УНИВЕРСИТЕТ ИТМО
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2022 Vol. 22 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2022-22-1-67-73
УДК 004.772

Алгоритм обнаружения RFID-дубликатов

Наталия Викторовна Волошина[1], Александр Андреевич Лавринович[2]✉

[1,2] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] nataliv@yandex.ru, https://orcid.org/0000-0001-9435-9580
[2] Lavrinovich600@gmail.com✉, https://orcid.org/0000-0002-5058-3473

Аннотация

Предмет исследования. При расширении применения RFID (Radio Frequency Identification)-технологии в качестве способа маркировки импортируемых товаров все более актуальной становится проблема использования злоумышленниками дубликатов RFID-меток. На дубликат может быть записана информация о товаре, которая отличается от его фактических характеристик. В работе предложен алгоритм обнаружения RFID-дубликатов как метод достижения целостности сведений, которые поступают в информационные системы международной транспортировки товаров. Актуальность создания алгоритма определена потребностью снижения риска создания и использования импортерами RFID-дубликатов при трансграничном перемещении маркируемых товаров. Существующие алгоритмы обнаружения дубликатов не подходят для применения в системе RFID-маркировки импортируемых в Россию товаров. Предложенный алгоритм ограничивает возможности злоумышленника считывать с оригинальной RFID-метки сведения, необходимые для создания RFID-дубликата. **Метод.** Алгоритм основан на разделении Electronic Product Code (EPC)-области памяти RFID-метки на части и применении команды самоуничтожения метки (kill) для предотвращения несанкционированных считываний. Рассмотрены сценарии реализации алгоритма и определены риски его использования. Алгоритм представлен в виде графической модели на основе нотации Business Process Model and Notation (BPMN). **Основные результаты.** Оценка эффективности предлагаемого алгоритма проведена с использованием формулы гипергеометрической вероятности. В качестве исходных данных приняты результаты проведения выборочной проверки RFID-меток таможенными органами. Показано, что в сравнении с существующим подходом реализация алгоритма в программно-аппаратном комплексе создает условия повышения вероятности обнаружения RFID-дубликатов при условии проведения контроля только в отношении высокорисковых декларантов. **Практическая значимость.** Применение алгоритма снижает риск поступления искаженной или недостоверной информации в информационные системы международной транспортировки товаров и повышает обоснованность принимаемых юридических и экономических решений в информационных системах таможенных органов.

Ключевые слова

RFID-технология, RFID-метка, RFID-дубликат, RFID-маркировка, информационная система, EPC-память, команда kill, целостность информации, маркировка товаров

Ссылка для цитирования: Волошина Н.В., Лавринович А.А. Алгоритм обнаружения RFID-дубликатов // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 67–73. doi: 10.17586/2226-1494-2022-22-1-67-73

An algorithm for detecting RFID duplicates

Natalia V. Voloshina[1], Aleksandr A. Lavrinovich[2]✉

[1,2] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] nataliv@yandex.ru, https://orcid.org/0000-0001-9435-9580
[2] Lavrinovich600@gmail.com✉, https://orcid.org/0000-0002-5058-3473

Abstract

The problem of using duplicate RFID tags by attackers is becoming more and more actual with the expansion of RFID technology for marking imported goods. The duplicate may contain information about goods, which differs from their

actual characteristics. This paper proposes an algorithm for detecting RFID duplicates as a method for achieving the integrity of information that enters the information systems of international goods transportation. The relevance of creating an algorithm deals with the need to reduce the risk of creating and using RFID duplicates by importers during the cross-border movement of marked goods. Existing duplicate detection algorithms are unsuitable for use in the RFID-marking system of goods imported into Russia. The algorithm hinders an attacker from reading data from the original RFID tag, which is necessary to create an RFID duplicate. The proposed algorithm is based on dividing the EPC memory area of an RFID tag into parts and using the tag self-destruction command (kill) to prevent unauthorized readings. The authors considered the scenarios for implementing the algorithm and identified the risks of using the algorithm. The algorithm is presented as a graphical model based on BPMN notation. The efficiency of the proposed algorithm was evaluated using the hypergeometric probability formula. The results of a selective check of RFID tags by the customs authorities were taken as the initial data. It is shown that, in comparison with the existing approach, the implementation of the algorithm in software and hardware complex increases the probability of detecting RFID duplicates, provided that control is carried out only in relation to high-risk declarants. The use of the algorithm reduces the risk of receiving distorted or inaccurate data in the information systems dealing with international goods transportation and increases the validity of legal and economic decisions taken in the information systems of customs authorities.

