о том, как и где они применяются. Сегодня вы узнаете о новшествах рынка RFID-меток, их особенностях и различиях.

Всё дело в металле

Одним из перспективных направлений в микроэлектронике, ориентированном на RFID-сектор, является применение в пилеях особого вида антенн, которые профессионалы называют «3D». Не вдаваясь в технические подробности, можно сказать, что эти антенны обладают большей чувствительностью и позволяют улавливать сигнал на гораздо большем расстоянии, в отличии от обычных плоских антенн. Как правило, эта дистанция составляет около 10 м. Один из секретов антенны использует металл, на который закрепляется метка, в качестве усилителя сигнала.

Благодаря этой особенности, сфера применения 3D-меток очень обширная – практически везде, где требуется дистанционная идентификация на металлических поверхностях. Например, это может быть оборудование на промышленном производстве, стеллажи на складах, транспорт, объекты инфраструктуры, фонарные столбы или трансформаторные будки.

Новое предложение на рынке – метка с креплением на сильных неодимовых магнитах (сплав неодима, бора и железа), которая закрепляется за секунду (см. рис. 1), снимается сдвиганием и может быть использована сколько угодно раз в циклических производствах, на конвейерах.

Сантехниками 3D создана целая серия RFID-продуктов для разных областей использования. Есть 3D-метки, специально предназначенные для крепления в труднодоступных местах или там, где между объектами эксплуатации, которые планируется маркировать, небольшое расстояние. Для таких условий создана специальная низкопрофильная метка с очень устойчивым к внешней агрессивной среде корпусом, который сохраняет свою защитную функцию при климатическом или вибрационном воздействии (см. рис. 2). Кроме того, используются специальные пластики для создания корпусов, которые выдерживают экстремальные температуры и агрессивные жидкости (кислоты, щёлочи), при этом радиофизические свойства пилея остаются неизменными. Универсальные крепления позволяют легко и просто устанавливать метки на различных объектах не только из металла, но из пластика и дерева. Для монтажа можно использовать любые доступные средства – винты, саморезы, шурупы, стяжки, проволоку, двухстороннюю клейкую ленту.

На вкус и цвет...

Современные материалы, используемые в производстве корпусированных RFID-меток, дают возможность разработчикам и технологам реализовывать свои самые смелые идеи – как по форме, так и по цветовой гамме. Почему это важно? Представим большой цех предприятия, наполненный множеством технических объектов (промышленное оборудование, линии, станки, инвентарь), которым нужно определённое внимание. Разнообразная цветовая палитра (см. рис. 3) позволяет добавить дополнительный фактор идентификации объектов, например, в зонах опасного производства, где важна визуальная сигнализация. Это имеет значение также при наличии сложной системы маркировки, когда несколько однотипных агрегатов маркируются в соответствии с разными функциональными характеристиками или признаками. Поэтому большинство новинок на рынке можно заказать практически в любом цвете. Например, корпус может быть изготовлен из прозрачного поликарбоната, который имеет флуоресцентный оранжевый цвет.

Что касается конфигурации корпуса меток, то здесь производители охотно идут навстречу заказчикам и готовы воплотить в жизнь любой креатив. Уже никого не удивишь миниатюрными метками (см. рис. 4), круглыми, с обтекаемым корпусом, с встроенны-

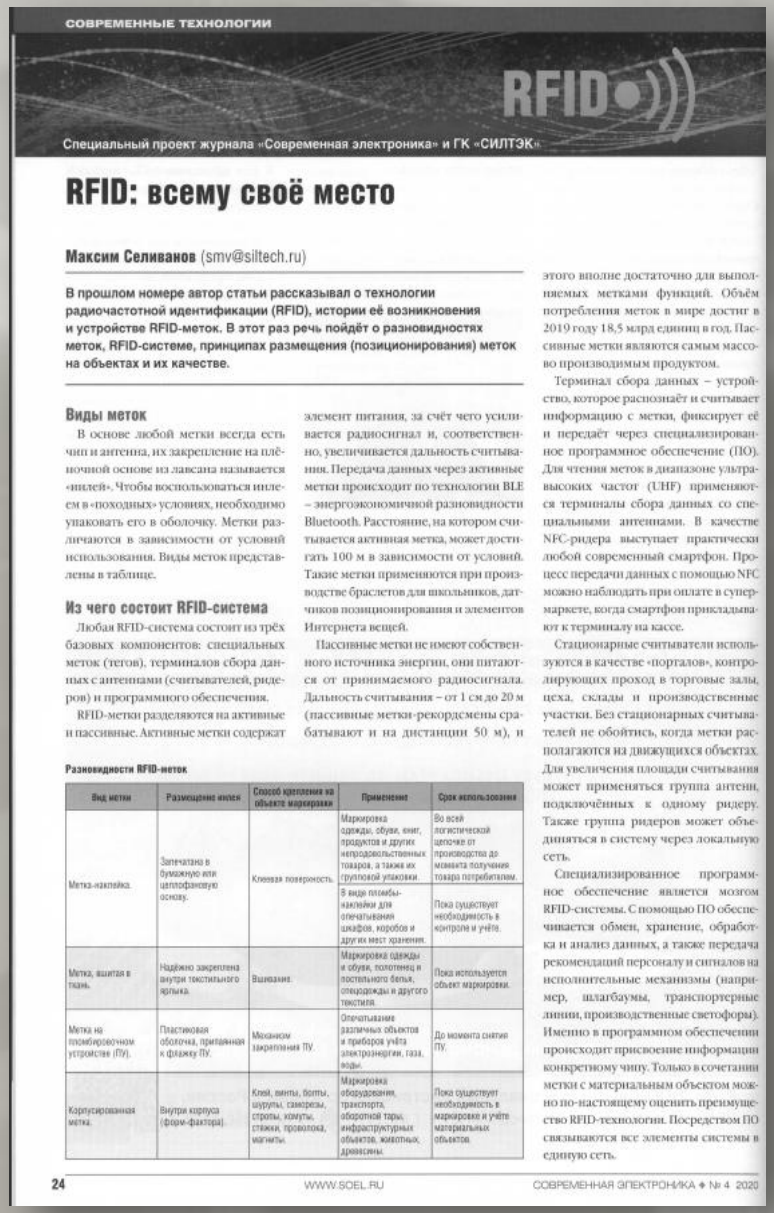
Рис. 1. RFID-метка S-Tag 3D Slim M на неодимовых магнитах

Рис. 2. S-TAG 3D slim F низкопрофильная метка с обтекаемым корпусом

Рис. 3. Разнообразие цветов RFID-меток

Селиванов, М. Разработка RFID-меток: что нового? / М. Селиванов. – Текст : непосредственный // Современная электроника. - 2020. - № 6. - С. 14-15.

О новшествах рынка RFID-меток, их особенностях и различиях.



СОВРЕМЕННЫЕ ТЕХНОЛОГИИ

RFID

Специальный проект журнала «Современная электроника» и ГК «СИЛТЭК»

RFID: всему своё место

Максим Селиванов (smv@siltech.ru)

В прошлом номере автор статьи рассказывал о технологии радиочастотной идентификации (RFID), истории её возникновения и устройстве RFID-меток. В этот раз речь пойдёт о разновидностях меток, RFID-системе, принципах размещения (позиционирования) меток на объектах и их качестве.

Виды меток

В основе любой метки всегда есть чип и антенна, их закрепление на плёночной основе из лавсана называется «инлей». Чтобы воспользоваться инлеем в «походных» условиях, необходимо упаковать его в оболочку. Метки различаются в зависимости от условий использования. Виды меток представлены в таблице.

Из чего состоит RFID-система

Любая RFID-система состоит из трёх базовых компонентов: специальных меток (тегов), терминалов сбора данных с антеннами (считывателей, ридеров) и программного обеспечения.

RFID-метки разделяются на активные и пассивные. Активные метки содержат элемент питания, за счёт чего усиливается радиосигнал и, соответственно, увеличивается дальность считывания. Передача данных через активные метки происходит по технологии BLE – энергоэкономичной разновидности Bluetooth. Расстояние, на котором считывается активная метка, может достигать 100 м в зависимости от условий. Такие метки применяются при производстве браслетов для школьников, датчиков позиционирования и элементов Интернета вещей.

Пассивные метки не имеют собственного источника энергии, они питаются от принимаемого радиосигнала. Дальность считывания – от 1 см до 20 м (пассивные метки-рекордсмены срабатывают и на дистанции 50 м), и этого вполне достаточно для выполняемых метками функций. Объём потребления меток в мире достиг в 2019 году 18,5 млрд единиц в год. Пассивные метки являются самым массово производимым продуктом.

Терминал сбора данных – устройство, которое распознаёт и считывает информацию с метки, фиксирует её и передаёт через специализированное программное обеспечение (ПО). Для чтения меток в диапазоне ультравысоких частот (UHF) применяются терминалы сбора данных со специальными антеннами. В качестве NFC-ридера выступает практически любой современный смартфон. Процесс передачи данных с помощью NFC можно наблюдать при оплате в супермаркете, когда смартфон прикладывают к терминалу на кассе.

Стационарные считыватели используются в качестве «порталов», контролирующих проход в торговые залы, цеха, склады и производственные участки. Без стационарных считывателей не обойтись, когда метки располагаются на движущихся объектах. Для увеличения площади считывания может применяться группа антенн, подключённых к одному ридеру. Также группа ридеров может объединяться в систему через локальную сеть.

Специализированное программное обеспечение является мозгом RFID-системы. С помощью ПО обеспечивается обмен, хранение, обработка и анализ данных, а также передача рекомендаций персоналу и сигналов на исполнительные механизмы (например, шлагбаумы, транспортерные линии, производственные светофоры). Именно в программном обеспечении происходит присвоение информации конкретному чипу. Только в сочетании метки с материальным объектом можно по-настоящему оценить преимущество RFID-технологии. Посредством ПО связываются все элементы системы в единую сеть.

Разновидности RFID-меток

Вид метки	Размещение инлея	Способ крепления на объекте маркировки	Применение	Срок использования
Метка-наклейка.	Запечатано в бумажную или целлофановую основу.	Клеевая поверхность.	Маркировка одежды, обуви, книг, продуктов и других непродовольственных товаров, а также их групповой упаковки.	Во всей логистической цепочке от производства до момента получения товара потребителем.
			В виде пломбы-наклейки для опечатывания шкафов, коробов и других мест хранения.	Пока существует необходимость в контроле и учёте.
Метка, вшитая в ткань.	Надёжно закреплена внутри текстильного ярлыка.	Вшивание.	Маркировка одежды и обуви, полотенец и постельного белья, спецодежды и другого текстиля.	Пока используется объект маркировки.
Метка на пломбировочном устройстве (ПУ).	Пластиковая оболочка, притянная к фрагменту ПУ.	Механизм закрепления ПУ.	Опечатывание различных объектов и приборов учёта электроэнергии, газа, воды.	До момента снятия ПУ.
Корпусированная метка.	Внутри корпуса (форм-фактора).	Клей, винты, болты, шурупы, саморезы, стропы, хомуты, стяжки, проволока, магниты.	Маркировка оборудования, транспорта, оборотной тары, инфраструктурных объектов, животных, древесины.	Пока существует необходимость в маркировке и учёте материальных объектов.

Селиванов, М. RFID: всему свое место / М. Селиванов. - Текст : непосредственный // Современная электроника. - 2020. - № 4. - С. 24-25.

О разновидностях меток, RFID-системе, принципах размещения меток на объектах и их качестве.

КОЛОНКА РЕДАКТОРА

Защита средств защиты

Системы идентификации с защитой от копирования

Мнения экспертов

Системы контроля доступа редко играют роль систем физической защиты объекта. Зачастую они являются средством упорядочивания маршрутов движения персонала и контроля дисциплины, а в остальных случаях используются в связке с видеонаблюдением и охранной сигнализацией. Эксперты компаний PERCo, ЗАО НВП "Болид", "AAM Системз" и HID Global обсудили способы защиты идентификаторов от копирования, наиболее распространенные протоколы обмена информацией, технологии визуальной защиты карт, возможность копирования биометрических идентификаторов, а также где хранятся рисунки отпечатков пальцев

Игорь Ядрихинский
Заместитель директора
Дивизиона маркетинга
компании PERCo

Павел Соколов
Руководитель направления СКД
ЗАО НВП "Болид"

Какие методы наиболее распространены и эффективны при защите от копирования в RFID-системах при передаче данных идентификатора на считыватель?

Павел Соколов,
ЗАО НВП "Болид"

Алексей Гинце
Редактор раздела "Системы контроля и управления доступом", директор по связям с общественностью компании "ААМ Системз"

Системы идентификации с защитой от копирования. Мнения экспертов / И. Ядрихинский, П. Соколов, Д. Шипелов, С. Гордеев. - Текст : непосредственный // Системы безопасности = Security and safety. - 2019. - № 5 (149). - С. 114-118.

В статье эксперты крупных компаний обсудили способы защиты идентификаторов от копирования, наиболее распространенные протоколы обмена информацией, технологии визуальной защиты карт, возможность копирования биометрических идентификаторов, а также где хранятся рисунки отпечатков пальцев.

