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 неко-

торую информацию об объекте идентификации, и антенны, посредством которой микросхема получает питание, принимает и передает электромагнитный сигнал считывателю.

В настоящее время область применения информационных систем на основе технологии RFID весьма широка, особенно в сфере автоматизации бизнес-процессов, где происходит процесс последовательного замещения технологии штрихового кодирования. Это связано с тем, что RFID-системы имеют значительно больше уже зарекомендовавших себя преимуществ по сравнению с традиционными системами штрихового кодирования. Среди основных преимуществ технологии радиочастотной идентификации можно выделить следующие:

- возможность дистанционного считывания информации с радиочастотных меток (допустимое расстояние от считывателя до радиочастотной метки зависит от применяемого частотного диапазона и может достигать десятков метров);
- возможность считывания радиочастотных меток, находящихся внутри радиопрозрачной упаковки, что позволяет быстро определять содержимое упаковочных единиц (коробок, ящиков и т.д.) без их вскрытия;
- возможность быстрого считывания информации с большого количества радиочастотных меток, что позволяет быстро определять содержимое упаковочных единиц даже в случае, когда внутри упаковки находится большое количество маркированных изделий, причем эти изделия могут быть как одинаковыми, так и разными;
- отсутствие жестких требований по точности позиционирования относительно считывателя и по пространственной ориентации радиочастотных меток, что упрощает автоматизацию процесса считывания (антенны считывателя, при необходимости, могут быть расположены в воротах, дверных проемах, в специальных порталах или в портативных RFID-считывателях);
- возможность дистанционной записи и перезаписи информации в радиочастотных метках;
- возможность использования радиочастотных меток не только для автоматизированного учета маркированных изделий, но и для обнаружения их несанкционированного перемещения, в частности хищения;
- возможность маркировки не только номенклатуры продукта, но и присвоения уникального номера каждой единице продукта с хранением информации о технологическом процессе производства и транспортировки [1].

Радиочастотные метки по своей конструкции укладываются в общую схему построения универсальных вычислительных устройств, отличаясь бесконтактными интерфейсами взаимодействия с окружающими их элементами и внешней средой. Это способствует постоянному расширению области применения RFID-систем и появлению новых взглядов на развитие и способы использования информационно-телекоммуникационных систем.

Наряду с отмеченными преимуществами, современные системы радиочастотной идентификации различного уровня сложности имеют и некоторые ограничения.

RFID-системы включают в себя достаточно широкий спектр беспроводных устройств различной функциональности, мощности и сложности, что позволяет их отнести к классу сложных систем автоматизации с предъявлением соответствующих требований по обеспечению защиты от несанкционированного доступа к информации. Защита данных и сохранение информации, циркулирующей в радиочастотной системе, является вопросом, который приобретает жизненно важное значение для деловой практики и востребованности технологии.

По мере развития и распространения бесконтактных информационно-телекоммуникационных систем идет масштабное нарастание угроз информационной безопасности, проникающих во все более глубокие уровни обработки данных, поэтому при моделировании и разработке радиочастотных систем особое внимание следует уделять вопросам защищённости информационной среды и разработке системы защиты информации.

Обязательным элементом разработки RFID-систем становится анализ потенциальных угроз и обеспечение защиты информации на физическом уровне обработки данных, защита элементов RFID-систем от фальсификации, подделки и несанкционированных действий, а также обеспечение информационной безопасности и разгрузки логического (информационного) уровня обработки от экспоненциально нарастающего числа транзакций и большого потока информации, ожидаемого и идущего с физического уровня обработки данных, по мере развития и распространения бесконтактных информационно-телекоммуникационных систем [1].

В рамках проблемы защиты информации в RFID-системах решаются следующие задачи: обеспечение конфиденциальности и аутентификации.