Keywords
RFID technology, RFID mark, RFID duplicate, RFID marking, information system, EPC memory, kill command, information integrity, marking of goods

For citation: Voloshina N.V., Lavrinovich A.A. An algorithm for detecting RFID duplicates. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 1, pp. 67–73 (in Russian). doi: 10.17586/2226-1494-2022-22-1-67-73

Введение

Для учета товаров в рамках внешней торговли применяется RFID (Radio Frequency Identification)-технология. RFID-метки — устройство, состоящее из чипа и антенны, закрепленных в этикетке — контрольном (идентификационном) знаке. RFID-метки выступают в качестве источника сведений о товарах. С помощью считывания RFID-меток формируются данные для информационных систем (ИС) международной транспортировки товаров, на основе которых пользователи системы могут принимать решения о товаре.

Работа посвящена формированию целостности информации, которая поступает в ИС с помощью RFID-технологии. При использовании изучаемых ИС актуально требование к отсутствию неправомерных искажений и добавлений к информации, что может быть обеспечено, если злоумышленник применяет RFID-дубликат.

В работах [1, 2] проанализированы два способа борьбы с RFID-дубликатами: профилактика и обнаружение. Преобладает мнение [1–7], что способ обнаружения — более эффективный, но менее затратный и универсальный. В работах [1–4, 8] рассмотрены алгоритмы метода обнаружения. Недостатки данных алгоритмов связаны с возможностью их применения лишь при наличии определенных условий, которые отсутствуют при формировании сведений в ИС международной транспортировки товаров.

С учетом невозможности применения существующих алгоритмов обнаружения RFID-дубликатов для решения проблемы формирования искаженных сведений в изучаемых ИС необходимо создание нового алгоритма для применения в данной сфере.

Новизна предлагаемого алгоритма обнаружения RFID-дубликатов заключается в том, что он основан на разделении Electronic Product Code (EPC)-области памяти RFID-меток на три части и применении команды kill (команда уничтожения RFID-метки, после этого метку уже нельзя использовать). Алгоритм применим в сфере использования государственных ИС международной транспортировки товаров. Он позволяет повысить вероятность обнаружения дубликатов на 14,1 % (без применения алгоритма вероятность обнаружения равна 24,8 %, а с наличием алгоритма — 38,9 %). Повышение вероятности обнаружения RFID-дубликатов связано с обеспечением информационной безопасности для снижения рисков поступления недостоверной, искаженной информации в ИС. Авторами рассмотрена государственная ИС международной транспортировки товаров, которая используется таможенными органами, как органами государственной власти, назначение которой — реализация полномочий таможенными органами в пределах своей компетенции.

Постановка задачи повышения безопасности информационных систем международной транспортировки товаров

Рассмотрим RFID-технологии [9] и обеспечение целостности информации при формировании сведений в ИС международной транспортировки товаров с ее применением. Сведения, поступающие с RFID-меток в изучаемые ИС, должны быть достоверными, иначе таможенными органами могут быть приняты некорректные юридические (например, решение о выпуске товаров таможенными органами) и экономические (например, взимание таможенных платежей) решения в отношении товаров. Пользователи ИС должны работать с информацией, которая не содержит несанкционированных модификаций.

Способом нарушения целостности в данном случае является использование RFID-дубликатов злоумышленниками. Реализация данного способа показана на рис. 1.

Чтобы не допустить формирования сведений в ИС с RFID-дубликатов, необходимы способы проверки оригинальности RFID-меток. Характеристики существующих алгоритмов обнаружения RFID-дубликатов представлены в табл. 1.