СПбГУТ))) ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
Март 2018 Том 6 № 1 ISSN 2307-1303 http://www.ittsut.ru
TELECOM IT
March 2018 Vol. 6 Iss. 1 ISSN 2307-1303 http://www.ittsut.ru

ОБЗОР ТЕХНОЛОГИЙ И СТАНДАРТОВ RFID СИСТЕМ

Н. А. Верзун[1], Д. М. Воробьева[2*], А. М. Колбанёв[3], М. О. Колбанёв[1]

[1] СПбГЭТУ «ЛЭТИ», Санкт-Петербург, 197376, Российская Федерация
[2] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
[3] АО «ЭР-Телеком Холдинг», Санкт-Петербург, 194352, Российская Федерация
* Адрес для переписки: vorobyeva.dm@spbgut.ru

Аннотация

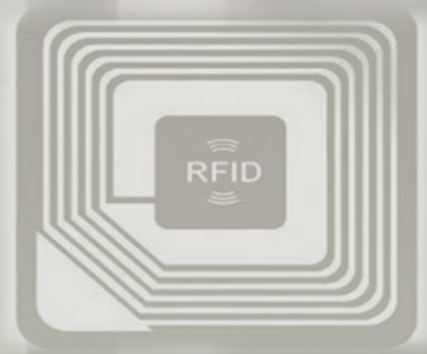
Предмет исследования. Данная статья посвящена обзору современных технологий построения систем RFID идентификации, являющихся неотъемлемой частью интернета вещей. Рассматриваются общие характеристики RFID систем и их сравнение с другими методами идентификации, классификация технологий построения меток, особенности активных, полупассивных и пассивных RFID меток с чипом, вопросы стандартизации RFID технологий. **Метод.** В основе исследования лежит анализ технических решений, принимаемых производителями RFID меток и разработчиков соответствующих стандартов. **Основной результат.** Полученный обзор в отличии от известных выявляет основные особенности пассивных и активных меток с чипом, что позволяет принимать рациональные решения при выборе элементной базы систем RFID идентификации. **Практическая значимость** полученных результатов состоит в создании научно обоснованных рекомендаций по созданию и планированию RFID систем и их использования при построении приложений интернета вещей.

Ключевые слова
Интернет вещей, идентификация объектов, RFID система, стандартизация RFID технологий.

Информация о статье
УДК 004.087
Язык статьи – русский.
Поступила в редакцию 11.01.18, принята к печати 28.02.18.

Ссылка для цитирования: Верзун Н. А., Воробьева Д. М., Колбанёв А. М., Колбанёв М. О. Обзор технологий и стандартов RFID систем // Информационные технологии и телекоммуникации. 2018. Том 6. № 1. С. 1–11.

Обзор технологий и стандартов RFID систем / Н. А. Верзун, Д. М. Воробьева, А. М. Колбанёв, М. О. Колбанёв. - Текст : непосредственный // Информационные технологии и телекоммуникации. - 2018. - Том 6, № 1. - С. 1-11. - ISSN 2307-1303.



Статья посвящена обзору современных технологий построения систем RFID идентификации, являющихся неотъемлемой частью интернета вещей. Рассматриваются общие характеристики RFID систем и их сравнение с другими методами идентификации, классификация технологий построения меток, особенности активных, полупассивных и пассивных RFID меток с чипом, вопросы стандартизации RFID.

УДК 007.53

ПРОБЛЕМЫ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ И ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ В СРЕДЕ ИНТЕРНЕТ ВЕЩЕЙ

В. Д. Артемьева[1], А. Ю. Гришенцев[2], Д. И. Дикий[2], А. Г. Коробейников[2,3]

[1]Балтийский федеральный университет им. И. Канта
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[3]Санкт-Петербургский филиал Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук

В работе рассмотрены проблемы информационной безопасности на уровне беспроводных сенсорных и исполнительных устройств среды Интернет вещей. Рассмотрены аспекты применения технологии радиочастотной идентификации и методы повышения уровня защищенности. Описаны проблемы безопасности сенсорных сетей.

Интернет вещей, безопасность, исполнительные и сенсорные устройства, RFID-технологии, беспроводные сенсорные сети.

Прогнозируется, что в третьем десятилетии XXI века число устройств, подключенных к среде Интернет вещей [1] превысит 18 млрд устройств. Наряду с большим распространением и внедрением этих технологий в повседневную жизнь людей, а также в промышленные процессы, немаловажным становится вопрос о безопасности. Здесь под безопасностью подразумевается не только физическая безопасность устройств от хищения или уничтожения, но и все другие аспекты информационной безопасности, свойственные автоматизированным системам, обрабатывающим информацию [2, 3, 4]. Под угрозой становятся процессы приема и передачи информации, ее обработки и хранения с учетом особенностей устройств, подключаемых к среде Интернет вещей [5].

Как правило, принято изначально рассматривать архитектуру среды Интернет вещей [6]. Здесь существует множество мнений о том, сколько всего можно выделить слоев в данной системе, также распределение их границ, взаимосвязей и другое. Например, в архитектуре ITU-T Y.2002 предлагается разделение на 3 слоя [7]. Однако, все они сходятся к тому, что основой среды Интернет вещей являются исполнительные и сенсорные устройства. Объединяя в сеть десятки и сотни таких устройств под управлением одним или несколькими вычислительными центрами [8, 9] (или в случае для самоопределяющихся ad-hoc сетей [10] – самими устройства-

Проблемы безопасности беспроводных сенсорных и исполнительных устройств в среде интернет вещей / В. Д. Артемьева, А. Ю. Гришенцев, Д. И. Дикий, А. Г. Корабейников. - Текст : непосредственный // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018), Санкт-Петербург, 28 февраля - 01 марта 2018 г. : VII Международная научно-техническая и научно-методическая конференция : сборник научных статей : в 4 томах / под редакцией С. В. Бачевского. - 2018. - Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. М. А. Бонч-Бруевича. – Том 2. - С. 49-53. - ISSN 2307-1303. - Имеется электронная версия печатной публикации: URL: http://www.sut.ru/doci/nauka/7apino/APINO%202018-T2.pdf (дата обращения: 02.02.2022).

В работе рассмотрены проблемы информационной безопасности на уровне беспроводных сенсорных и исполнительных устройств среды Интернет вещей. Рассмотрены аспекты применения технологии радиочастотной идентификации и методы повышения уровня защищенности. Описаны проблемы безопасности сенсорных

Человек и RFID

Доктор физико-математических наук
И.Б.Вендик,
кандидат технических наук
И.В.Мунина
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)

Зачем три пилота и их корабль, вернувшись из рейса EH101—EH2657, сделались источниками радиоволн с длиной волны шесть и восемьдесят три тысячных? Нас исследовали врачи. Нас исследовали физики. Все пришли к единственному выводу: это невозможно. Можно было умереть от смеха, глядя на их удивленные лица.

А. и Б.Стругацкие. Полдень, XXII век

Постановка задачи

«Химия и жизнь» уже писала (2009, 2) о системах радиочастотной идентификации, RFID (Radio Frequency Identification). На любой объект, хоть на контейнер для морских перевозок, хоть на галстук-бабочку в магазине, можно наклеить метку — микросхемку, приемопередатчик с антенной, которая по запросу сообщает информацию. Например, что в контейнере лежит и кто изготовитель этой тряпочки.

С другой стороны, медики используют системы так называемого мониторирования чтобы отслеживать, скажем, в течение суток параметры человека — температуру тела, пульс, давление крови и др. Эти системы пишут информацию на флешку, с которой ее потом можно и скачать, и просмотреть.

А что делать, если надо не через сутки, а сразу? Установить радиометку и устройство для регистрации параметра на человека или внутрь него и принимать сигнал с некоторого расстояния. На словах-то все просто... Возникающим при этом проблемам посвящена данная статья; проблемы эти понемногу решаются, и системы дистанционного контроля и оценки состояния биологических объектов находят все больше потребителей.

Вот лишь несколько потенциальных областей их применения. В больницах можно ввести систему контроля разнообразных нарушений в работе организма человека, где информация от радиометок передается с помощью сотовой, Wi-Fi или других видов связи. Если пациент находится дома, а метка умеет передавать информацию через Интернет, врач может связаться с пациентом и определить проблему, исходя из его слов (где и как болит) и данных, собранных системой. Особо важное применение — контроль состояния организма в чрезвычайных ситуациях: пожар, природная или техногенная катастрофа, военные действия и т. п. А метка на упаковке лекарства пригодится в фармацевтике: для хранения информации о препаратах, имеющихся в фондах лечебного заведения или аптеки, для того, чтобы вовремя напомнить об окончании срока хранения данной упаковки.

Из чего состоит

Система радиочастотной идентификации состоит из радиометки и считывателя, тому и другому нужны антенны и системы обработки информации. В радиометке имеется датчик — устройство, которое реагирует на измеряемую величину, например температуру, химсостав, пульс и т. д. Главные особенности радиометки для «человеческих» применений — миниатюрность, совместимость с организмом и возможность считывания с нее информации. Напомним, что метка может находиться и в глубине тканей, а их свойства — высокая диэлектрическая проницаемость и значительное поглощение электромагнитного сигнала — представляют проблему с точки зрения радиотехники.

Принято выделять два вида систем радиоидентификации: работающие в ближнем поле и использующие излучение в дальней зоне. Системы ближнего поля используют магнитную связь между антеннами, на нее не влияют диэлектрические свойства человека, а магнитных у нас с вами почти нет. Однако такая связь возможна только на малых расстояниях. Системы дальнего поля позволяют, кроме собственно передачи информации, обнаружить объект и определить, где он находится, — это необходимо во всякого рода чрезвычайных ситуациях. Но при этом способе передачи диэлектрические свойства человека играют принципиальную роль.

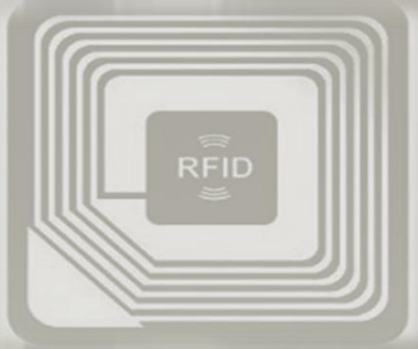
Сами радиометки бывают носимыми (на поверхности тела или одежде) и имплантируемыми — их вводят в организм путем хирургического вмешательства. И те, и другие могут передавать сигнал непосредственно тому устройству, которое его обрабатывает и «понимает», а могут по цепочке, через ретрансляторы. Конкретное решение зависит от того, далеко ли надо его передавать. При этом носимый прибор может просто его усиливать и транслировать, а может и делать что-то свое, например контролировать состояние кожного покрова, и опять же передавать эти данные. Связь между всеми элементами цепочки обеспечивается электромагнитными волнами, распространяющимися внутри или по поверхности тела пациента. Посмотрим, как они это делают и от чего это зависит.

Волна в человеке

Распространение электромагнитной волны в среде определяется в основном двумя параметрами — диэлектрической проницаемостью ε и «потерями», превращением мощности волны в тепло. Потери, в свою очередь, определяются самой обычной проводимостью, той, которая в законе Ома, и так называемыми «диэлектрическими потерями» — теми, благодаря которым греет СВЧ-печь. Попутно — если у вас физика была не только в школе, но и в институте, вы помните, что там вводилось понятие «комплексной диэлектрической проницаемости», — так вот, мнимая ее часть как раз и характеризует эти самые потери.

Диэлектрическая проницаемость биологической ткани велика на низких частотах, в первую очередь потому, что мы состоим в среднем на 70% из воды. У молекул воды очень большой дипольный момент и соответственно диэлектрическая проницаемость на низких частотах. В книжках пишут, что

Вендик, И. Б. Человек и RFID / И. Б. Вендик, И. В. Мунина. - Текст : непосредственный // Химия и жизнь - XXI век. - 2016. - № 11. - С. 20-23 : ил. - Библиогр. в конце ст. - ISSN 1727-5903.



О системах радиочастотной идентификации (RFID) и потенциальных областях их применения.

УДК 004.056
DOI: 10.14489/vkit.2016.07.pp.030-033

А. Б. Левина, канд. физ.-мат. наук, **Д. М. Слепцова** (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Россия);
e-mail: levina@cit.ifmo.ru

АНАЛИЗ АТАК ПО СТОРОННИМ КАНАЛАМ НА RFID-СИСТЕМЫ НА ОСНОВЕ ПРОТОКОЛА MIFARE CLASSIC

Изучена уязвимость систем радиочастотной идентификации к атакам по сторонним каналам. Выявлены уязвимости в шифре криптоалгоритма Crypto-1. Даны описания результатов атаки по электромагнитному излучению на карту, использующую протокол Mifare Classic. Приведен план дальнейшего улучшения характеристик атаки.

Ключевые слова: атаки по сторонним каналам; радиочастотная идентификация; анализ электромагнитного излучения; протокол Mifare Classic.

A. B. Levina, D. M. Sleptsova
(Saint-Petersburg University of Information Technologies, Mechanics and Optics, Saint-Petersburg, Russia)

STUDY OF SIDE-CHANNEL ATTACKS ON RFID SYSTEMS BASED ON MIFARE CLASSIC

RFID (Radio-Frequency IDentification) systems consist of a reader device and passive tags, powered from an electromagnetic field created by a reader. Majority of applications of such systems operate on secret data or financial information, e.g. person identification systems or fare systems. For this reason main part of their operation relies on cryptographic protocols, preserving confidentiality of secret information in transfer or storage. Security estimations of RFID-systems seldom include vulnerabilities to side-channel attacks. Said attacks exploit vulnerabilities in physical implementation of cryptosystem and provide opportunity to recover secret key of a system which is not vulnerable to classical cryptanalysis. In this paper side-channel attacks vulnerabilities of RFID-systems are studied. As a two main approaches to mounting an attack on Mifare Classic protocol power consumption and electromagnetic emanations are used. The attack vector is Crypto-1 algorithm, namely the moment of initialization of the LFSR (Linear Feedback Shift Register) with a secret key. Signal pre-processing included filtration, alignment and decimation of signal. Obtained signal depending on the exploited channel was compared to hypothetical values of power consumption or electromagnetic emanation, acquired on modeling step of the attack. Basis for model of Crypto-1 register was Hamming distance, obtained and hypothetical vectors comparison was made by means of correlation coefficient. As a result full key stored on a tag was recovered. Computing correlation coefficient and key recovery took 4 hours. Current lab setup has long signal acquisition and pre-processing time, that in the future can be shortened by using hardware pre-processing or oscilloscope made in the form of a PCI (Peripheral Component Interconnect) card. Conducted work shows possibility of side-channel exploitation of RFID-systems and proves it with a practical attack on a widely deployed system based on Mifare Classic protocol.