Системы радиочастотной идентификации, построенные на базе технологии EPCglobal, подвержены атакам, связанным с перехватом электромагнитных излучений между считывателем и меткой, а так же с доступом к информации, содержащейся на радиочастотной метке, или её компрометацией. Основная угроза может исходить от нарушителя, оснащенного высокотехнологичными радиочастотными средствами и стандартным лабораторным контрольно-измерительным оборудованием, с помощью которого происходит «прослушивание» авторизованной операции связи между считывателем и радиочастотной меткой. При помощи подобного оборудования возможна организация DoS-атак (атак, вызывающих отказ в обслуживании) на инфраструктуру радиочастотной системы путем наполнения диапазона 860–930 МГц, используемого для радиочастотных меток стандарта EPC Gen2, шумовыми помехами или использованием большого количества фиктивных радиочастотных меток. Подобная атака может привести как к временной потере работоспособности системы из-за технологических ограничений, связанных с невозможностью опроса единовременно большого количества радиочастотных меток, так и к продолжительному отказу в обслуживании, исходящему от RFID-считывателей [4].

Вторая группа возможных атак связана с отсутствием «невзламываемой» защиты информации, записанной на радиочастотную метку. Существующий уровень обеспечения безопасности, реализованный в протоколе EPC Gen2, позволяет разработчикам RFID-систем ограничить доступ к функциональным командам радиочастотной метки, с помощью которых радиочастотная метка может быть полностью деактивирована или её EPC номер (уникальный идентификатор объекта идентификации) может быть скрыт, путем защиты их 32-разрядными паролями, которые могут выступать как базовый уровень защиты радиочастотных меток. К сожалению, подобный метод защиты информации имеет ряд уязвимостей:

1. При работе с радиочастотной меткой пароль передается в отрытом виде и может быть получен путем прослушивания канала связи.
2. Используя атаки, основанные на анализе мощности излучения, возможно выявление пароля, так как метка в процессе аутентификации использует разный уровень мощности сигнала, зависящий от того, насколько каждый следующий предоставляемый бит соответствует значению действующего пароля. Для подбора ключа можно использовать направленную антенну и цифровой осциллограф. При посылке чипу неверного бита ключа шифра, используя 8- и 32-битное шифрование данных, энергопотребление интегральной микросхемы возрастает и радиочастотная метка излучает мень-

ше энергии, в отличие от случая, когда бит ключа оказывается верным, что может быть легко зафиксировано. Используя данный метод, возможен взлом достаточно длинных ключей за фиксированное время, что невозможно при использовании методов подбора пароля.

Таким образом, злоумышленник может получить конфиденциальную информацию об объекте идентификации путем физической атаки, изменить данные, сформировать нужное количество копий или деактивировать радиочастотные метки. При получении злоумышленником доступа к изменению информации, содержащейся на радиочастотной метке, не исключена запись вредоносных данных, при помощи которых возможно осуществление таких атак, как SQL-инъекция или переполнение буфера, успешная реализация которых может привести к нарушениям в работе и предоставлению доступа к RFID-системе третьим лицам [3–5].

Следовательно, большинство угроз может быть реализовано при воздействии на радиоканал с целью манипуляции с данными, передаваемыми по этому каналу, что приведет к нарушению работоспособности системы, в т.ч. к нарушению связи между считывателем и радиочастотными метками, блокированию информации.

С этими угрозами можно бороться, используя криптографические протоколы обмена информацией, построенные на асимметричных алгоритмах с открытым ключом, и шифрование хранимых данных. Однако, наделение радиочастотных меток подобными функциями требует дополнительных вычислительных ресурсов и расширенной энергонезависимой памяти, что ведет к усложнению и, как следствие, повышению стоимости меток. В случае с пассивными метками, к которым относятся радиочастотные метки технологии EPCglobal, может возникнуть ситуация, когда необходимой энергии, получаемой антенной радиочастотной метки от считывателя, не хватит для выполнения подобных операций и потребуется разработка особых рекомендаций для обеспечения высокой надежности и работоспособности радиочастотной системы. Данные ограничения пассивных меток могут стать серьезным препятствием для использования и внедрения RFID-систем.

