DOI 10.36622/VSTU.2022.25.4.010
УДК 004.056.53

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА ИНИЦИАЛИЗАЦИИ RFID-КАРТЫ С ИСПОЛЬЗОВАНИЕМ СКАНИРОВАННОГО ИЗОБРАЖЕНИЯ ОТПЕЧАТКА ПАЛЬЦА

Ю.Ю. Громов, П.Ю. Пушкин, П.И. Карасев, М.А. Гладышев

В работе предлагается разработка усовершенствованной высокочастотной RFID-карты (NFC-карты) со сканером отпечатка пальцев. Описывается стек протоколов NFC для различных существующих реализаций данной технологии и выбора подходящего места для внедрения элементов управления сканером отпечатка пальцев. Приводится описание процесса инициализации карт, основанных на протоколе ГОСТ Р ИСО/МЭК 14443-3-2014. Осуществляется сравнительный анализ существующих видов сканеров отпечатков пальцев и поиск приемлемого решения в отношении применения его в разработке по параметрам стоимости, должного уровня безопасности и типоразмера самого датчика. Приводится новый алгоритм инициализации карты после внедрения в её состав сканера отпечатка пальцев, а также преимущества данного подхода в отношении решения проблем передачи карт третьим лицам, ретрансляции или копирования к затрачиваемым средствам. Предлагаются потенциальные сферы применения данной разработки и преимущества её внедрения по отношению к стандартным решениям. В завершении делаются заключения о перспективах внедрения данной разработки в описанные сферы применения и целесообразности данного процесса для компаний-потребителей разрабатываемого продукта.

Ключевые слова: RFID-карта, NFC-карта, биометрия, сканер отпечатка пальцев, информационная безопасность.

Введение

На сегодняшний день использование высокочастотных RFID-карт, именуемых также NFC-картами, получило широкое распространение [7], начиная от проездных билетов и карт доступа систем контроля и управления доступом, заканчивая банковскими картами и аппаратными идентификаторами в средствах доверенной загрузки. Как следствие, появилось огромное количество разнообразных протоколов взаимодействия между картами и считывателями, но ни одна из них одновременно не решает проблемы передачи самой карты третьему лицу, её ретрансляции или копирования, что потенциально снижает безопасность их использования [8]. Разработчики протоколов и производители карт предпринимали попытки решения данных проблем, применяя алгоритмы двухсторонней аутентификации в картах и считывателях, что решало проблемы ретрансляции и копирования. Но противостояние передаче карты третьему лицу, как правило, решалось добавлением еще одной системы аутентификации, то есть созданием двухфакторной аутентификации. Такой подход требует больше затрат.

Разработкой, описанной в статье, предлагается решить озвученные ранее проблемы и, получив такую же по уровню обеспечения безопасности систему, значительно снизить стоимость её создания или внедрения в уже существующие системы.

Для этого следует выдвинуть определенные требования к разрабатываемой RFID-карте: должна обладать всеми преимуществами стандартных карт, не нарушать функционирование существующей инфраструктуры и решать приведённые ранее проблемы. Сам же подход решения, как следствие многообразия реализаций RFID-карт, должен быть универсален для многих протоколов и незначительно удорожать производство изделия. Учитывая все вышеперечисленное, предлагается внедрить в RFID-карту сканер отпечатка пальцев.

Основная часть. Стек протоколов

Для выбора места внедрения функционала сканера отпечатка пальцев необходимо определить стек протоколов NFC для типа A, рис. 1 [10].