Keywords: Side-channel attacks; Radio-Frequency Identification; Electromagnetic analysis, Mifare Classic protocol.

Статья поступила в редакцию 10.10.2015 г.

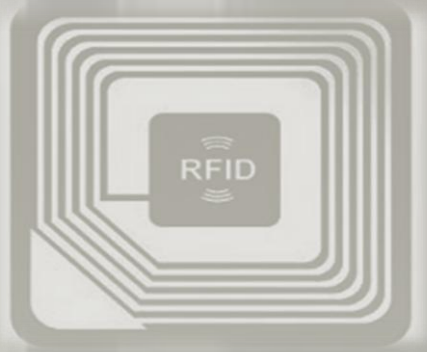
Введение

Радиочастотная идентификация *RFID* (*Radio Frequency IDentification*) – технология беспроводной коммуникации, используемая для идентификации объекта. Согласно стандартам [1 – 4], основными участниками коммуникации являются два компонента: *PICC* (*Proximity Integrated CirCuit*) – интегральная схема ближней зоны, т.е. метка-транспондер; *PCD* (*Proximity Coupling Device*) – устройство ближней связи, что подразумевает под собой устройство чтения.

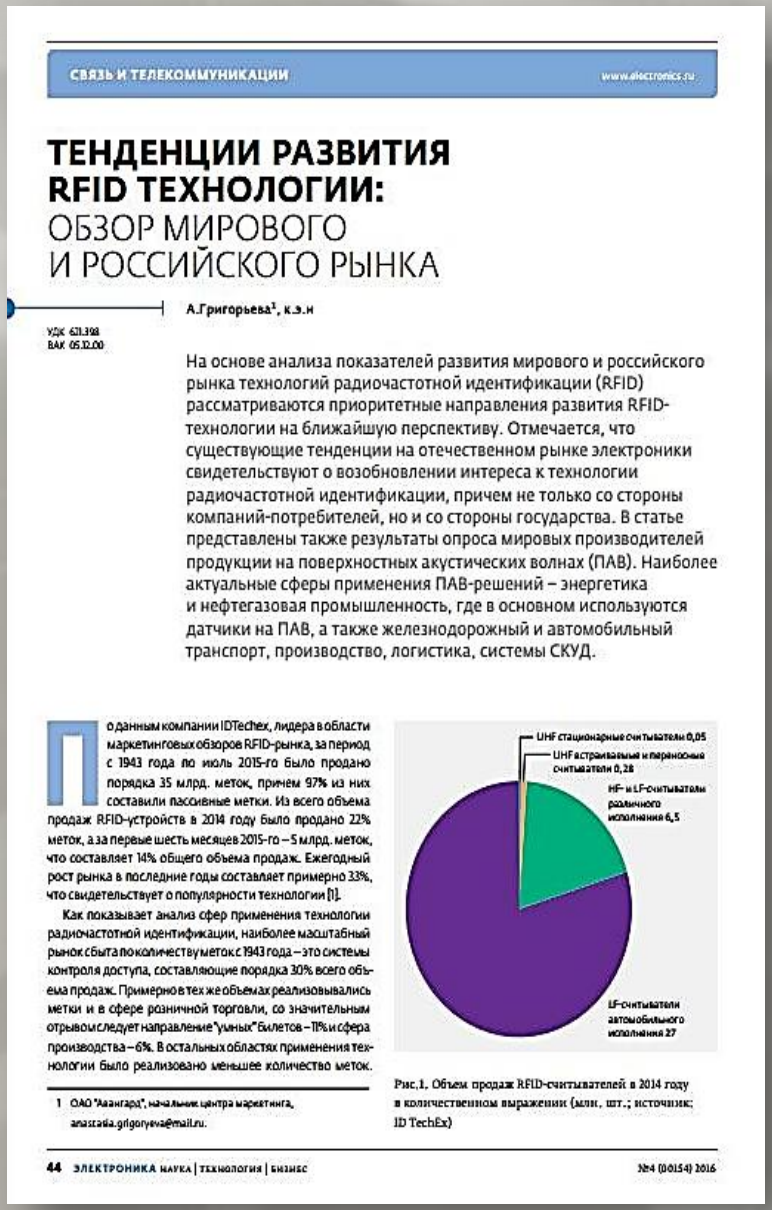
Метки – небольшие и питающиеся пассивно электронные устройства, содержащие данные. Наличие источника питания – важная характеристика для RFID-метки. Пассивные метки не имеют собственного источника питания и не могут самостоятельно начать сеанс. Поэтому энергия, необходимая для работы, должна быть получена от считывателя. Антенная катушка устройства чтения создает сильное высокочастотное электромагнитное поле, которое проникает, перссекает катушку и область вокруг.

Помимо пассивных, существуют активные и полуактивные метки, имеющие в своей конструкции, соответственно, источник питания и передатчик или только источник питания. Благодаря наличию источника питания увеличивается дальность

Левина, А. Б. Анализ атак по сторонним каналам на RFID-системы на основе протокола Mifare Classic = Study of side-channel attacks on RFID systems based on Mifare Classic / А. Б. Левина, Д. М. Слепцова. - Текст : непосредственный // Вестник компьютерных и информационных технологий. - 2016. - № 7. - С. 30-33. - Библиогр.: с. 33 (11 назв.). - ISSN 1810-7206.



В статье изучена уязвимость систем радиочастотной идентификации к атакам по сторонним каналам. Даны описания результатов атаки по электромагнитному излучению на карту, использующую протокол Mifare Classic. Приведен план дальнейшего улучшения характеристик атаки.



СВЯЗЬ И ТЕЛЕКОММУНИКАЦИИ www.elocctronics.ru

ТЕНДЕНЦИИ РАЗВИТИЯ RFID ТЕХНОЛОГИИ: ОБЗОР МИРОВОГО И РОССИЙСКОГО РЫНКА

А.Григорьева[1], к.э.н

УДК 621.398
ВАК 05.12.00

На основе анализа показателей развития мирового и российского рынка технологий радиочастотной идентификации (RFID) рассматриваются приоритетные направления развития RFID-технологии на ближайшую перспективу. Отмечается, что существующие тенденции на отечественном рынке электроники свидетельствуют о возобновлении интереса к технологии радиочастотной идентификации, причем не только со стороны компаний-потребителей, но и со стороны государства. В статье представлены также результаты опроса мировых производителей продукции на поверхностных акустических волнах (ПАВ). Наиболее актуальные сферы применения ПАВ-решений – энергетика и нефтегазовая промышленность, где в основном используются датчики на ПАВ, а также железнодорожный и автомобильный транспорт, производство, логистика, системы СКУД.

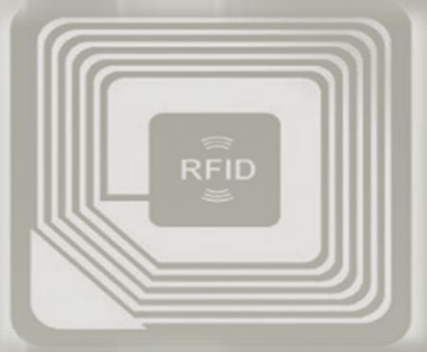
По данным компании IDTechEx, лидера в области маркетинговых обзоров RFID-рынка, за период с 1943 года по июль 2015-го было продано порядка 35 млрд. меток, причем 97% из них составили пассивные метки. Из всего объема продаж RFID-устройств в 2014 году было продано 22% меток, а за первые шесть месяцев 2015-го – 5 млрд. меток, что составляет 14% общего объема продаж. Ежегодный рост рынка в последние годы составляет примерно 33%, что свидетельствует о популярности технологии [1].

Как показывает анализ сфер применения технологии радиочастотной идентификации, наиболее масштабный рынок сбыта по количеству меток с 1943 года – это системы контроля доступа, составляющие порядка 30% всего объема продаж. Примерно в тех же объемах реализовывались метки и в сфере розничной торговли, со значительным отрывом следует направление "умных" билетов – 11% и сфера производства – 6%. В остальных областях применения технологии было реализовано меньшее количество меток.

Рис.1. Объем продаж RFID-считывателей в 2014 году в количественном выражении (млн. шт.; источник: ID TechEx)

1 ОАО "Авангард", начальник центра маркетинга, anastasia.grigoryeva@mail.ru.

Григорьева, А. Тенденции развития RFID-технологии : обзор мирового и российского рынка / А. Григорьева. - Текст : непосредственный // Электроника: наука, технология, бизнес. - 2016. - № 4. - С. 44-49. - ISSN 1992-4178.



В статье проанализированы показатели мирового и российского рынка технологий радиочастотной идентификации (RFID) и приоритетные направления развития этих технологий на ближайшую перспективу.

72 СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ www.all-over-ip.ru

ALL-OVER-IP

18–19 ноября 2015
Москва, Сокольники

Identity Management and Access Control: новый образ рынка управления идентификацией и контроля доступа

В 2014 г. объем мирового рынка СКУД (исключая Китай) превысил 3 млрд долларов. В 2018 г. достигнет 8,6 млрд, а в 2020 г. – 10,4 млрд (по данным IHS и MarketsandMarkets).
СКУД движутся к открытым платформам, открытым интерфейсам и масштабированию под требования пользователей. Считыватели, читающие карты разного формата или работающие одновременно с биометрией, RFID и PIN, кардинально меняют СКУД.
Устройства на базе стандартизированных протоколов, мультифункциональные считыватели, мобильные идентификаторы, беспроводные онлайн-замки, биометрические и облачные технологии стимулируют бизнес инсталляторов и интеграторов.
Лидеры индустрии контроля доступа и управления идентификацией рассказывают о технологиях будущего, которые будут представлены на форуме All-over-IP Expo 2015

Олег Тихонов
Директор Департамента интегрированных систем компании "АРМО-Системы"

Технологические тренды от "АРМО-Системы"

В качестве яркой и высокотехнологичной новинки в нашем продуктовом портфеле я отметил бы решение для доступа с помощью мобильных телефонов, разработанное компанией HID Global. Здесь применены самые современные технологии, в том числе облачный сервис, а обмен информацией между считывателем и смартфоном реализован на базе NFC и Bluetooth. Надежность, удобство использования и поддержка всех самых распространенных мобильных операционных систем, скорее всего, обеспечат этой технологии популярность у пользователей в весьма недалеком будущем.

Новинки "АРМО-Системы" на All-over-IP Expo 2015

В этом году на All-over-IP Expo мы делаем упор на бюджетную линейку СКУД марки Smartec, что, в первую очередь, диктуется текущими состояниями рынка. Планируем также показать интеграцию СКУД/СУРВ Smartec с системой видеонаблюдения этой марки и охранной сигнализацией Satel. Основной новинкой нашей экспозиции является контроллер СКУД собственной разработки, в котором запланирована реализация глобальных логических связей без участия ПК. ■

Александр Рыжов
Технический директор компании "ПромАвтоматика"

Технологические тренды от "ПромАвтоматика"

1. Защищенная идентификация на базе карт MIFARE. Традиционно распространенные карточки (EM Marine, HID Prox) легко копируются. Мы предлагаем решение этой проблемы на базе карт MIFARE. Среди линейки MIFARE можно найти как простые карты Classic, обеспечивающие достаточный уровень защиты для многих применений, так и карты Plus, в которых применяется стойкое AES-шифрование.
2. Работа с беспроводными замками. Плюс к традиционным проводным контроллерам мы поддерживаем беспроводные интегрированные замки ряда производителей. Недавно импульс развитию этой теме дало появление стандарта SOAA, позволившего легче комбинировать замки разных производителей на одном внедрении.
3. Алкотестирование на проходных. Недавно на рынке появились алкотестеры, которые имеют потенциал глубокой интеграции со СКУД, снятие результатов тестирования с них. Мы можем протоколировать результаты в отчеты, устанавливать индивидуальные пороги допустимого опьянения разным отделам. ■

Вячеслав Шашков
Генеральный директор компании "АСТЕРО"

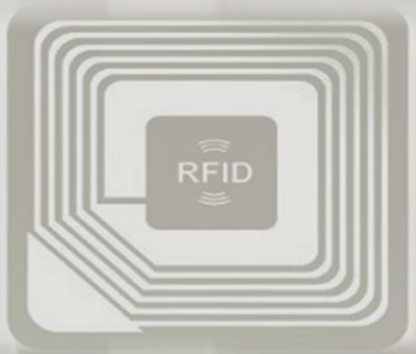
Технологические тренды от "АСТЕРО"

Мы занимаемся видеодомофонными системами (ВДС), являющимися составной частью СКУД. Мы абсолютно уверены, что будущее как в СКУД, так и в ВДС – за передачей данных по интернет-протоколам. В частности, в предлагаемом нами оборудовании ВДС компании Guinaz (Испания) и компании 2N (Чехия) используется набирающий все большую популярность протокол SIP, который позволяет строить мобильные, легко расширяемые ВДС и собственно системы телефонной связи. Большим плюсом также является возможность использовать в ВДС в качестве ответной части смартфон или планшет.

Новинки "АСТЕРО" на All-over-IP Expo 2015

Основной темой нашего участия в форуме All-over-IP Expo 2015 являются IP-видеодомофонные системы.
Мы покажем работу ВДС различных производителей в интеграции со СКУД, SIP-телефонией и IP-видеокамерами. Будут представлены решения как для жилого сектора, так и для офисных центров, индустриальных зданий, протяженных промышленных площадок. ■

Identity Management and Access Control: новый образ рынка управления идентификацией и контроля доступа / О. Тихонов, А. Рыжов, В. Шашков [и др.]. - Текст : непосредственный // Системы безопасности. - 2015. - № 4 (124). - С. 72-75.



СКУД движутся к открытым платформам, открытым интерфейсам и масштабированию под требования пользователей. Считыватели, читающие карты разного формата или работающие одновременно с биометрией, RFID и PIN, кардинально меняют СКУД. Лидеры индустрии контроля доступа и управления идентификацией рассказывают о технологиях будущего, которые будут представлены на форуме All-over-IP Expo 2015.