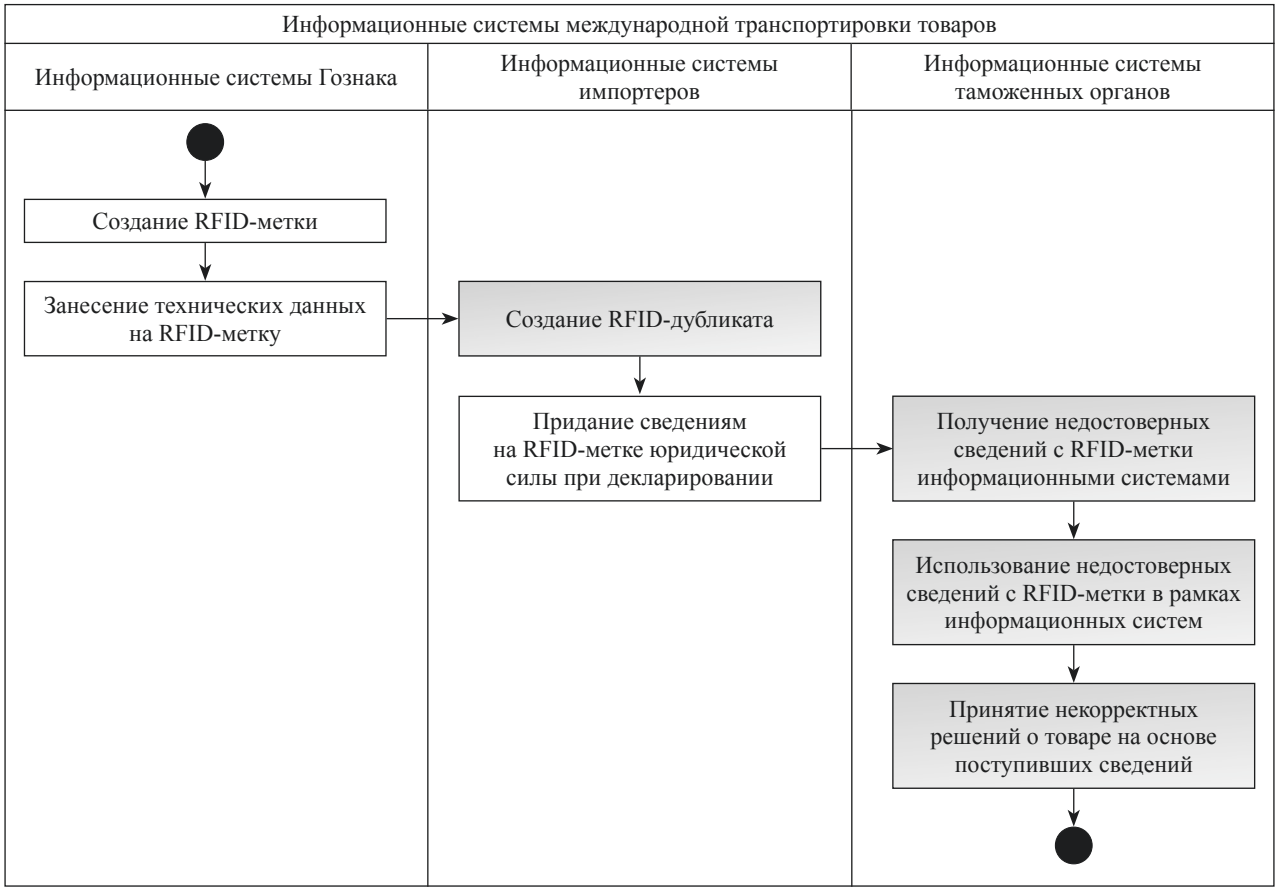

Рис. 1. Модель использования RFID-дубликатов для формирования искаженных сведений в информационных системах международной транспортировки товаров

Fig. 1. The model of using RFID duplicates for the formation of distorted information in information systems for the international transportation of goods

Рассмотренные алгоритмы (табл. 1) действуют по схожему принципу. Для их реализации требуются RFID-метки с перезаписываемой памятью, так как на метки заносится некоторая информация, которая впоследствии сопоставляется с другими сведениями. Применение алгоритмов обусловлено требованием к целостности информации, которую пользователь получает с RFID-метки.

Таблица 1. Критерии алгоритмов обнаружения RFID-дубликатов

Table 1. Characteristics of RFID duplicate detection algorithms

Критерий	Алгоритмы обнаружения RFID-дубликатов, рассмотренные в работах		
	[1]	[2]	[3]
Основной принцип метода	Согласованность двойных хеш-коллизий и модифицированный вектор эскиза count-min	При каждом считывании на метку записываются случайные значения, из них создается «хвост»	Перезаписываемая память меток: при каждом считывании случайное число изменяется
Определение дубликата	Частота чтения дубликата ниже, чем оригинальной метки	Хвосты дубликатов отличаются от хвостов оригинальных меток	Сравнение сведений о случайном числе на метке и случайном числе в базе данных
RFID-считыватели	Минимум три авторизованных считывателя	Минимум четыре авторизованных считывателя	—
Сфера применения	Системы с временными границами для прибытия маркируемых товаров	Цепочка поставок; система с использованием подконтрольных RFID-считывателей	Коммерческие системы с многократным считыванием меток
Команда kill	Не используется	Не используется	Не используется
Базы данных для проверки подлинности метки	Не используются	Используются локальные базы данных	Используются централизованные базы данных

Но недостатки алгоритмов связаны с узкой сферой применения каждого из них. Во всех случаях алгоритмы разработаны для систем, в которых объекты с RFID-метками проходят путь согласно плану, и в рамках этого пути периодически происходит считывание RFID-меток, что позволяет и записать новую информацию, и проверить предыдущие записанные на метку сведения. В случае с изучаемыми ИС международной транспортировки товаров такой возможности нет, так как метка производится уполномоченной организацией, она поставляется импортерам, которые заносят на метку сведения и далее используют метки при таможенном оформлении. В связи с этим ставится задача разработки нового алгоритма по обнаружению RFID-дубликатов, который мог бы быть применен в изучаемых ИС.