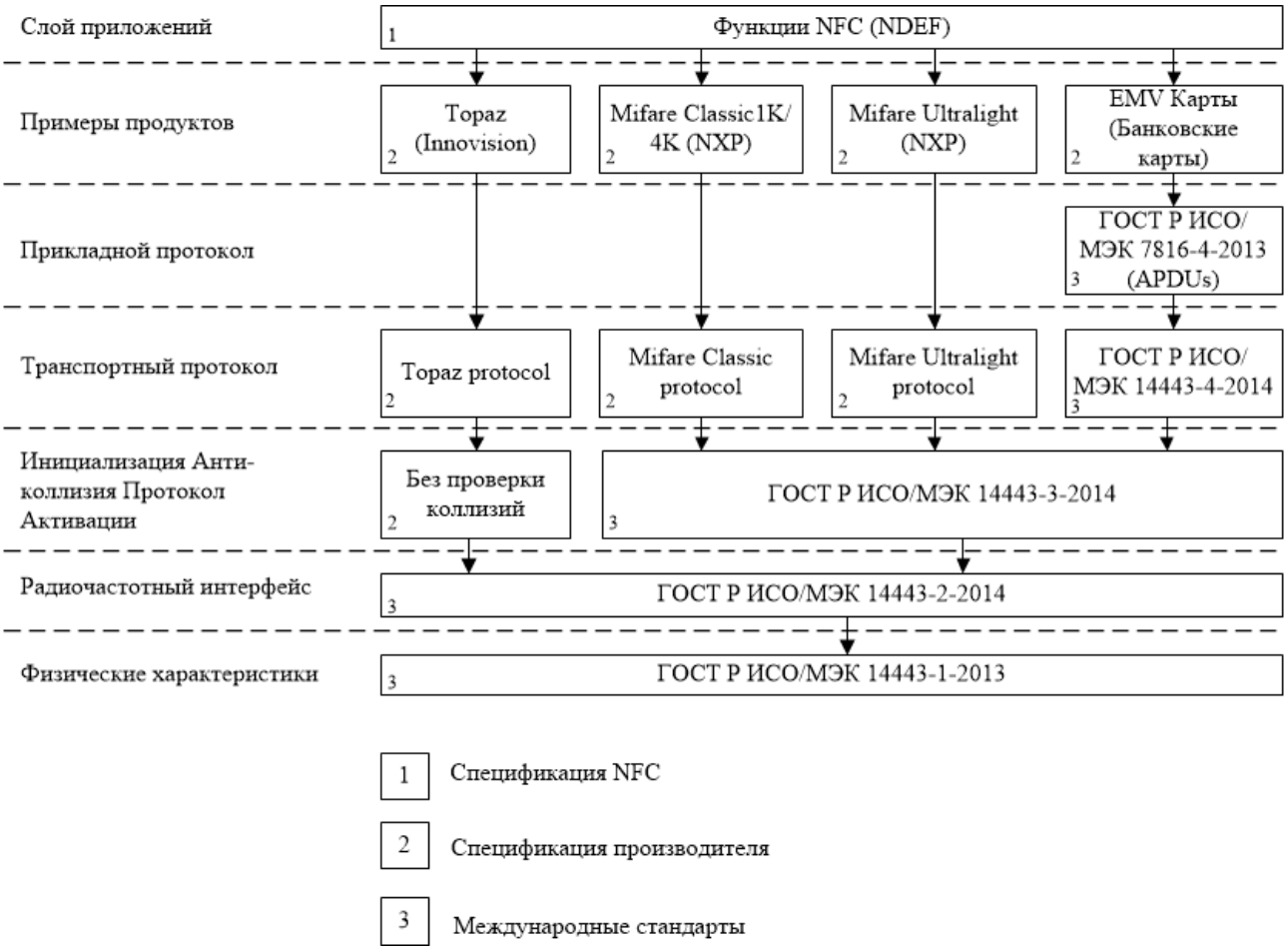

Рис. 1. Стек протоколов NFC

Глобально протоколы можно разделить на 3 группы:

1. Спецификация NFC
2. Спецификация производителя
3. Международные стандарты

Спецификация NFC, как и слой приложения, – это определенный NFC Forum общий стандарт данных, названный NDEF, который может использоваться, чтобы сохранять и передавать различные виды элементов данных.

Спецификация производителя – это проприетарные транспортные протоколы обмена информацией, созданные одним вендором. На схеме представлены протоколы, разработанные компаниями Topaz, Mifare и Europay+MasterCard+Visa(EMV).