Радиочастотная идентификация

О развитии возможностей RFID-систем

В развитых странах разработаны и активно применяются стандарты, обеспечивающие внедрение технологий радиочастотной идентификации – RFID для унификации содержания и структуры данных о распознаваемом объекте (EPC-метки, EPC-электронный код продукта). Это позволяет на основе международных стандартов поддерживать преемственность технологий автоматической идентификации и осуществлять итерационный поэтапный переход, к примеру, от метода маркирования товаров штриховыми кодами к RFID-технологиям (в том числе может быть применено одновременное их использование). При этом значительно расширяются возможности и эффективность товаро-транспортных и логистических систем.

Виктор Дравица, директор Центра систем идентификации НАН Беларуси, кандидат физико-математических наук

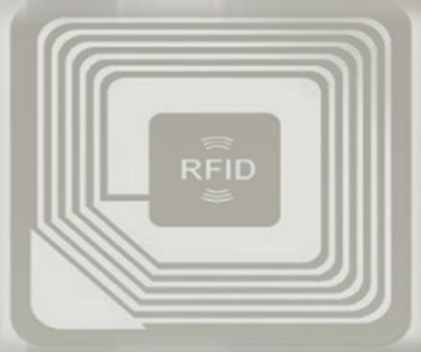
Александр Решетняк, заместитель технического директора Центра систем идентификации НАН Беларуси

Игорь Равин, начальник лаборатории технических средств радиочастотной идентификации Центра систем идентификации НАН Беларуси

Технологии автоматической идентификации начали формироваться с 1973 г., когда был принят первый стандарт по обозначению продукции штриховыми кодами [1]. В 2003 г. Международной ассоциацией GS1 была создана отдельная организация, которая обеспечивает техническое развитие и стандартизацию EPC/RFID-технологий, – EPCglobal. В 2004 г. ею была опубликована первая версия международного стандарта, определяющего основные физические и логические требования для RFID-систем, считывателей и RFID-меток, а также радиоинтерфейса. В 2005 г. эту инициативу поддержал Международный комитет по стандартизации ISO, которым был утвержден стандарт ISO/IEC 18000–6C, включающий в себя требования стандарта EPC Gen2. В период 2008–2013 гг. он несколько раз дорабатывался в связи с бурным развитием RFID-технологий. В прошлом году в ISO/IEC 18000–63 включена окончательная редакция EPC Gen2v2, которая совместима с предыдущей и имеет дополнительные возможности, включая криптозащиту данных и аутентификацию доступа [2]. Также новой редакцией документа для обеспечения достоверности происхождения товара предусмотрено использование расширенной памяти метки в решениях, которые требуют больших описаний продукции (например, пеленгатонка, техническое обслуживание и пр.) [3].

Стандарт EPC Gen2v2 может применяться для реализации RFID-систем различного назначения: в аэрокосмической отрасли, оборонной и фарма-

Дравица, В. О развитии возможностей RFID-систем / В. Дравица, А. Решетняк, И. Равин. - Текст : непосредственный // Наука и инновации. - 2015. - № 4. - С. 8-12 : 3 фот. - Библиогр.: с. 12 (7 назв.). - ISSN 1818-9857.



О международных стандартах, обеспечивающих внедрение технологий радиочастотной идентификации.

82 СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ www.all-over-ip.ru

КОЛОНКА РЕДАКТОРА

И швец, и жнец, и на дуде игрец!

Многофункциональность в СКУД лучше иллюстрировать в контексте считывателей и идентификаторов. Простейший пример – считыватель, совмещенный с клавиатурой для ввода PIN. Другой сегмент СКУД, где многофункциональность широко распространена, – считыватели с возможностью чтения карт разного формата и даже разных производителей. Часто такие считыватели предназначены для безболезненной миграции старых систем на современные технологии, например с Proximity на Smart или с оборудования одного производителя на оборудование другого.

На отечественном рынке лет 10 назад появились многофункциональные RFID-считыватели, позволяющие одновременно использовать пассивные карты с малой дальностью для идентификации персонала и дальнобойные идентификаторы для автотранспорта, читаемые на расстоянии нескольких метров.

- RFID-метки 2,4 ГГц.
- Proximity-карты 125 кГц (EmMarin и HID).
- Smart-карты 13,56 МГц (MIFARE и iClass).

Нельзя сказать, что такие задачи были очень распространенными, но они встречаются, и их можно решить с помощью имеющегося оборудования.

Появление биометрических технологий привело к разработке считывателей, работающих одновременно на нескольких технологиях (биометрические, RFID, PIN). Использование бесконтактных Smart-карт в сочетании с биометрией дало синергетический эффект, поскольку биометрический темплейт стало возможным хранить не в памяти считывателя, а на карте. Это снимало проблему ограничения количества пользователей на одном считывателе.

Появляется все больше многофункциональных считывателей, объединяющих не просто несколько технологий идентификации, а функции, относящиеся к разным сегментам рынка СКУД и не только. Пример – объединение в одном устройстве: биометрического и RFID-считывателей, клавиатуры, контроллера СКУД, вызывной панели IP-видеодомофона, видеокамеры, терминала учета рабочего времени. И все это работает! Другой пример – две разных биометрических технологии в одном считывателе.

Термин МФУ (многофункциональное устройство) уже актуален не только в области офисной техники. Получается такой "и швец, и жнец", не знаю, как насчет игры на дуде, но очень интересно, что из этого в результате выйдет.

Алексей Гинце

Редактор раздела "Системы контроля и управления доступом"

Обзор новинок СКУД первой половины 2015 г.

Новости рынка RFID

Согласно маркетинговым исследованиям компании J'son & Partners Consulting, в 2014 г. мировой рынок RFID-технологий вырос на 14,5% и составил 11,1 млрд долл. Действительно, в последние годы оборудование RFID широко применяется в самых различных областях – транспортная инфраструктура, системы безопасности, финансовый сектор, сельское хозяйство, логистика, ритейл и др. Что же сегодня предлагает рынок RFID в России?

Алексей Гинце
Директор по связям с общественностью компании "ААМ Система"

Рассматривая текущую ситуацию в сегменте RFID, можно выделить ряд интересных новинок, которые по своей функциональности отражают важные тренды, характерные для данной области.

Мультитехнологичные считыватели iCLASS SE®

HID Global расширяет свою платформу iCLASS SE® для предоставления новых возможностей в сфере контроля доступа. Новые считыватели multiCLASS SE® с функцией Trust & Go для мобильного доступа усиливают платформу, повышая уровень безопасности, конфиденциальности и удобства использования.

Считыватели multiCLASS SE® от HID Global имеют две основные функции, отличающие их от аналогичных устройств других производителей и отвечающие потребностям рынка СКУД.

1. Способность одновременного чтения карт доступа различных технологий, используемых сегодня в СКУД (HID Prox, EM4102, iCLASS, iCLASS SE®, MIFARE Classic, MIFARE DESFire EV1, iCLASS Seos). Данная функция облегчает переход на новые, более защищенные технологии на объектах, построенных на традиционных технологиях, ставших уязвимыми для взлома.
2. Поддержка смартфонов с технологиями NFC и Bluetooth, что позволяет использовать новый класс переносных средств идентификации в системах контроля доступа.

В условиях возрастающего числа угроз считывателем multiCLASS SE® обеспечивают возможность гибкого перехода от старых, ставших уязвимыми технологий идентификации к новым, более защищенным. Кроме того, в будущем, если технология станет уязвимой, нет необходимости в замене оборудования, достаточно будет осуществить его перепрошивку, обеспечив новый уровень безопасности.

В современном мире мобильные устройства стали незаменимыми техническими средствами, которые всегда под рукой. Использование мобильных устройств для открывания дверей означает эволюцию систем физического контроля доступа, так как это позволяет объединить безопасность и комфорт.

Смартфон в качестве идентификатора

Рынок мобильных технологий по праву считается одним из наиболее инновационных и динамично развивающихся сегментов.

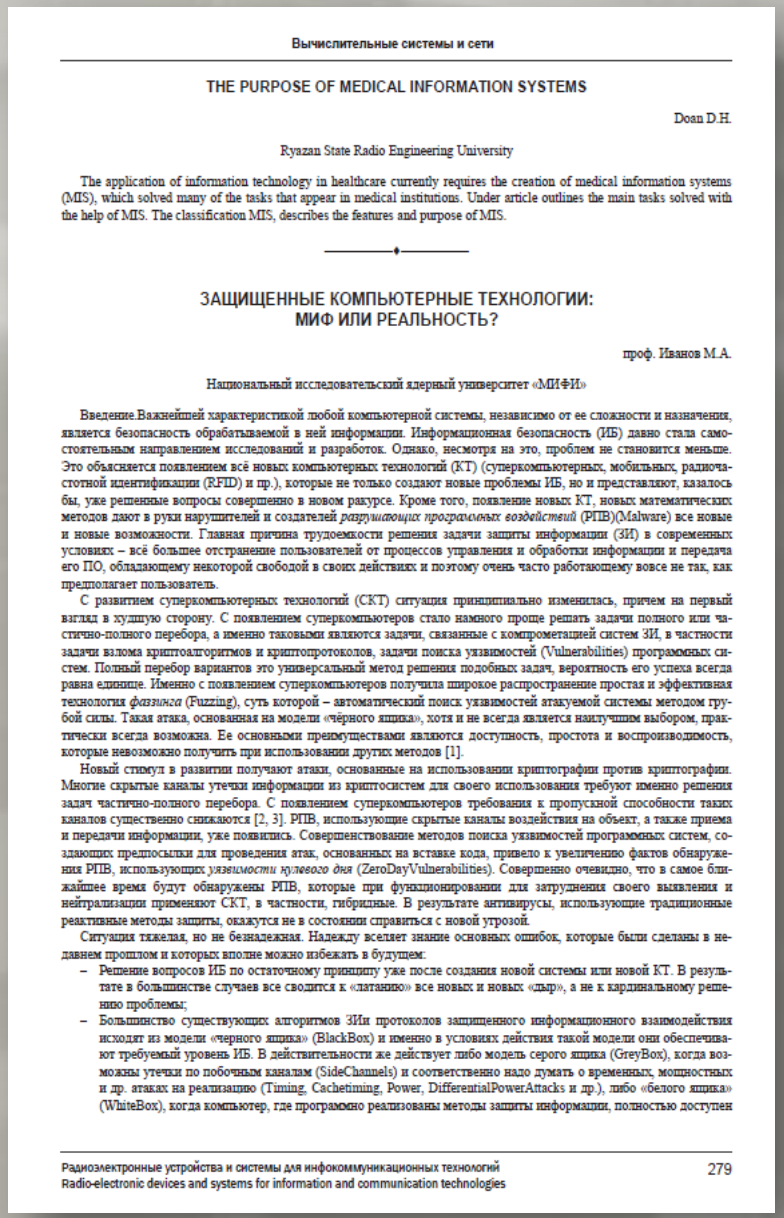
Растущий образовательный уровень потребителей в области использования бесконтактных приложений и технологий, таких как NFC и Bluetooth, делает эти технологии весьма привлекательными для организации мобильного контроля доступа.

В 2013 г. компания Google представила технологию Host-based Card Emulation (HCE). HCE позволяет эмулировать бесконтактную

Смартфон в качестве идентификатора – чтение по Bluetooth

Гинце, А. Обзор новинок СКУД первой половины 2015 г. Новости рынка RFID / Алексей Гинце. - Текст : непосредственный // Системы безопасности. - 2015. - № 3 (123). - С. 82-85.

Согласно маркетинговым исследованиям компании J'son & Partners Consulting, в 2014 мировой рынок RFID-технологий вырос на 14, 5% и составил 11, 1 млрд долл. Действительно, в последние годы оборудование RFID широко применяется в самых различных областях - транспортная инфраструктура, системы безопасности, финансовый сектор, сельское хозяйство, логистика, ритейл и др. Что же сегодня предлагает рынок RFID в России?



Вычислительные системы и сети

THE PURPOSE OF MEDICAL INFORMATION SYSTEMS

Doan D.H.

Ryazan State Radio Engineering University

The application of information technology in healthcare currently requires the creation of medical information systems (MIS), which solved many of the tasks that appear in medical institutions. Under article outlines the main tasks solved with the help of MIS. The classification MIS, describes the features and purpose of MIS.

ЗАЩИЩЕННЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ:
МИФ ИЛИ РЕАЛЬНОСТЬ?

проф. Иванов М.А.

Национальный исследовательский ядерный университет «МИФИ»

Введение.Важнейшей характеристикой любой компьютерной системы, независимо от ее сложности и назначения, является безопасность обрабатываемой в ней информации. Информационная безопасность (ИБ) давно стала самостоятельным направлением исследований и разработок. Однако, несмотря на это, проблем не становится меньше. Это объясняется появлением всё новых компьютерных технологий (КТ) (суперкомпьютерных, мобильных, радиочастотной идентификации (RFID) и пр.), которые не только создают новые проблемы ИБ, но и представляют, казалось бы, уже решенные вопросы совершенно в новом ракурсе. Кроме того, появление новых КТ, новых математических методов дают в руки нарушителей и создателей *разрушающих программных воздействий* (РПВ)(Malware) все новые и новые возможности. Главная причина трудоемкости решения задачи защиты информации (ЗИ) в современных условиях – всё большее отстранение пользователей от процессов управления и обработки информации и передача его ПО, обладающему некоторой свободой в своих действиях и поэтому очень часто работающему вовсе не так, как предполагает пользователь.