Таким образом, уровень защиты информации, реализованный в стандартах EPC Gen2, не является достаточным для удовлетворения современных требований к защите данных, и предоставляет возможности для осуществления угроз, описанных выше. В связи с этим разработчики систем, для снижения рисков несанкционированного доступа к данным, вынуждены руководствоваться рекомендациями по усилению защиты информации радиочастотной системы в целом. Рекомендуем следующие способы повышения устойчивости RFID-систем к перечисленным выше угрозам:

1. Минимизация конфиденциальных данных на метке. Данный способ основывается на переносе данных из памяти радиочастотной метки в надежное хранилище данных информационно-управляющей системы организации и использовании уникального идентификатора или EPC-номера метки в качестве ключа доступа к этим данным. К сожалению, этот подход не исключает возможности получения злоумышленником ценной информации и от одного идентификатора. Например, зная структуру EPC можно выявить минимальную информацию об объекте идентификации.
2. Парольная защита радиочастотных меток. Современные радиочастотные метки уже располагают достаточными техническими ресурсами для верификации с помощью пароля, который уже стал неотъемлемой частью комплекса решений для защиты данных. Радиочастотная метка не позволит выполнить защищенные паролем команды на чтение, запись, деактивацию или на доступ к защищенному участку памяти, если они не сопровождаются правильным паролем. В то время как в традиционных информационных системах происходит периодическая смена паролей, в RFID-системах подобные изменения могут быть невозможными в силу того, что радиочастот-

ные метки зачастую не всегда доступны для процесса назначения паролей. В связи с этим, хорошей практикой является назначение разных паролей для каждой метки и каждой области данных внутри метки, что существенно увеличит количество требуемых ресурсов на компрометацию паролей. Подобный подход требует использования и распространения базы данных, содержащей пароли, привязанные к идентификаторам меток. Возможен также подход с использованием некоторого секретного алгоритма генерации паролей на основе уникального идентификатора метки, что освобождает организацию от хранения и сопровождения баз данных с паролями.

3. Шифрование данных. Шифрованием возможно обеспечение надежной защиты хранимых и передаваемых открытыми каналами данных. Шифрование не исключает внешних угроз, связанных с физическим слежением и проникновением в радиоканалы связи, но значительно усложняет задачу для злоумышленника [2].
4. Подписывание данных. Подписывание информации, содержащейся на радиочастотной метке, электронной цифровой подписью позволяет исключить из участия в информационном обмене RFID-системы как копии меток, так и меток с измененными злоумышленником данными. Данный способ основан на добавлении неизменяемого уникального идентификатора радиочастотной метки к подписываемой информации, содержащейся на радиочастотной метке, с последующей генерацией некоторой цифровой подписи при помощи приватного ключа. Цифровая подпись хранится совместно с данными на радиочастотной метке и проверяется посредством открыто распространяемого публичного ключа. В данной схеме важным фактором является получение публичного ключа проверки подписи из достоверного источника.
5. Обеспечение физической защиты RFID-систем. Данный подход позволяет обеспечить защиту от фальсификации данных или генерации помех в работе RFID-системы путем реализации мероприятий по обеспечению электромагнитного экранирования места работы радиочастотной системы или через уменьшение мощности считывателя и, как следствие, расстояния считывания в цепочке считыватель – радиочастотная метка.

Имеющиеся возможности технологии радиочастотной идентификации и использование описанного выше комплекса мер по обеспечению защиты информации RFID-систем позволяют сделать вывод, что современное состояние мировой отрасли RFID можно охарактеризовать как фазу зрелого совершенствования. Несмотря на актуальность вопросов защищённости пассивных радиочастотных меток, требующих разработки специальных технических решений, предложенный разработчиками EPCglobal функционал, обеспечивающий защиту данных, совместно с классическими подходами защиты информации в информационных системах, имеет управляемые риски и может применяться для разработки RFID-систем.