При создании универсального подхода необходимо опираться на протокол, используемый максимально большим числом продуктов. Одним из таких протоколов является NDEF, но так как этот протокол выше всех в иерархии, есть вероятность передачи части полезной информации на нижележащих уровнях, что, в свою очередь, не обеспечит требуемый уровень безопасности после встраивания сканера отпечатков пальцев в состав RFID-карты.

Следующими максимально общими являются протоколы: ГОСТ Р ИСО/МЭК 14443-1-2013, описывающий физические характеристики карт [1], и ГОСТ Р ИСО/МЭК 14443-2-2014, описывающий радиочастотный энергетический и сигнальный интерфейс [2]. Но в силу своей низкоуровневой специфики они не подходят для использования в

элементах управления сканером отпечатков пальцев.

Следующим по частоте использования идет протокол инициализации, описанный в ГОСТ Р ИСО/МЭК 14443-3-2014, являющимся единым для многих разновидностей карт. На его основе строится большая часть транспортных протоколов различных производителей, в нем есть управляющие команды, опираясь на которые можно сформировать искомый универсальный подход решения поставленных задач.

Процесс инициализации

Для определения способа встраивания на данном уровне механизмов управления сканером отпечатка пальцев необходимо подробно изучить процесс инициализации карты, представленный на рис. 2 [3].