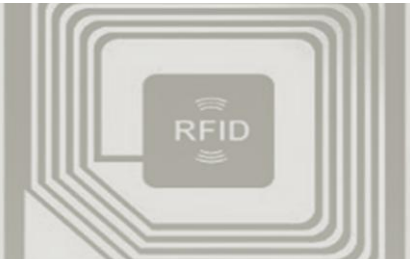
С развитием суперкомпьютерных технологий (СКТ) ситуация принципиально изменилась, причем на первый взгляд в худшую сторону. С появлением суперкомпьютеров стало намного проще решать задачи полного или частично-полного перебора, а именно таковыми являются задачи, связанные с компрометацией систем ЗИ, в частности задачи взлома криптоалгоритмов и криптопротоколов, задачи поиска уязвимостей (Vulnerabilities) программных систем. Полный перебор вариантов это универсальный метод решения подобных задач, вероятность его успеха всегда равна единице. Именно с появлением суперкомпьютеров получила широкое распространение простая и эффективная технология *фаззинга* (Fuzzing), суть которой – автоматический поиск уязвимостей атакуемой системы методом грубой силы. Такая атака, основанная на модели «чёрного ящика», хотя и не всегда является наилучшим выбором, практически всегда возможна. Ее основными преимуществами являются доступность, простота и воспроизводимость, которые невозможно получить при использовании других методов [1].

Новый стимул в развитии получают атаки, основанные на использовании криптографии против криптографии. Многие скрытые каналы утечки информации из криптосистем для своего использования требуют именно решения задач частично-полного перебора. С появлением суперкомпьютеров требования к пропускной способности таких каналов существенно снижаются [2, 3]. РПВ, использующие скрытые каналы воздействия на объект, а также приема и передачи информации, уже появились. Совершенствование методов поиска уязвимостей программных систем, создающих предпосылки для проведения атак, основанных на вставке кода, привело к увеличению фактов обнаружения РПВ, использующих *уязвимости нулевого дня* (ZeroDayVulnerabilities). Совершенно очевидно, что в самое ближайшее время будут обнаружены РПВ, которые при функционировании для затруднения своего выявления и нейтрализации применяют СКТ, в частности, гибридные. В результате антивирусы, использующие традиционные реактивные методы защиты, окажутся не в состоянии справиться с новой угрозой.

Ситуация тяжелая, но не безнадежная. Надежду вселяет знание основных ошибок, которые были сделаны в недавнем прошлом и которых вполне можно избежать в будущем:

- Решение вопросов ИБ по остаточному принципу уже после создания новой системы или новой КТ. В результате в большинстве случаев все сводится к «латанию» все новых и новых «дыр», а не к кардинальному решению проблемы;
- Большинство существующих алгоритмов ЗИи протоколов защищенного информационного взаимодействия исходят из модели «черного ящика» (BlackBox) и именно в условиях действия такой модели они обеспечивают требуемый уровень ИБ. В действительности же действует либо модель серого ящика (GreyBox), когда возможны утечки по побочным каналам (SideChannels) и соответственно надо думать о временных, мощностных и др. атаках на реализацию (Timing, Cachetiming, Power, DifferentialPowerAttacks и др.), либо «белого ящика» (WhiteBox), когда компьютер, где программно реализованы методы защиты информации, полностью доступен

Иванов, М. А. Защищенные компьютерные технологии: миф или реальность? / М. А. Иванов. - Текст: непосредственный // REDS: Телекоммуникационные устройства и системы. - 2015. - Т. 5. - № 3. - С. 279-282. - ISSN 9999-9355.



Информационная безопасность (ИБ) давно стала самостоятельным направлением исследований и разработок. Однако, несмотря на это, проблем не становится меньше. Это объясняется появлением всё новых компьютерных технологий (КТ) (суперкомпьютерных, мобильных, радиочастотной идентификации (RFID) и пр.), которые не только создают новые проблемы ИБ, но и представляют, казалось бы, уже решенные вопросы совершенно в новом ракурсе. Главная причина трудоемкости решения задачи защиты информации (ЗИ) в современных условиях - всё большее отстранение пользователей от процессов управления и обработки информации и передача его ПО, обладающему некоторой свободой в своих действиях и поэтому очень часто работающему вовсе не так, как предполагает пользователь.

Под контролем

Лилия Варюхина

Никогда нельзя верить системе. Я же говорил, пока ты в системе, один щелчок пальцами — и тебя нет. И все эти спутники, сотовые, микрочипы, Интернет, глобальные сети, данпасты...

Мервин Болт

Сегодня из-за ускоренного развития технологий в нашей жизни стали возникать новые угрозы — такие, например, как киберпреступность, которая преследует нас из-за незащищенности информационного пространства. Мы не можем уберечь своих детей от просмотра сцен насилия, остановить эту пропаганду в Интернете. Мы не можем защитить себя и своих близких от похищения личных данных.

Наряду с этими угрозами российское правительство второй год подряд продолжает обсуждение создания электронных паспортов, которые должны заменить традиционные.

«Федеральная миграционная служба РФ планирует начать в 2015 году выдачу универсальных пластиковых карт, которые к 2017 году должны будут заменить традиционные паспорта. На официальном портале подготовки нормативных актов опубликован проект указа, согласно которому 1 января 2015 года электронная карта станет основным удостоверением личности в РФ. На карте будут содержаться персональные данные, как в графической, так и в электронной форме, а также биометрические данные. Предполагается, что пластиковая карта позволит владельцу совершать электронные услуги. В 2015 году ФМС рассчитывает выдать не менее 300 тысяч электронных удостоверений» (из сообщений СМИ)

Как известно, все электронные карты имеют чип и RFID-систему (радиочастотная идентификация). Способ автоматической идентификации объектов позволяет посредством радиосигналов считывать или записывать данные, хранящиеся в так называемых «транспондерах», или RFID-метках.

По дальности считывания RFID-системы можно подразделить на подсистемы:

– ближней идентификации (считывание производится на расстоянии до 20 см);

– идентификации средней дальности (от 20 см до 5 м);

– дальней идентификации (от 5 до 100 м).

С одной стороны – это прорыв в технологиях, который может решить многие проблемы, упростить нашу жизнь.

С другой стороны – это угроза частной жизни людей. Использование RFID-меток вызвало серьёзную полемику, критику и даже бойкотирование товаров.

Вот наиболее серьёзные проблемы, связанные с неприкосновенностью частной жизни:

Порой покупатель может даже не знать о наличии RFID-метки. Или не может её удалить.

Данные с метки могут быть считаны дистанционно без ведома владельца. Если помеченный предмет оплачивается кредитной картой, то возможно однозначно связать уникальный идентификатор метки с покупателем. Основное беспокойство вызывает то, что иногда RFID-метки остаются в рабочем состоянии даже после того, как товар куплен и вынесен из магазина, и поэтому могут быть использованы для слежки и других неблаговидных целей, не связанных с инвентаризационной функцией меток.

Считывание с небольших расстояний также может представлять опасность, если, например, считанная информация накапливается в базе данных, или грабитель использует карманный считыватель для оценки богатства проходящей мимо потенциальной жертвы. Серийные номера на RFID-метках могут вызвать дополнительную информацию даже после избавления от товара. Например, метки в перепроданных или подаренных вещах могут быть использованы для установления круга общения человека.

Данные с RFID-чипа в электронных документах и пластиковых картах можно мгновенно считывать простым сканером, лежащим в небольшой барсетке, проведя им возле кармана или сумки человека, носящего электронный документ. Вся информация о владельце тут же выводится на экране мини-ноутбука.

Более мощное (но вполне общедоступное) оборудование позволит считывать такие персональные данные с расстояния в сотни метров.

Хакер Крис Паджет придумал, как на расстоянии до девяти метров считывать и клонировать метки RFID-паспортов. Для этого ему понадобились RFID-ридер Symbol XR400 производства Motorola, антенна AN400 той же компании и ноутбук Dell 710m. Все оборудование Крис приобрел

Варюхина, Л. Под контролем / Лилия Варюхина. - Текст : непосредственный // Наша молодежь. - 2015. - № 2. - С. 30-32 : фот. - ISSN 2222-5382.

В статье рассмотрена проблема информационной безопасности. В Конституции РФ указано, что личная жизнь гражданина неприкосновенна. Универсальные электронные карты (электронные паспорта) лишают неприкосновенности личную жизнь гражданина РФ, следовательно, введение их является антиконституционным. Наряду с этим, универсальные электронные карты (электронные паспорта), по мнению автора, угрожают обороноспособности Российской Федерации, работе спецслужб и не только.

ТЕХНИЧЕСКОЕ ОБОЗРЕНИЕ

РАБОТА В ПАРЕ: КОМБИНИРОВАННЫЕ СЧИТЫВАТЕЛИ RFID + БИО

«Усиление» радиочастотной СКУД с помощью биометрического фактора идентификации позволяет повысить защищенность системы, а комбинированные устройства обеспечивают не только удобство использования, но и процесс миграции между технологиями.

Юрий Савостьянов, эксперт

Обычно заказчик предпочитает простые системы, которые надежны в работе, легко обслуживаются и относительно недорого стоят. В контексте контроля доступа к таким системам относятся СКУД, построенные на базе proximity-технологий, которые, к сожалению, имеют не очень хорошую защиту от копирования и подделки идентификаторов. Повысить степень защищенности особо важных сегментов системы доступа можно, добавив к RFID еще один фактор идентификации — например, биометрический. В качестве примера симбиоза технологий при ограничении доступа рассмотрим сочетание распознавания по бесконтактной карте и отпечатку пальца.

КАК РАБОТАЕТ РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ

Для ближней бесконтактной идентификации в СКУД используются две рабочих частоты: 125 кГц (НЧ) и 13,56 МГц (ВЧ), при этом низкочастотное оборудование является более дешевым. Пассивные RFID-карты, не имеющие встроенного источника питания, попадают в радиус действия считывателя, который постоянно излучает сигнал на соответствующей частоте и генерирует ответный сигнал с кодом, используя полученную от ридера энергию. Данная технология реализована в идентификаторах на базе встроенного миниатюрного чипа, в состав которого входит передатчик, приемник, процессор и антенна. В памяти процессора хранится уникальный идентификационный код карты, запрограммированный в заводских условиях.

ТЕХНОЛОГИИ СЧИТЫВАНИЯ ОТПЕЧАТКОВ

Что касается считывателей отпечатков пальцев, на рынке лидируют устройства, имеющие сенсоры трех типов — оптические, полупроводниковые емкостные и полупроводниковые термические. При этом самой распространенной является оптическая технология считывания. Это объясняется ее дешевизной и надежностью работы. К недостаткам оптических сенсоров можно отнести их малоэффективную защиту от муляжей. Емкостной метод также является весьма распространенным в биометрии, его существенный недостаток — подверженность сенсоров этого типа негативному влиянию электростатики. Термосканеры стабильно работают в широких температурных диапазонах, устойчивы к электростатическому

SMARTEC ST-FR030EMW

Уличный биометрический/EM-считыватель ST-FR030EMW работает под управлением ПО Timex, имеет интерфейсы RS-485, USB, Ethernet. Прочный герметичный корпус обеспечивает устройству надежную защиту от пыли и влаги, а встроенный обогреватель с термостатом позволяет эксплуатировать считыватель в уличных условиях при температуре от –40 до +50°С. Также устройство оснащено Wiegand-входом/выходом и входами для подключения кнопки выхода и датчика положения двери.

Савостьянов, Ю. Работа в паре: комбинированные считыватели RFID+БИО / Ю. Савостьянов. - Текст : непосредственный // Безопасность. Достоверность. Информация. - 2014. - № 5. - С. 56-58.

"Усиление" радиочастотной СКУД с помощью биометрического фактора идентификации позволяет повысить защищенность системы, а комбинированные устройства обеспечивают не только удобство использования, но и процесс миграции между технологиями.

108 СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ www.all-over-ip.ru

UHF vs. HF RFID:

новый взгляд на старую полемику

EXPERT OPINION

UHF-считыватели для СКУД значительно превосходят по дальности чтения Proximity и Smart-считыватели, позволяют одновременного считывать большое количество карт и отличаются невысокой стоимостью. Они являются оптимальным решением для идентификации легкового автотранспорта в режиме Hands Free; организации систем учета, поиска и инвентаризации с большой номенклатурой и необходимостью автоматизации. Однако бесплатного сыра не бывает – эксперты журнала всесторонне рассматривают особенности UHF-считывателей для СКУД и дают практические рекомендации по их эффективному применению

Алексей Коноплев
Руководитель направления СКУД компании "АРМО-Системы"

UHF-диапазон для RFID-считывателей в СКУД – случайный "гость" или закономерное явление?

Считыватели с УВЧ-диапазоном границы СКУД из логистики, где их применение серьезно упрощало работу с большими объемами товаров. В области контроля доступа эти технологии решают задачи дистанционной идентификации в радиусе около 10 м. Помимо этого, как и в логистике, важным для СКУД преимуществом УВЧ является возможность одновременного считывания большого количества карт. Интегрированная часть памяти чипов обеспечивает достаточно высокий уровень безопасности работы. Конечно, высокочастотные решения – не самые бюджетные, что обусловлено отсутствием аналогов по стоимости и диапазону считывания, а также спектру решаемых задач. Эти характеристики позволяют рассматривать их преимущественно в проектах СКУД как вполне закономерное явление.

Для решения каких задач в СКУД применение UHF-считывателей будет наиболее оптимальным?

На сегодня УВЧ-технологии в задачах СКУД чаще всего используются для дистанционного считывания при проезде автотранспорта, но скорее всего зоны применения будут расширяться благодаря поддержке идентификации Hands free, не требующей от пользователя выполнения дополнительных действий. Например, в системах контроля доступа УВЧ может задействоваться для отслеживания перемещения материальных ценностей. Помимо этого, были проекты реализации СКУД, где УВЧ-оборудование применялось для идентификации и учета рабочего времени на крупном добывающем предприятии без использования ограничивающих пропускную способность турникетов.

Каковы достоинства и недостатки UHF-технологии в сравнении с классическими технологиями идентификации людей Proximity (125 кГц) и Smart (13,56 МГц)?