Предложенный алгоритм обнаружения RFID-дубликатов

Сфера применения предлагаемого алгоритма — государственные ИС, входящие в систему государственной маркировки импортируемых товаров [10]. Рассмотрим принципы предлагаемого алгоритма.

1. EPC-область памяти делится на три части. В первую часть при создании метки на Гознаке должно быть записано число I. Вторая часть резервируется для результата считывания импортером. Третья часть резервируется для числа T, которое записывается при считывании таможней. После получения сведений считыватель таможни проверяет EPC-область памяти, и делается вывод о статусе метки.
2. Последующие считывания доступны только считывателям таможенного органа путем обновления числа T в третьей части EPC-области памяти. Если это действительно число T, метка направляет информацию этому считывателю, а если нет, то срабатывает команда kill и метка уничтожается. В данном случае команда kill играет защитную функцию [11], она не выступает в качестве угрозы информационной безопасности [12].
3. Данный алгоритм предполагает, что метка содержит два числа, получив которые злоумышленник может изготовить дубликат — Transponder identification number (TID)-номер и число I. Для получения этих чисел требуется два считывания. Но у импортера есть возможность произвести только одно считывание, если им будет произведено второе считывание, то RFID-меткой будет установлено, что оно производится считывателем импортера, а не считывателем таможенного органа, и тогда метка применит команду kill, в результате чего она становится непригодной для использования, и дальнейшие действия по считыванию метки станут невозможными.

Алгоритм применения метода в виде блок-схемы в обобщенном виде представлен на рис. 2.

В алгоритме можно выделить следующие два сценария.

1. «Оригинальная метка». Если импортер планирует легальным образом использовать RFID-метку, то он записывает на нее Global Trade Item Number (GTIN)-номер, который заносится на вторую часть EPC-области памяти RFID-метки. Далее метка представляется к считыванию таможенному органу. Авторизованный RFID-считыватель таможенного органа записывает число T в третью часть EPC-области памяти. Метка проверяет структуру числа T, и если это действительно число T, отвечающее требованиям к этому числу, то метка передает информацию из EPC-области памяти считывателю таможенного органа. Данный считыватель проверяет структуру информации, полученной из EPC-области памяти с помощью сведений, поступивших из централизованной базы данных Гознака. В данном сценарии делается вывод о том, что метка оригинальна, и поступившая с нее информация – достоверна. Следовательно, обеспечивается целостность информации для ИС международной транспортировки товаров, что позволяет принимать корректные решения в отношении товаров.
2. «Дубликат». Если импортер планирует ввести в процесс использования RFID-технологии дубликат, то ему необходимо сначала создать его. При условии применения предлагаемого метода, одним из способов создания дубликата является считывание информации с оригинальной метки [13] (TID-номера и числа I), создание дубликата с этими сведениями и GTIN-номером, который указывает на недостоверные сведения о товаре. Для получения сведений, необходимых для создания дубликата, требуется произвести, во-первых, считывание TID-номера, так как эта информация заносится на метку производителем метки, в данном случае это импортер, а не Гознак. Тогда в EPC-области памяти во вторую часть делается запись TID, а не GTIN, как в первом сценарии. Во-вторых, требуется считывание числа I, которое также заносится производителем метки. Считывание числа I повлечет за собой занесение в третью часть EPC-области памяти числа I, но для третьей части EPC-области памяти установлено требование, что в ней должно находиться число T. Соответственно, меткой при обнаружении записи, отличной от числа T, в третьей части EPC-области памяти, применяется команда kill, что приводит к самоуничтожению метки. Это делает невозможным ее дальнейшее использование, и импортер вынужден будет заново заказывать метки у Гознака. Если импортер решит использовать метку с легальным TID-номером, но с пустой EPC-памятью, то это будет обнаружено RFID-считывателем таможенного органа, так как EPC-область памяти не будет содержать структуру «I-GTIN-T». В таком случае будет сделан вывод о статусе метки – «дубликат».

Риски при использовании алгоритма связаны с тем, что злоумышленнику может быть заранее известно число TID или число I. Контрмерами в таком случае должны выступать меры по обеспечению защиты ИС Гознака, каналов связи, по которым передаются сведения из базы данных Гознака в ИС таможенных органов, обеспечению защиты помещений Гознака.