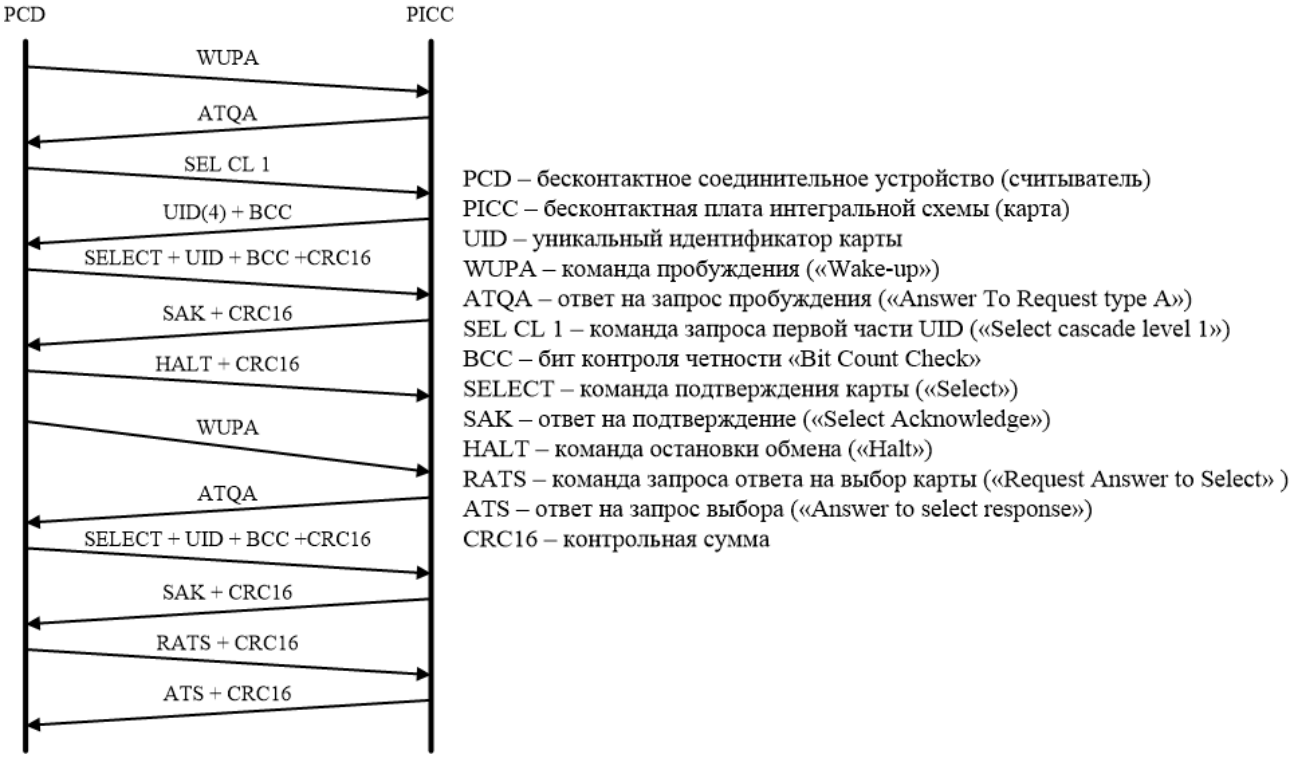

Рис. 2. Процесс инициализации карты

В терминологии ГОСТа PCD – бесконтактное соединительное устройство (считыватель) и PICC – бесконтактная плата интегральной схемы (карта), у каждой из которых есть свой уникальный идентификатор (UID).

Считыватель постоянно передает команду «Wake-up» (WUPA), как только в поле действия появляется карта, она отвечает командой «Answer To Request type A» (ATQA). Получив этот ответ, считыватель начинает процедуру выявления коллизий для определения есть ли в поле действия более одной карты, посылая команду «Select cascade level 1» (SEL CL 1), запрашивая у всех карт первую часть своих идентификаторов UID. В ответ карта присылает первые четыре байта UID и бит контроля четности«Bit Count Check» (BCC) в конце. Получив идентификаторы карт, считыватель обращается к конкретной карте командой «SELECT», за которой следует UID, BCC и CRC16. Карта отвечает «Select Acknowledge» (SAK) и CRC16. Если на этом шаге получено более одного SAK, считыватель может уменьшить длину UID в команде «SELECT», пока не ответит одна карта. Как только это происходит, считыватель посылает команду «HALT» и CRC16, завершая связь.

Дальше процедура повторяется. Считыватель пробуждает карту (команда WUPA) и сразу исполняет команду «SELECT», за которой следует UID, BCC и CRC16 без проверки коллизий. Получает ответ SAK и посылает команду «Request Answer to Select» (RATS) и CRC16, на что

карта отвечает «Answer to select response» (ATS), содержащий информацию о максимальном размере кадра и параметрах канального уровня, и CRC16. На этом процесс инициализации завершен и начинается работа более высокоуровневых протоколов карты, то есть процесс передачи считывателю полезной нагрузки карты.

Такой обмен может быть опасен, так как возможна ретрансляция или копирование карт для прохода через СКУД или идентификации в средстве доверенной загрузки, а для банковских карт получение номера карты, данных о владельце, даты истечения, когда они просто лежат в кармане одежды [9].

Для решения данных проблем, как ранее уже упоминалось, предлагается встроить в RFID-карту сканер отпечатка пальцев.

Выбор сканера отпечатка пальцев

На рынке существует множество разновидностей сканеров, которые глобально можно разделить на три группы [5]:

– Оптические;
– Кремниевые (полупроводниковые);
– Ультразвуковые.

Каждая из этих групп включает в себя конкретные реализации. В табл. 1 представлено сравнение потенциально применимых оптических сканеров отпечатков пальцев.[4,6]

Таблица 1

Сравнение оптических сканеров

Тип	Преимущества	Недостатки
FTIR-сканеры	Низкая себестоимость	Неэффективная защита от муляжей
		Чувствительность к загрязнениям
Оптоволоконные сканеры	Высокая надежность считывания	Сложность реализации
	Устойчивость к обману	
Бесконтактные сканеры	Низкая себестоимость	Большие размеры
		Неэффективная защита от муляжей

Основным недостатком данного класса сканеров, останавливающим его применение в разработке, являются размеры датчика. Данный тип сканеров в силу особенностей используемого типа считывания папиллярного рисунка не может быть вписан в габариты RFID-карты, а одним из требований к разработке было полное соответствие стандартным размерам RFID-карт, описанным в ГОСТ Р ИСО/МЭК 14443-1-2013 [1].