Принципиальное отличие УВЧ – возможность идентификации в радиусе 10 м, что не могут обеспечить ни Proximity, ни Smart.

Применение УВЧ в СКУД дает ограничения из-за невысоких показателей безопасности, но варианты повышения защиты УВЧ-идентификации все же имеются.

Память УВЧ-чипа разделена на несколько банков – пользовательские и заводские. Пользователь имеет полные полномочия по считыванию и записи, поскольку УВЧ-технология создавалась для "открытой" идентификации. В заводской зоне программа производителя чипа может записывать уникальный для каждого чипа код. Уникальный код можно считать, но нельзя будет скопировать в другую область памяти, поскольку она не является перепрограммируемой. Таким образом, ориентируясь на уникальный номер чипа, можно построить систему, в том числе и контроля доступа, с достаточно высоким уровнем безопасности при дистанционной идентификации. Proximity-чипы защищены слабее, так как их уникальные номера легко копируются и дублируются.

Если говорить о стоимости, УВЧ-метки недорогие, не требуют обслуживания, но считыватели гораздо дороже, чем Proximity. Это связано с более сложной конструкцией антенны, а также с более "узкой" линейкой, позволяющей использовать эти считыватели в любые сторонние приложения. Если ограничиться функционалом, требуемым для СКУД, то стоимость УВЧ-считывателей может быть скорректирована в сторону уменьшения.

Идентификация автотранспорта – что бы вы выбрали: UHF-считыватели или 2,45 ГГЦ считыватели?

Выбор считывателя в первую очередь зависит от нужд проекта. Оборудование 2,45 ГГц обеспечивает большее расстояние срабатывания и большую вероятность считывания меток, что дает определенную гибкость в ходе реализации проектов при более высокой стоимости как меток, так и считывателей. Помимо этого, в процессе работы требуется замена элементов питания, а соответственно обслуживание: поскольку метка 2,45 ГГц активна, постоянное обращение к ней приводит к быстрому разряду батареи и возникает необходимость ее замены. 2,45 ГГц имеет диапазон считывания в несколько десятков метров, а также возможность перечтения пункта идентификации без снижения скорости. Подобные задачи решаем далеко не во всех проектах, поэтому более доступной технологией для автомобильной идентификации в назовем все-таки УВЧ.

Ваше мнение о перспективах использования UHF-считывателей и меток в СКУД

Перспективы применения УВЧ-оборудования в проектах СКУД связаны с выпуском комбинированных карт с разной дальностью считывания. Наряду с УВЧ-составляющей они будут иметь, например, компоненты MIFARE. Высокочастотная составляющая будет срабатывать в зонах удаленной идентификации, а в точках с повышенными требованиями к уровню защиты канала обмена данными между картой и считывателем информация будет считываться из сектора памяти MIFARE, в котором для этого применяется дополнительная защита с цифровыми ■

Мнение экспертов. UHF vs. HF RFID: новый взгляд на старую полемику / А. Коноплев, А. Бухаров, П. Иванченко [и др.]. - Текст : непосредственный // Системы безопасности. - 2014. - № 3 (117). - С. 108-117.

В статье эксперты журнала всесторонне рассматривают особенности UHF-считывателей для СКУД и дают практические рекомендации по их эффективному применению.

ТЕЛЕКОМ: УРАВНЕНИЕ ПЕРЕНОСА | Андрей Черкасенко и др.

RFID — умная технология

В статье рассматриваются перспективы развития и использования информационной технологии радиочастотной идентификации. Оцениваются возможности создания новой подотрасли телекоммуникационной отрасли и основные направления применения технологии для решения практических задач.

УДК 6.07.2.+338.47

Ключевые слова
Радиочастотная метка, идентификация, аутентификация, безопасность.

Авторы

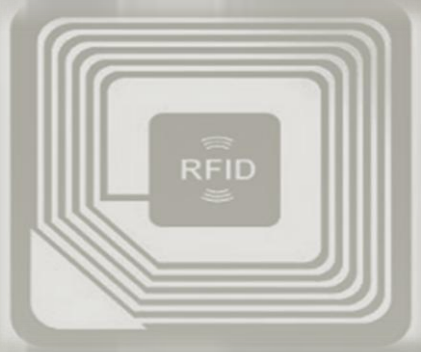
Черкасенко Андрей Иванович — генеральный директор группы компаний «Атомпромресурсы», доктор экономических наук.
Рудашевский Владимир Давыдович — заместитель председателя Комитета ТПП РФ по научно-техническим инновациям и высоким технологиям, доктор экономических наук, профессор.

Средства вычислительной техники и современные телекоммуникационные сети являются неотъемлемой частью нашей жизни и одним из главных факторов, влияющих на все сферы жизни и развития общества. Интенсивное внедрение информационных технологий привело к тому, что информационный ресурс стал сегодня таким же богатством, как производственный и людской потенциал. Поэтому во многом отличительной особенностью нашего времени с полной уверенностью следует считать формирующееся окружение человека, наполненное разного рода электронными помощниками, такими как банковские карты, мобильные телефоны, навигаторы, средства скрытого наблюдения и т.д. Их «умными помощниками» являются миниатюрные устройства (чипы). Они обеспечивают круглосуточный оперативный учет и контроль передвижения товаров, оплаты услуг, открытие/закрытие доступа к информации, что дает возможность практического применения в повседневной жизни чипа посредством технологии RFID (Radio Frequency Identification) — бесконтактные радиочастотные метки с модулем памяти.

Число устройств, подключенных к Глобальной сети, растет по экспоненте, и столь же стремительно возрастают ценность информационных технологий, самого Интернета и преимущества подключения к нему. Сначала тысячи больших и мини-компьютеров позволяли коллективно работать с коммерческой информацией. Их потеснили миллионы персональных компьютеров, за которыми последовали десятки миллионов мобильных телефонов и карманных компьютеров, планшетов, породивших еще более ценные сетевые услуги, такие как электронная почта, прямая телефонная связь, совместное использование файлов, B2B-коммерция и т.д. Сегодня совместный доступ к сервисам и приложениям — привычное дело. На очереди подключение миллиардов устройств, каждое из которых имеет собственный «цифровой код».

Во весь рост встает проблема идентификации и аутентификации хотя бы для того, чтобы предотвратить угрозы безопасности личности, компании и страны. Радиочастотная идентификация позволяет выделять объект наблюдения из общей массы и отличать его, а затем следить за его переме-

Черкасенко, А. И. RFID - умная технология / Андрей Черкасенко, Владимир Рудашевский. - Текст : непосредственный // Экономические стратегии. - 2013. - № 7. - С. 60-66 : 2 фот. - ISSN 1680-094X.



В статье рассматриваются перспективы развития и использования информационной технологии радиочастотной идентификации. Оцениваются возможности создания новой подотрасли телекоммуникационной отрасли и основные направления применения технологии для решения практических задач.

64 СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ www.all-over-ip.ru

КОЛОНКА РЕДАКТОРА

Безопасный город – больше чем домофон

В повседневной жизни для многих понятие "безопасный город" в контексте СКУД сводится к домофону на подъезде. Однако такая трактовка – сильное упрощение вопроса. Думаю, более правильно рассматривать "безопасный город" как защищенность всех объектов городской инфраструктуры, и в первую очередь объектов повышенной важности, от четкой работы которых зависят жизнь, здоровье и благополучие сразу многих людей.

Можно также вспомнить, что в качестве наследия прошлых лет нам достались масса промышленных предприятий, расположенных в черте города и являющихся потенциальной мишенью для терроризма. Многие из этих предприятий работают с опасными материалами и веществами или используют производственные процессы, нарушение которых может привести к неблагоприятным последствиям для жителей и города в целом (а иногда даже для большого региона). Пока еще не все такие производства выведены за городскую черту, обеспечить их защиту – первоочередная задача, и СКУД в этом вопросе играет не последнюю роль.

При контроле и управлении доступом довольно часто возникает необходимость решения специфических задач, для которых не подходят стандартные решения и оборудование.

Одной из таких задач является доступ в режиме Hands-Free, или "свободные руки". В больницах, на складах и в логистических центрах, кассовых залах и на других объектах порой нет возможности достать карту – например, вы врач и везете больного в реанимацию или вы инкассатор и несете мешки с деньгами. В данном случае процесс идентификации должен осуществляться без лишних манипуляций с картой (не надо доставать ее и куда-то прикладывать). Обычно для решения таких задач используются либо наиболее мощные модели считывателей 125 кГц (Proximity) и 13,56 МГц (Smart), либо маломощные транспортные RFID-считыватели 2,45 ГГц, либо считыватели частотного диапазона UHF. С данным оборудованием можно ознакомиться в техническом обозрении на стр. 74.

В следующих номерах журнала мы продолжим тему специализированного оборудования СКУД.

Алексей Гинце
Редактор раздела "Системы контроля и управления доступом"

RFID, SaaS, Mobile, биометрия: новейшие технологии

Эксперты компаний HID Global, "Компания Семь печатей", "Релвест" и "Смарт Секьюрити" представляют свой нетривиальный взгляд на развитие современных технологий в области систем контроля и управления доступом

EXPERT OPINION

1. Почему большую часть рынка RFID-считывателей продолжает занимать Proximity-технология, несмотря на все свои недостатки?
2. SaaS (Software as a Service) на российском рынке СКУД – реальное завтра или туманное когда-нибудь?
3. Биометрия так и останется нишевым продуктом или сможет в обозримой перспективе потеснить RFID-технологии в СКУД?
4. Функционал современных СКУД избыточен или недостаточен для отечественного потребителя?
5. Современные мобильные технологии и СКУД – где возможны "точки соприкосновения"?

Аркадий Гамбург
Генеральный директор
ООО "Компания Семь печатей"

Почему доминирует Proximity?
А собственно, какие недостатки у Proximity-технологий? По сравнению с реально работающими технологиями я вижу только недостаточно хорошее шифрование, которое позволяет либо считать код, либо клонировать карту. Но взламывать систему таким образом слишком дорого, и на подавляющем большинстве объектов злоумышленникам дешевле подкупить охрану или перелезть через забор.

SaaS – завтра или когда-нибудь?
Мое мнение, что облачные решения для систем безопасности – это примерно то же самое, что хранение секретных планов нашего Генерального штаба на сервере ЦРУ.

Биометрия – нишевой продукт?
Как только какой-нибудь способ идентификации даст такую же надежность и быстродействие, как RFID, он сразу же не точно полезет – заменит его. Так же, как когда-то RFID сменил Touch. Я думаю, что это время уже близко.

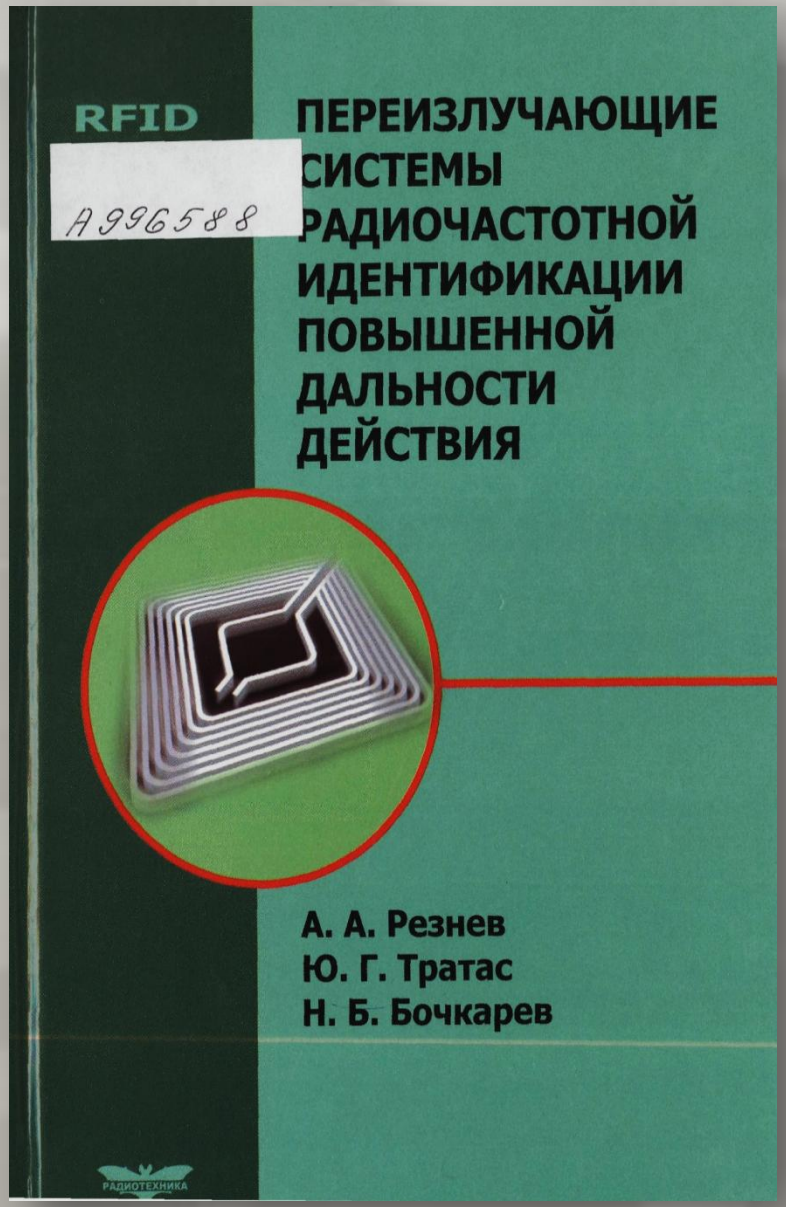
Функционал СКУД: избыточен или недостаточен?
Этот вопрос – как уравнение с двумя неизвестными: чтобы его решить, надо знать, о каком потреблении идет речь. Для каких-то мелких объектов достаточно даже автономной системы с функциональностью турникета: пускать – не пускать. А для ряда крупных заказчиков недостаточно возможностей самой интеллектуальной СКУД: им необходимы адаптация под свои задачи, которая зачастую выливается в создание целой системы интеграции с инженерными, производственными, информационными структурами предприятия.