Предложенный в работе алгоритм отличается от существующих [1, 3] разделением EPC-области памяти на

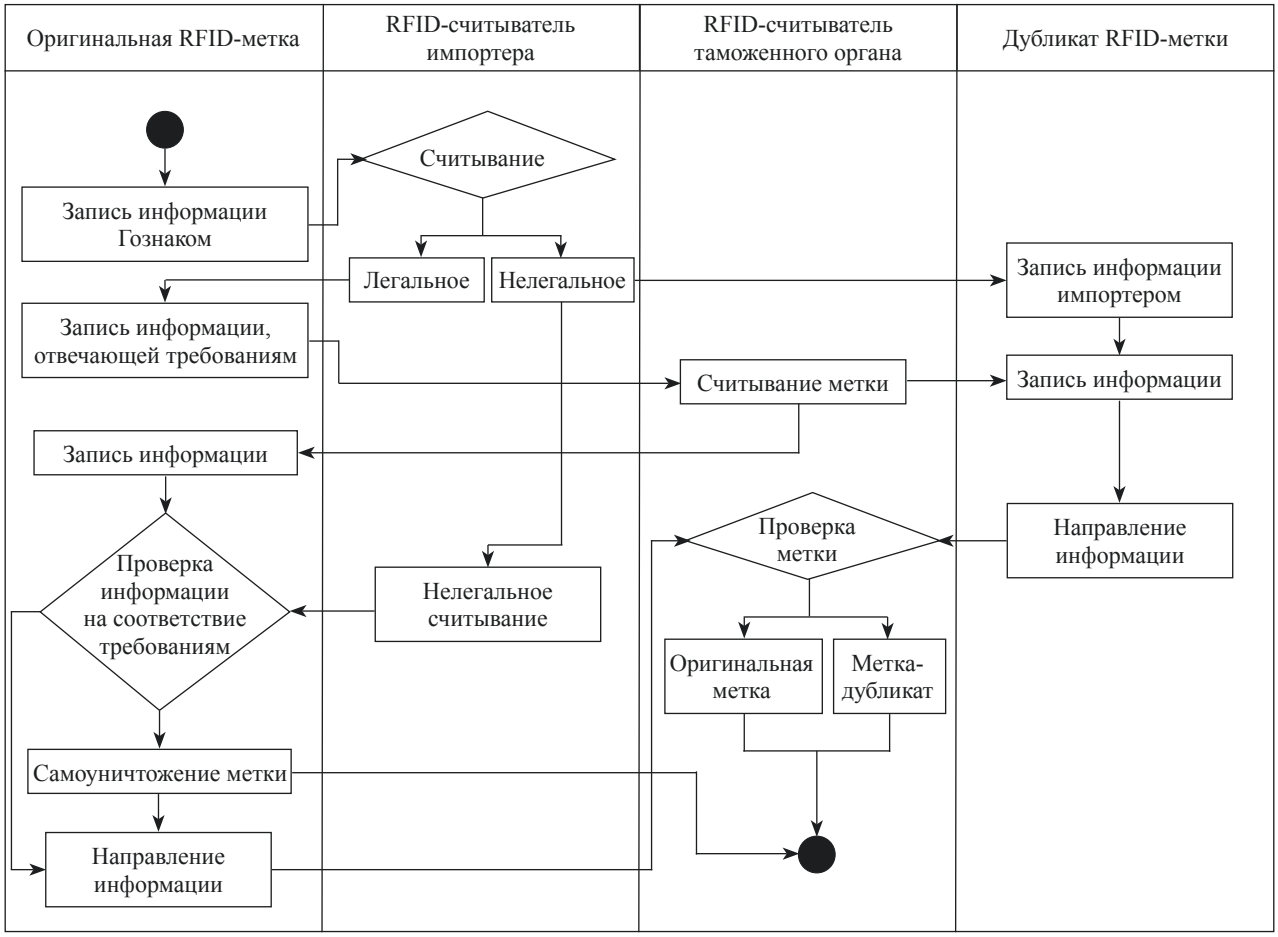

Рис. 2. Предлагаемый алгоритм обнаружения RFID-дубликатов

Fig. 2. The proposed algorithm for detecting RFID duplicates

части, применением команды kill при несанкционированных считываниях, применением централизованных баз данных для проверки подлинности метки, меньшим числом требуемых авторизованных считывателей и меньшим числом операций в протоколе взаимодействия метки и считывателя.