Однако, несмотря на все достоинства и преимущества радиочастотных систем, следует признать существование реальных угроз конфиденциальности, что ограничивает область применения таких систем. В связи с этим, заинтересованные во внедрении RFID-систем структуры должны использовать различные методы защиты и управления системой защиты информации, оперативного и технического контроля для нивелирования рисков, возникающих при внедрении RFID-систем. Необходимо учитывать, что каждое конкретное внедрение RFID-системы неразрывно связано со спецификой выполняемых задач и не все действующие на сегодняшний день методы защиты могут быть эффективны в своей области применения. В первую очередь необходимо оценить риски, связанные с внедрением RFID-технологии, и выработать соответствующие решения по обеспечению контроля и

применению методов защиты информации, принимая во внимание все возможные факторы, такие как: величина угроз, стоимость внедрения и обеспечения технической поддержки, а так же производительность системы и возможный ущерб.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Васильев С.В., Силкин А.Т., Тикменова И.В., Уткин А.В.* Организация противодействия техническим средствам разведки в автоматизированных системах управления с элементами радиочастотной идентификации // Научно-методические материалы исследований, труды семинаров и научно-технических конференций 3 ЦНИИ МО РФ. Книга 12. – М.: 3ЦНИИ МО РФ, 2008. – С. 38-41.
2. *Агафьин С. С.* LW-криптография: шифры для RFID-систем // Безопасность информационных технологий. – 2011. – № 1. – С. 30-33.
3. *Sanjay E. Sarma, Stephen A. Weis, Daniel W.* Engels RFID Systems and Security and Privacy Implications, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139 // B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523. – 2003. – P. 454-469.
4. *Maricel O.* Balitanas and Taihoon Kim Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol // International Journal of Smart Home. – 2010. – Vol. 4, № 1, January. – P. 23-36.
5. *Liang Y., Rong C.,* Strengthen RFID Tags Security Using New Data Structure // International Journal of Control and Automation. – 2008. – Vol. 1, № 1. – P. 51-58.

Статью рекомендовал к опубликованию к.т.н. С.К. Самогин.

Михеев Вячеслав Алексеевич – ОАО “ИМЦ Концерна “Вега”; e-mail: mikheev@imc-vega.ru; 125190, г. Москва, ул. Балтийская, 14; тел.: 84957874381, доб. 200; генеральный директор; к.т.н.

Уткин Андрей Владимирович – e-mail: a.utkin@rfidcenter.ru; тел.: 84957874381, доб. 295; начальник отдела радиочастотной идентификации.

Виноградов Дмитрий Алексеевич – e-mail: d.vinogradov@rfidcenter.ru; тел.: 84957874381, доб. 318; начальник сектора разработки программного обеспечения.

Mikheev Vyacheslav Alekseevich – JSC "IMC of “Vega” Corporation”; e-mail: mikheev@imc-vega.ru; 14, Baltiyskaya street, Moscow, 125190, Russia; phone: +74957874381, ext. 200; director general; cand. of eng. sc.

Utkin Andrey Vladimirovich – e-mail: a.utkin@rfidcenter.ru; phone: +74957874381, ext. 295; head of department of radio frequency identification.

Vinogradov Dmitry Alekseevich – e-mail: d.vinogradov@rfidcenter.ru; phone: +74957874381, ext. 318; head of sector of software engineering.

УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В НЕОПРЕДЕЛЕННЫХ УСЛОВИЯХ ИХ ВОЗНИКНОВЕНИЯ*

В настоящее время организации используют электронный документооборот, при котором конфиденциальная информация циркулирует – хранится и обрабатывается в информационных системах. Информационные системы подвергаются всевозможным уг-

* Работа выполнена в соответствии с Госзаданием Министерства образования и науки проекты: № 7.701.2011; № 1/12.