СКУД Mobile
Термин "точки соприкосновения" (см. вопрос 5) напоминает хорошо знакомое старшему поколению "мирное сосуществование". Правильнее, наверное, говорить об использовании в СКУД современных, в том числе и мобильных, технологий. Не просто ради крутости системы, а для решения конкретных задач. Например, было бы очень удобна идентификация пользователей СКУД по NFC, прежде всего для самих пользователей, которые скорее забудут дома карточку, чем мобильник. Для администраторов СКУД большой радостью стало бы оповещение о сбоях в системе посредством того же сотового телефона. Начальники бы с огромным удовольствием отслеживали на iPad в Куршевеле опоздания и прогулы подчиненных. Для серьезных заказчиков можно было бы внедрять в систему мобильный Интернет. Например, для создания единой СКУД с удаленными филиалами. Хотя, почему "было бы", это уже есть. ■

февраль – март 2013 www.securitech.ru

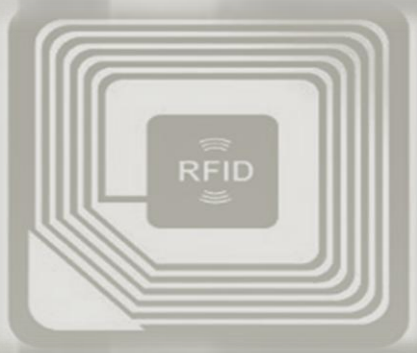
Гамбург А. RFID, SaaS, Mobile, биометрия: новейшие технологии / А. Гамбург, А. Катренко, С. Гордеев. - Текст : непосредственный // Системы безопасности. - 2013. - № 1 (109). - С. 64-69.

В статье эксперты представляют свой нетривиальный взгляд на развитие современных технологий в области систем контроля и управления доступом.



A996588

Резнев, А. А. Переизлучающие системы радиочастотной идентификации повышенной дальности действия / А. А. Резнев, Ю. Г. Тратас, Н. Б. Бочкарев. - Москва : Радиотехника, 2013. - 175, [1] с. : ил., табл., фото. цв. - ISBN 978-5-88070-360-9. - Текст : непосредственный.



В книге рассмотрены особенности распространения радиосигналов в системах на дальних трассах. Проанализированы варианты систем, осуществляющие обнаружение меток.

Книга может быть полезна специалистам, занимающимся созданием новых систем радиочастотной идентификации, а также студентам аспирантам, проявляющим интерес к системам RFID.

УДК 004.71

В.А. Михеев, А.В. Уткин, Д.А. Виноградов

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В RFID-СИСТЕМАХ ВЫСОКОГО УРОВНЯ СЛОЖНОСТИ, ПОСТРОЕННЫХ НА ПРИНЦИПАХ EPCGLOBAL

Целью данной работы является исследование путей повышения информационной защищенности систем радиочастотной идентификации различного уровня сложности. Для достижения этой цели в работе решены следующие задачи: проведен анализ основных преимуществ, а так же ограничений в части защиты информации систем радиочастотной идентификации перед системами оптического кодирования при их использовании по одному и тому же назначению; исследованы существующие методы защиты информации в RFID-системах, основные угрозы несанкционированного вмешательства в эти системы и способы повышения их устойчивости.

Показано, что технология радиочастотной идентификации при правильном проектировании RFID-систем позволяет обеспечить заданный уровень их информационной защищенности.

Радиочастотная идентификация; радиочастотная система; система защиты информации.

V.A. Mikheev, A.V. Utkin, D.A. Vinogradov

ANALYZING THE PROBLEMS OF THE INFORMATION SECURITY IN RFID SYSTEMS HIGH LEVEL OF COMPLEXITY BASED ON THE PRINCIPLES EPCGLOBAL

The article describes the research of security in different levels of complexity radio frequency identification systems. To achieve the goal were solved following tasks: analysis of the main advantages and also limits of using radio frequency technology relative to technology optical encoding; research of existing methods of the security RFID systems, main threat to the security and methods of improving reliability the RFID systems, also presents analysis of security risks.

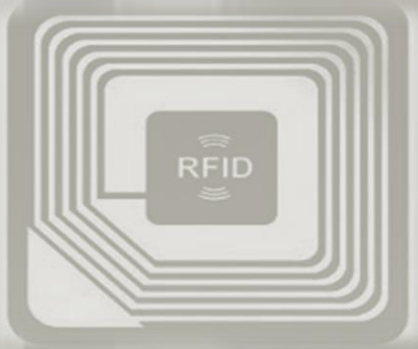
Shown that though imperfection of the RFID system security, radio frequency identification is safe and convenient tool high-technology of business process automation, in case correct designing the RFID system. In future it let to achieve high level of efficiency into a different ranges of application.

Radio frequency identification; radio frequency system; protection system of the information.

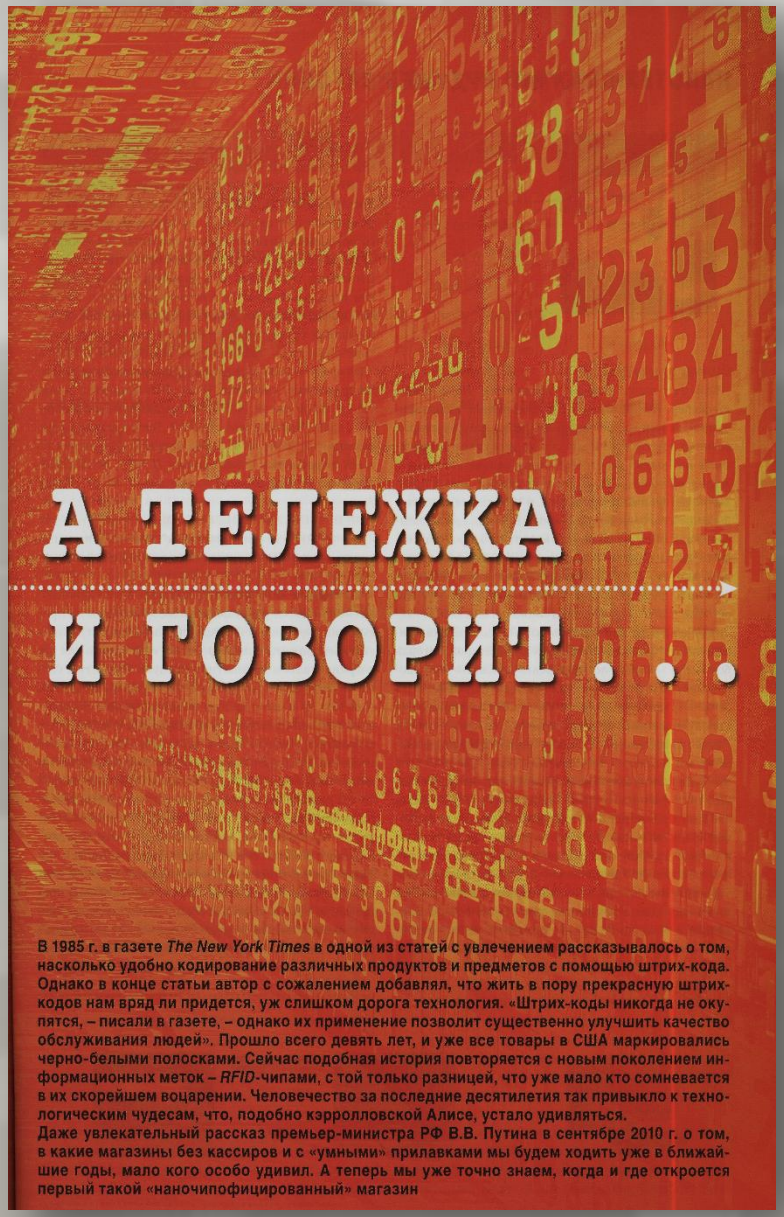
Радиочастотная идентификация (RFID) – технология автоматической идентификации объектов с помощью радиоволн. Современные радиочастотные системы не требуют от пользователей дополнительных навыков и специальных технических знаний, что делает процесс работы с ними интуитивно понятным и высоко автоматизированным. Это и определяет широту внедрения RFID-систем в различных предметных областях. В некоторых из них, например, в системах контроля доступа и борьбы с контрафактом, технология RFID уже является безусловным лидером.

Функционально, с точки зрения особенностей информационного взаимодействия, обычная RFID-система представляет собой двухзвенную замкнутую систему с жесткой обратной связью. Первым звеном системы выступает RFID-считыватель информации в виде условно стационарного программно-аппаратного комплекса, вторым – радиочастотная метка в виде мобильного (технологически неразрывно связанного с объектом идентификации) носителя определенной информации. Пассивная (не требующая внутреннего элемента питания) радиочастотная метка состоит из интегральной микросхемы, которая хранит в памяти нео-

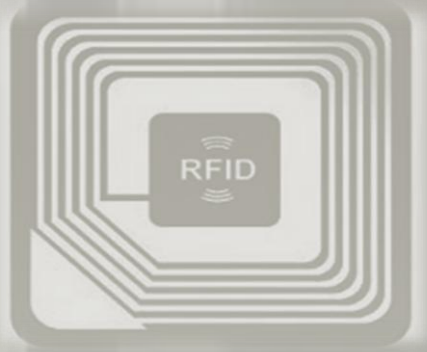
Михеев, В. А. Проблемы защиты информации в RFID-системах высокого уровня сложности, построенных на принципах EPCglobal / В. А. Михеев, А. В. Уткин, Д. А. Виноградов. - Текст : непосредственный // Известия Южного федерального университета. Технические науки. - 2012. - № 12 (137). - С. 34-39. - Библиогр.: с. 39 (5 назв.). - ISSN 1999-9429.



Целью данной работы является исследование путей повышения информационной защищенности систем радиочастотной идентификации различного уровня сложности. Показано, что технология радиочастотной идентификации при правильном проектировании RFID-систем позволяет обеспечить заданный уровень их информационной защищенности.



А тележка и говорит... / составитель В. Чумаков. - Текст : непосредственный // В мире науки. - 2011. - N 9. - С. 60-69 : 4 схемы, 6 диагр., 4 ил., 1 табл. - ISSN 0208-0621.



В статье утверждается, что RFID-технологии завоюют мир, и тогда человечество вступит в новую эпоху - эру моментальной идентификации.

УДК 621.382.26

И. Ю. Жуков, д-р техн. наук, доц.,
первый зам. директора — генеральный конструктор,
ОАО "Всероссийский научно-исследовательский
институт автоматизации управления
в непромышленной сфере им. В. В. Соломатина",
Д. М. Михайлов, аспирант, ассистент,
e-mail: mdmitry@bk.ru,
А. В. Стариковский, аспирант, ассистент,
Национальный исследовательский
ядерный университет "МИФИ"

Усовершенствованный протокол аутентификации бюджетных RFID-меток

Рассматривается усовершенствованный протокол аутентификации RFID-меток (Radio Frequency Identification), в которых отсутствуют ресурсы, необходимые для мощных криптографических преобразований. Подобные метки являются удобным и очень дешевым средством мониторинга, и поэтому получили повсеместное применение. В связи с этим их удобно называть бюджетными RFID-метками. Они используются в логистике при транспортировке грузов, в магазинах для защиты товаров от кражи и т. д. Универсальное применение RFID-меток привлекает внимание злоумышленников в целях промышленного шпионажа, вторжения в частную жизнь, хищения собственности пользователей, что создает новые угрозы безопасности и конфиденциальности информации.

В целях обеспечения безопасности использования подобных RFID-систем приводится базовое описание RFID-модели и предлагается решение на основе алгоритма RSA для обеспечения защищенного процесса аутентификации при обмене информацией между RF-сканером и метками.

Ключевые слова: *протокол аутентификации, RFID-метки, криптография, безопасность, защита данных*

1. Проблема аутентификации RFID-меток

Современный мир товарооборота невозможно представить без применения RFID-технологий. Дешевые, так называемые "бюджетные", радиочастотные метки с низкими функциональными возможностями оказались очень удобным механизмом логистики и мониторинга и поэтому получили необыкновенно широкое распространение. Универсальное применение RFID-меток привлекает внимание злоумышленников в целях промышленного шпионажа, вторжения в частную жизнь, хищения собственности пользователей, что создает новые угрозы безопасности и конфиденциальности информации.

Первые упоминания о необходимости обеспечения безопасности в RFID-системах встречаются в работе [1]. Авторы разработали новые облегченные криптографические протоколы для бюджетных RFID-меток. Они создали механизм защиты от угрозы клонирования меток [1], благодаря которой злоумышленник может подменять товар в магазине меткой-клоном. При этом RFID-система, установленная в магазине, будет считать, что товар по-прежнему находится на полке.

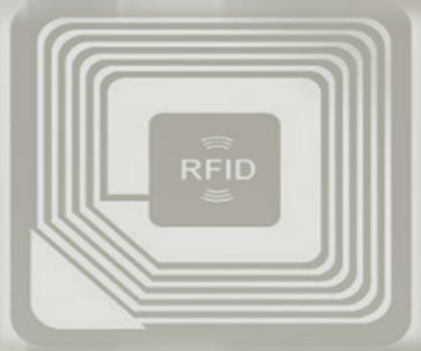
Авторы работы [2] использовали в смарт-картах и сетевых датчиках облегченные криптосистемы с открытым ключом, получившие название NTRU. В то же время, авторы работы [3] предложили использовать электронную цифровую подпись. Несмотря на то, что оба эти варианта по сравнению с ранее известными криптосистемами ведут к очень эффективным механизмам на основе открытых ключей и цифровых подписей, они все равно требуют гораздо больший объем для ресурсов, чем он доступен на бюджетных RFID-метках.