Ситуацию обнаружения дубликатов RFID-меток можно рассмотреть, как обнаружение объекта, обладающего заданными свойствами, среди некоторого количества объектов (выборки). Вероятность обнаружения RFID-дубликата в выборке RFID-меток, нанесенных на товары, можно определить по формуле гипергеометрической вероятности:

$$P = \frac{C_K^k C_{N-K}^{n-k}}{C_N^n}, \qquad (1)$$

где P — вероятность обнаружения RFID-дубликата в выборке RFID-меток, нанесенных на товары; k — число обнаруженных RFID-дубликатов среди совокупности RFID-меток; n — число проверенных RFID-меток; N — совокупность RFID-меток; K — число RFID-дубликатов в совокупности RFID-меток; C_K^k — число всех способов обнаружить k RFID-дубликатов из K возможных; C_{N-K}^{n-k} — число всех способов проверить $n - k$ RFID-меток из $N - K$ возможных; C_N^n — число возможных исходов результатов проверки RFID-меток.

Текущая ситуация выявления RFID-дубликатов связана с проведением досмотров должностными лицами таможенных органов (P_1). Повышение безопасности ИС должно быть обеспечено при использовании алгоритма обнаружения, являющегося базой программно-аппаратного комплекса (P_2).

Оценка предлагаемого алгоритма обнаружения RFID-дубликатов для двух ситуаций приведена в табл. 2. Исходные данные для оценки, полученные по результатам таможенного контроля[1,2]: 100 RFID-меток, нанесенных на импортируемые товары; 10 RFID-дубликатов, которые находятся среди RFID-меток.

При проведении оценки учитывалось, что таможенные досмотры проводятся в отношении 3 % товарных партий, поэтому вероятность обнаружить при проверке трех меток один RFID-дубликат $P(1)_1$ составляет 24,8 %. При условии реализации алгоритма обнаруже-

[1] Итоговые доклады о результатах деятельности ФТС России (официальный сайт ФТС России) [Электронный ресурс]. Режим доступа: https://customs.gov.ru/activity/results/itogovye-doklady-o-rezul-tatax-deyatel-nosti, свободный. Яз. рус. (дата обращения: 28.07.2021).

[2] Таможенная статистика внешней торговли РФ [Электронный ресурс]. Режим доступа: https://customsonline.ru/search_ts.html, свободный. Яз. рус. (дата обращения: 28.07.2021).

Таблица 2. Оценка предлагаемого алгоритма обнаружения RFID-дубликатов

Table. 2. Evaluation of the proposed RFID duplicate detection algorithm

Параметр оценки	Ситуация	
	Текущая ситуация обнаружения дубликатов RFID-меток	Ситуация с учетом внедрения алгоритма обнаружения дубликатов RFID-меток
Способ обнаружения	Проведение таможенного досмотра	Проведение автоматической проверки RFID-меток, нанесенных на товары, декларируемые импортерами высокой категории риска по системе категорирования
Охват проверки	Три RFID-метки	Семь RFID-меток
Требуемый результат	Обнаружение одного RFID-дубликата	Обнаружение одного RFID-дубликата
Вероятность получения требуемого результата $P(1)$ по формуле (1)	$P(1)_1 = \frac{C_{10}^1 C_{90}^2}{C_{100}^3} = \frac{10 \times 4005}{161700} = 0{,}248$	$P(1)_2 = \frac{C_{10}^1 C_{90}^6}{C_{100}^7} = \frac{10 \times 622614630}{16007560800} = 0{,}389$

ния RFID-дубликатов в виде программно-аппаратного комплекса в таможенных органах и его применении в отношении декларантов высокой категории риска по системе категорирования (7 % от общего числа декларантов), вероятность обнаружить при проверке семи меток один RFID-дубликат $P(1)_2$ — 38,9 %. Таким образом, реализация предлагаемого алгоритма позволит создать условия, при которых вероятность обнаружения дубликата будет выше на 14,1 %, чем при текущей практике их обнаружения, и при условии, что охват контроля ограничен только участниками внешнеэкономической деятельности (ВЭД) высокой категории риска. При этом не исключается, что по системе управления рисками таможенных органов контроль также может проводиться и в отношении участников ВЭД иных категорий риска, что позволит сделать вероятность получения требуемого результата еще выше.