Различные схемы контроля доступа к RFID-меткам предлагают авторы работы [4]. Метка может находиться в одном из двух режимов. В закрытом режиме метка отвечает лишь на запросы, имеющие определенный мета-идентификатор. В открытом режиме она может выполнять операции, связанные с безопасностью и настройками. Цель этой схемы гарантировать, что метка переходит в открытый режим, только если получает соответствующую команду от сопряженного RF-сканера. Отсюда можно сделать вывод, что предложенные протоколы [4] подходят по большей части для аутентификации RF-сканера. К тому же они используют стандартные криптографические хэш-функции и требуют установки генератора псевдослучайных чисел на метки, что также недостижимо в связи с ограничениями ресурсов бюджетных RFID-меток.

2. Условия и ограничения применения бюджетных RFID-меток

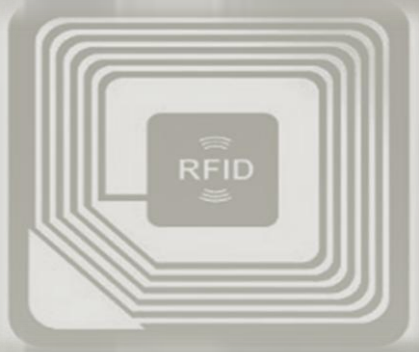
В магазине RF-сканер периодически опрашивает метки, прикрепленные к товарам, тем самым осуществляя их идентификацию. В подобной системе необходимо обеспечить защиту от кражи то-

Жуков, И. Ю. Усовершенствованный протокол аутентификации бюджетных RFID-меток / И. Ю. Жуков, Д. М. Михайлов, А. В. Стариковский. - Текст : непосредственный // Информационные технологии. - 2011. - N 7. - С. 49-51. - Библиогр.: с. 51 (6 назв.). - ISSN 1684-6400.



В статье рассматривается усовершенствованный протокол аутентификации RFID-меток, в которых отсутствуют ресурсы, необходимые для мощных криптографических преобразований.

Олбрехт, К. Радиометка - это вы / Катрин Олбрехт ; перевод И. Е. Сацевич. - Текст : непосредственный // В мире науки. - 2008. - N 12. - С. 44-49 : 3 схемы, 2 рис. - ISSN 0208-0621.

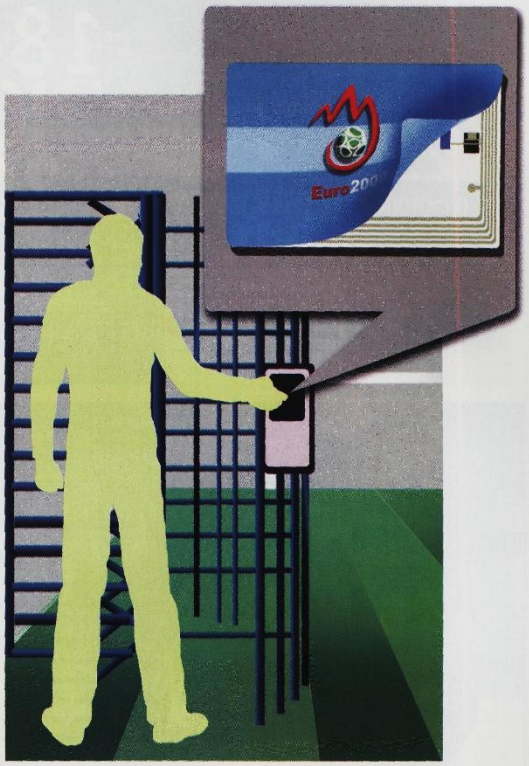


Миниатюрные радиочастотные идентификационные метки, давно используемые для отслеживания движения поставок и запасов, в последнее время стали все шире применяться для маркировки потребительских товаров, что представляет угрозу для тех, кто "носит" их, часто не подозревая об этом.

RFID-метки

РАДИОИДЕНТИФИКАЦИОННЫЕ МЕТКИ

АЛЕКСАНДР БАУЛИН

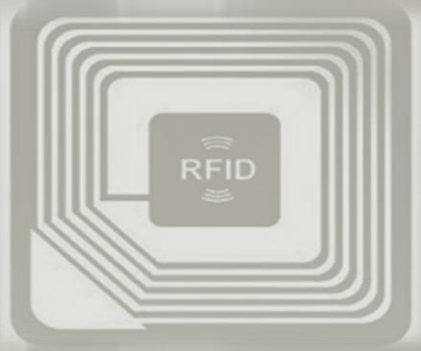


На продвинутых в техническом отношении футбольных матчах используются радиоидентификационные метки — RFID. Они вклеиваются в билет, который его владелец просто прикладывает к считывающему блоку, — и контролер не нужен. В отличие от подделки обычных билетов и даже билетов со штрихкодом, для имитации RFID-билета недостаточно его скопировать, надо еще воспроизвести информацию с вклеенной микросхемы. К тому же теоретически владелец такого билета может во время перерыва выйти со стадиона («контроль» то отрывать не приходится) — система отметит данный факт на микросхеме, а потом позволит вернуться. А вот передавать билет тем, кто не попал, оставаясь при этом на стадионе, бесполезно — RFID-метка помнит, что она уже «зашла», и откажет в доступе зайцу.

Создать столь миниатюрные RFID-метки, чтобы их не было заметно на билете, удалось, отказавшись от встроенных источников питания. Когда болельщик проходит через ворота, то прикладывает билет к блоку, излучающему радиоволну. Ее улавливает антенна RFID-метки, которая, чтобы быть длиннее, скручена спиралью по всей площади билета. «Пойманное» электромагнитное поле порождает электрический ток. Его хватает, чтобы считать информацию с микросхемы, изменить ее (если требуется) и послать ответный сигнал антенне. (За умение ответить на принятый сигнал RFID-метку называют транспондером.) Вышеупомянутый блок способен не только излучать радиоволны, но и принимать ответный сигнал. Расшифровав информацию с метки, он решает, подать ли команду на открывание.

Для тех, кто не ходит на футбол, отметим, что RFID-метки используются в складской деятельности, а лучше всего они знакомы тем, кто пользуется московским метро. На его картах нет магнитной полосы, подсчет поездок ведется микросхемой RFID, скрытой в билете, а турникеты служат передающей и получающей антенной.

Баулин, А. RFID-метки / А. Баулин. - Текст : непосредственный // Мир ПК. - 2008. - N 6. - С. 123. - ISSN 0235-3520.



Статья представляет собой короткий рассказ о технологии RFID.

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.

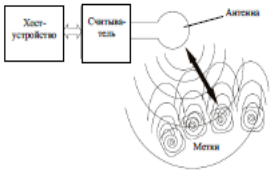
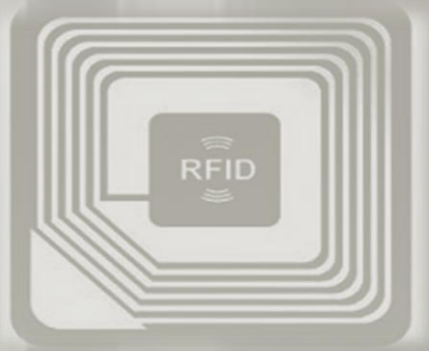


Рис. 1. Система RFID

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].

Матюш, М. В. Радиочастотная идентификация и ее применение / М. В. Матюш. - Текст : непосредственный // Вестник Полоцкого государственного университета. Серия С, Фундаментальные науки. - 2007. - N 9. - С. 115-122 : 6 рис. - Библиогр.: с. 122 (9 назв.).



В статье исследуется основная задача системы радиочастотной идентификации - хранение информации об объекте в виде идентификационного кода с возможностью его удобного считывания. Приводится анализ основных ограничений и настоящего уровня разработок аппаратуры RFID выявил большое число направлений будущих работ и исследований.

Торрес, Н. Л. Очипованные : следить за всеми и всегда? / Н. Л. Торрес. - Текст : непосредственный // Карьера. - 2006. - N 9. - С. 100.

FORWARD

ОЧИПОВАННЫЕ

СЛЕДИТЬ ЗА ВСЕМИ И ВСЕГДА?

МНОГООБРАЗИЕ средств обеспечения безопасности пополнилось новинкой. Речь идет о чипах радиочастотной идентификации – RFID. Они используются для решения множества задач – от контроля над прохождением почтовых отправлений до обнаружения потерявшихся домашних любимцев. И вот одна фирма в Огайо применила эту технологию к своим сотрудникам.

CityWatcher.com из Цинциннати работает в сфере безопасности, предлагая своим клиентам услуги видеонаблюдения. Разумеется, ее сотрудникам приходится иметь дело со строго конфиденциальной и важной информацией, а это значит, считает основатель фирмы 34-летний Шон Даркс, что и в самой фирме необходимо тщательно и скрупулезно контролировать доступ в тот или иной сектор. Потому-то Шон Даркс вшил себе и еще двум своим коллегам крохотные RFID-чипы, а еще два сотрудника CityWatcher.com предпочли носить чип на брелке с ключами. «Мы искали нестандартный ход, – рассказывает Даркс. – Что-то необычное и в то же время простое».

Очиповывание сотрудников – дело неоднозначное. Противники RFID считают, что чипы нарушают право человека на неприкосновенность частной жизни и его гражданскую свободу. «Работодатель должен спросить себя, чего именно он хочет добиться, используя технологию RFID, и подходит ли она для этого, – рекомендует Мартин Абрамс, исполнительный директор Center for Information Policy Leadership в юридической фирме Hunton&Williams из Вашингтона (федеральный округ Колумбия). – Например, RFID-чип нужен в качестве пропуска. Тогда встает вопрос: а почему, собственно, надо вшивать его именно в тело человека? Может быть, вполне достаточно, чтобы RFID находился, скажем, в бейджике?»

На это возражают, что со вшитым чипом спокойней – его нельзя украсть или потерять, что вполне может случиться с ключом. «Я бы согласился с теми HR-сотрудниками и специалистами по трудовым отношениям, которые считают, что пройдет немало времени, прежде чем все спорные моменты, связанные с RFID, будут урегулированы, – говорит Рэй О'Хара, старший вице-президент консалтинговой фирмы Vabe International Inc. из Оуктона (Вирджиния), занимающейся вопросами безопасности. – Полагаю, что придется немало потрудиться, прежде чем вшивание RFID-чипов в тела сотрудников станет широко применяемой практикой».

Отвечая на вопрос о том, в каком возрасте уже слишком поздно начинать собственный бизнес, **60%** американцев отвечают: «Никогда».

– НИКОЛЬ Л. ТОРРЕС. – ENTREPRENEUR

КОЛЕСА

ПИКАПЧИКИ

МАЛЕНЬКИЕ МАШИНКИ — НЕМАЛЕНЬКАЯ ПОМОЩЬ

БОЛЬШИНСТВО моделей пикапов вполне справится с задачей, если по делам вашей фирмы нужно перевезти небольшой груз или немного поработать тягачом. Длина кузова в среднем составляет около 180 см, вместимость – три–шесть человек. Плюс сравнительная дешевизна – от $20 тыс., и к тому же они значительно экономичнее своих более габаритных собратьев. Представляем три наиболее популярные модели небольших пикапов – Dodge Dakota, Ford Ranger и Toyota Tacoma. Грубоватая Dakota стоит $19 585. В своем классе это единственная модель с двигателем V-8 в качестве опции. Двери сделаны так, что садиться в машину и выходить из нее удобнее. В стандартной комплектации двигатель V-6, коробка передач 6-ступенчатая, ручная. Безопасность движения обеспечивают ABS, рулевая стойка особой конструкции, защита для коленей и боковые подушки безопасности. Грузоподъемность – около 900 кг.

Ranger от компании Ford продается уже без малого два десятка лет. Модель этого года в базовой комплектации стоит $15 085. В кабине стандартной модели – спальное место длиной 180 см, а в модели Styleside – 210 см. Силовой блок в базовой модели состоит из двигателя I-4 объемом 2,3 л и мощностью 143 л.с., а также ручной 5-ступенчатой трансмиссии. В варианте удлиненной кабины есть небольшие задние сиденья, сидящим на которых непросто пристроить свои колени. Грузоподъемность – примерно 630 кг.

Tacoma от Toyota – для тех, кому важна прежде всего цена. Tacoma стоит от $13 980. Двигатель 4-цилиндровый объемом 2,7 л и мощностью в 159 л.с. Если вам приходится часто ездить по бездорожью, пригодится усиленная подвеска (опция). ABS входит в стандартную комплектацию, а вот система электронного контроля стабильности – еще одна неплохая опция. Посадочных мест – три. Более дорогая 4-дверная модель – лучшая по итогам крэш-тестов National Highway Traffic Safety Administration. Toyota предлагает для Tacoma немало практичных аксессуаров, например, все, что необходимо для крепежа груза. Грузоподъемность – около 700 кг.

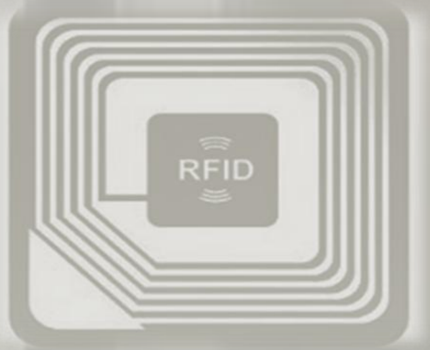
Есть и другие компактные пикапы: Mazda B-серии – сестренка Ranger от Ford; Colorado от Chevrolet и GMC Canyon.

DODGE DAKOTA

FORD RANGER

TOYOTA TACOMA

– ДЖИЛЛ АМАДИО. – ENTREPRENEUR



Некоторые американские работодатели дошли до того, что едва не клеймят своих сотрудников. Для чего им это нужно и как относиться к подобному?

За представленными на выставке изданиями приглашаем в Зональную научную библиотеку имени В. А. Артисевич СГУ (ул. Университетская, 42)

Отраслевой учебный отдел естественных наук,
виртуальная выставка, 2022