Рекомендации по реализации алгоритма: применение RFID-меток с типом памяти RW, создание программно-аппаратного комплекса в таможенных органах по считыванию RFID-меток и обработке сведений, позволяющий сделать вывод о статусе метки. С учетом того, что применение RFID-меток с типом памяти RW приведет к росту их стоимости, из экономических соображений целесообразно реализовывать данный проект в отношении категорий товаров, по которым установлен высокий уровень криминогенности при их импорте (уклонение от уплаты таможенных платежей, недостоверное декларирование, занижение таможенной стоимости). Стоит внедрять программно-аппаратный комплекс в рамках проектов по построению интеллектуальных пунктов пропуска, чтобы получение информации с RFID-меток было не только мерой контроля, но и стандартной операцией по перемещению товаров через границу вместо ручного досмотра. За счет этого может увеличиться скорость прохождения таможенного оформления, что приведет к снижению таможенных затрат участников ВЭД.

Заключение

Решение задачи обеспечения целостности при использовании RFID-технологии в информационных системах международной транспортировки товаров достигается путем снижения рисков создания и использования импортерами RFID-дубликатов. Снижение рисков в настоящем исследовании связывается с увеличением вероятности обнаружения RFID-дубликата в выборке RFID-меток, нанесенных на товары, такую вероятность можно определить по формуле гипергеометрической вероятности.

Предложен алгоритм обнаружения RFID-дубликатов, применимый для информационных систем международной транспортировки товаров, входящих в систему государственной маркировки импортируемых товаров. Алгоритм снижает риски создания и использования дубликатов путем ограничения возможностей злоумышленника по получению сведений, необходимых для создания дубликата. При реализации алгоритма в виде программно-аппаратного комплекса могут быть созданы условия, при которых вероятность обнаружения дубликата RFID-метки выше на 14,1 % по сравнению с текущей практикой (без учета алгоритма вероятность обнаружения составляет 24,8%, с учетом алгоритма — 38,9 %).

Таким образом, приведенные сведения позволяют сделать вывод о целесообразности предлагаемого алгоритма, так как он применим к специфической области (в государственных информационных системах в рамках системы маркировки импортируемых товаров), а за счет возможностей по его автоматизации он позволяет добиться увеличения вероятности обнаружения RFID-дубликатов в сравнении с существующим подходом по выборочной проверке RFID-меток в таможенных органах на 14,1 %. Перспективы исследования заключаются в дальнейшей детализации структуры EPC-области памяти RFID-метки для снижения рисков создания и использования злоумышленниками дубликатов RFID-меток.

Литература

1. Kamaludin H., Mahdin H., Abawajy J.H. Clone tag detection in distributed RFID systems // PLoS ONE. 2018. V. 13. N 3. P. e0193951. https://doi.org/10.1371/journal.pone.0193951
2. Zanetti D., Capkun S., Juels A. Tailing RFID tags for clone detection // NDSS Symposium. 2013.
3. Lehtonen M., Ostojic D., Ilic A., Michahelles F. Securing RFID systems by detecting tag cloning // Lecture Notes in Computer Science. 2009. V. 5538. P. 291–308. https://doi.org/10.1007/978-3-642-01516-8_20
4. Jokhio I.A., Jokhio S.H., Baloch J.A. A novel security method to protect RFID cloning attacks. 2012 [Электронный ресурс]. URL: http://oaji.net/articles/2016/2712-1454748209.pdf (дата обращения: 28.07.2021).
5. Shi J., Kywe S.M., Li Y. Batch clone detection in RFID-enabled supply chain // Proc. of the 2014 IEEE International Conference on RFID (IEEE RFID). 2014. P. 118–125. https://doi.org/10.1109/RFID.2014.6810721
6. Chen X., Liu J., Wang X., Zhang X., Wang Y., Chen L. Combating tag cloning with COTS RFID devices // Proc. of the 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). 2018. P. 1–9. https://doi.org/10.1109/SAHCN.2018.8397134
7. Bu K., Xu M., Liu X., Luo J., Zhang S., Weng M. Deterministic detection of cloning attacks for anonymous RFID systems // IEEE Transactions on Industrial Informatics. 2015. V. 11. N 6. P. 1255–1266. https://doi.org/10.1109/TII.2015.2482921
8. Jin B., Jin H. Security analysis of RFID based on multiple readers // Procedia Engineering. 2011. V. 15. P. 2598–2602. https://doi.org/10.1016/j.proeng.2011.08.488
9. Финкенцеллер К. RFID-технологии. Справочное пособие / пер. с нем. М.: Додека XXI век, 2016. 490 с.
10. Волошина Н.В., Лавринович А.А. Рекомендации по автоматическому обнаружению дубликатов RFID-меток таможенными органами // Таможенные чтения — 2020. Стратегия развития 2030: вызовы времени. наука и инновации: Сборник материалов Международной научно-практической конференции. В 2-х т. Т. 1. СПб., 2020. С. 88–93.
11. Okpara O. Detecting Cloning Attack in Low-Cost Passive RFID Tags. 2015 [Электронный ресурс]. URL: https://www.researchgate.net/publication/280077859_Detecting_Cloning_Attack_in_Low-Cost_Passive_RFID_Tags (дата обращения: 28.07.2021). https://doi.org/10.13140/RG.2.1.1709.4240
12. Mitrokotsa A., Rieback M.R., Tanenbaum A.S. Classifying RFID attacks and defenses // Information Systems Frontiers. 2010. V. 12. N 5. P. 491–505. https://doi.org/10.1007/s10796-009-9210-z
13. Huang W., Zhang Y., Feng Y. ACD: An adaptable approach for RFID cloning attack detection // Sensors. 2020. V. 20. N 8. P. 2378. https://doi.org/10.3390/s20082378

References

1. Kamaludin H., Mahdin H., Abawajy J.H. Clone tag detection in distributed RFID systems. *PLoS ONE*, 2018, vol. 13, no. 3, pp. e0193951. https://doi.org/10.1371/journal.pone.0193951
2. Zanetti D., Capkun S., Juels A. Tailing RFID tags for clone detection. *NDSS Symposium*, 2013.
3. Lehtonen M., Ostojic D., Ilic A., Michahelles F. Securing RFID systems by detecting tag cloning. *Lecture Notes in Computer Science*, 2009, vol. 5538, pp. 291–308. https://doi.org/10.1007/978-3-642-01516-8_20
4. Jokhio I., Jokhio S.H., Baloch J.A. *A novel security method to protect RFID cloning attacks*. 2012. Available at: http://oaji.net/articles/2016/2712-1454748209.pdf (accessed: 28.07.2021).
5. Shi J., Kywe S.M., Li Y. Batch clone detection in RFID-enabled supply chain. *Proc. of the 2014 IEEE International Conference on RFID (IEEE RFID)*, Orlando, FL, USA, 2014, pp. 118–125. https://doi.org/10.1109/RFID.2014.6810721
6. Chen X., Liu J., Wang X., Zhang X., Wang Y., Chen L. Combating tag cloning with COTS RFID devices. *Proc. of the 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2018, pp. 1–9. https://doi.org/10.1109/SAHCN.2018.8397134
7. Bu K., Xu M., Liu X., Luo J., Zhang S., Weng M. Deterministic detection of cloning attacks for anonymous RFID systems. *IEEE Transactions on Industrial Informatics*, 2015, vol. 11, no. 6, pp. 1255–1266. https://doi.org/10.1109/TII.2015.2482921
8. Jin B., Jin H. Security analysis of RFID based on multiple readers. *Procedia Engineering*, 2011, vol. 15, pp. 2598–2602. https://doi.org/10.1016/j.proeng.2011.08.488
9. Finkenzeller K. *RFID Handbook Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Wiley, 2010, 480 p.
10. Voloshina N.V., Lavrinovich A.A. Recommendations for automatic detection RFID-mark duplicates by customs bodies. *"Customs readings 2020. Strategy 2030: challenges, science and innovations". Proceedings of the International scientific and practical conference.* St. Petersburg, 2020, pp. 88–93. (in Russian)
11. Okpara O. *Detecting Cloning Attack in Low-Cost Passive RFID Tags*. 2015. Available at: https://www.researchgate.net/publication/280077859_Detecting_Cloning_Attack_in_Low-Cost_Passive_RFID_Tags (accessed: 28.07.2021). https://doi.org/10.13140/RG.2.1.1709.4240
12. Mitrokotsa A., Rieback M.R., Tanenbaum A.S. Classifying RFID attacks and defenses. *Information Systems Frontiers*, 2010, vol. 12, no. 5, pp. 491–505. https://doi.org/10.1007/s10796-009-9210-z
13. Huang W., Zhang Y., Feng Y. ACD: An adaptable approach for RFID cloning attack detection. *Sensors*, 2020, vol. 20, no. 8, pp. 2378. https://doi.org/10.3390/s20082378

Авторы

Волошина Наталия Викторовна — кандидат технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0001-9435-9580, nataliv@yandex.ru

Лавринович Александр Андреевич — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-5058-3473, Lavrinovich600@gmail.com

Authors

Natalia V. Voloshina — PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0001-9435-9580, nataliv@yandex.ru

Aleksandr A. Lavrinovich — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0002-5058-3473, Lavrinovich600@gmail.com

Статья поступила в редакцию 16.09.2021
Одобрена после рецензирования 07.12.2021
Принята к печати 27.01.2022

Received 16.09.2021
Approved after reviewing 07.12.2021
Accepted 27.01.2022