Следующей группой сканеров отпечатков пальцев являются кремниевые. В табл. 2 представлено сравнение потенциально применимых кремниевых сканеров отпечатков пальцев [4,6].

Таблица 2

Сравнение кремниевых сканеров

Тип	Преимущества	Недостатки
Емкостные сканеры	Низкая себестоимость	Неэффективная защита от муляжей
	Надежность	
Радиочастотные сканеры	Устойчивость к обману	Неустойчивая работа при плохом контакте с пальцем
Чувствительные к давлению сканеры	Низкая себестоимость	Низкая чувствительность
		Неэффективная защита от муляжей
		Подверженность повреждениям при чрезмерно прилагаемых усилиях
Термо-сканеры	Высокая чувствительность к электростатическому разряду	Быстрое исчезновение изображения, поскольку через короткое время палец и датчик приходят к температурному равновесию
	Устойчивая работа в широком температурном диапазоне	
	Эффективная защита от муляжей	

Данный класс сканеров устраняет главный недостаток оптических сканеров – размеры, сканеры любого типа данной группы обладают малыми размерами, что позволяет их встроить в габариты карты.

Также определенные виды способны обеспечить высокую степень защиты от фальсификации при необходимости.

Последней нерассмотренной группой сканеров отпечатков пальцев являются ультразвуковые. В табл. 3 представлено сравнение потенциально применимых ультразвуковых сканеров отпечатков пальцев. [4,6]

Таблица 3

Сравнение ультразвуковых сканеров

Тип	Преимущества	Недостатки
Ультразвуковые сканеры	Наилучшее качество изображения	Высокая стоимость
	Полная защита от муляжей	

Данный класс сканеров при очевидных преимуществах перед остальными группами сканеров и сравнительно небольшими размерами, проигрывает, например, кремниевым в соотношении цена/целесообразность. Так как цена ультразвуковых сканеров ощутимо выше остальных, это приведет к значительному удорожанию продукта в целом, что противоречит выдвинутому ранее требованию о минимальном удорожании конечного продукта после встраивания сканера отпечатка пальцев.

Усовершенствованный процесс инициализации

Из приведенного выше анализа существующих на рынке разновидностей сканеров отпечатков пальцев можно выделить два основных потенциально применимых в разработке сканера: емкостный и радиочастотный.

Как ранее упоминалось, данные сканеры обладают малыми габаритами, что позволяет сохранить размеры стандартной карты и, если рассматривается вариант с радиочастотными сканерами, получить высокую степень защиты от фальсификации отпечатка пальцев.

Также в карте появляется дополнительный блок управления сканером отпечатка пальцев, который считывает отпечаток со сканера и на основе сформированных данных определяет успешность аутентификации пользователя и возможность дальнейшего общения карты со считывателем. В нем присутствует защищаемая от считывания и изменения область памяти, хранящая данные эталонного отпечатка пальцев, загруженные в неё при оформлении карты в присутствии будущего владельца.

При такой реализации процесс инициализации карты усложняется. Усовершенствованный процесс инициализации карты представлен на рис. 3

Теперь на запрос «Wake-up» (WUPA) запускается модуль управления сканером, который ожидает предоставление отпечатка. Пока сканеру не предоставлен легитимный отпечаток пальца, карта никак не реагирует и не отвечает на запросы, то есть находится в заблокированном режиме. Как только сканеру предъявляется валидный отпечаток, модуль управления разрешает передачу и процесс проходит в режиме, описанном ранее.

Преимуществами такой реализации являются:

1. Решение проблемы передачи карт третьим лицам, так как они не смогут ее разблокировать из-за нелегитимного отпечатка пальцев;
2. Невозможность считать данные карты снифферами, пока она не разблокирована модулем управления сканера, который в свою очередь ожидает предоставление валидного отпечатка пальца;
3. Полное сохранение существующей инфраструктуры, так как работа протоколов обмена данными не нарушается;
4. Универсальность подхода для большого числа существующих решений;
5. Получение по сути двухфакторной аутентификации пользователя с минимальными изменениями технической базы.

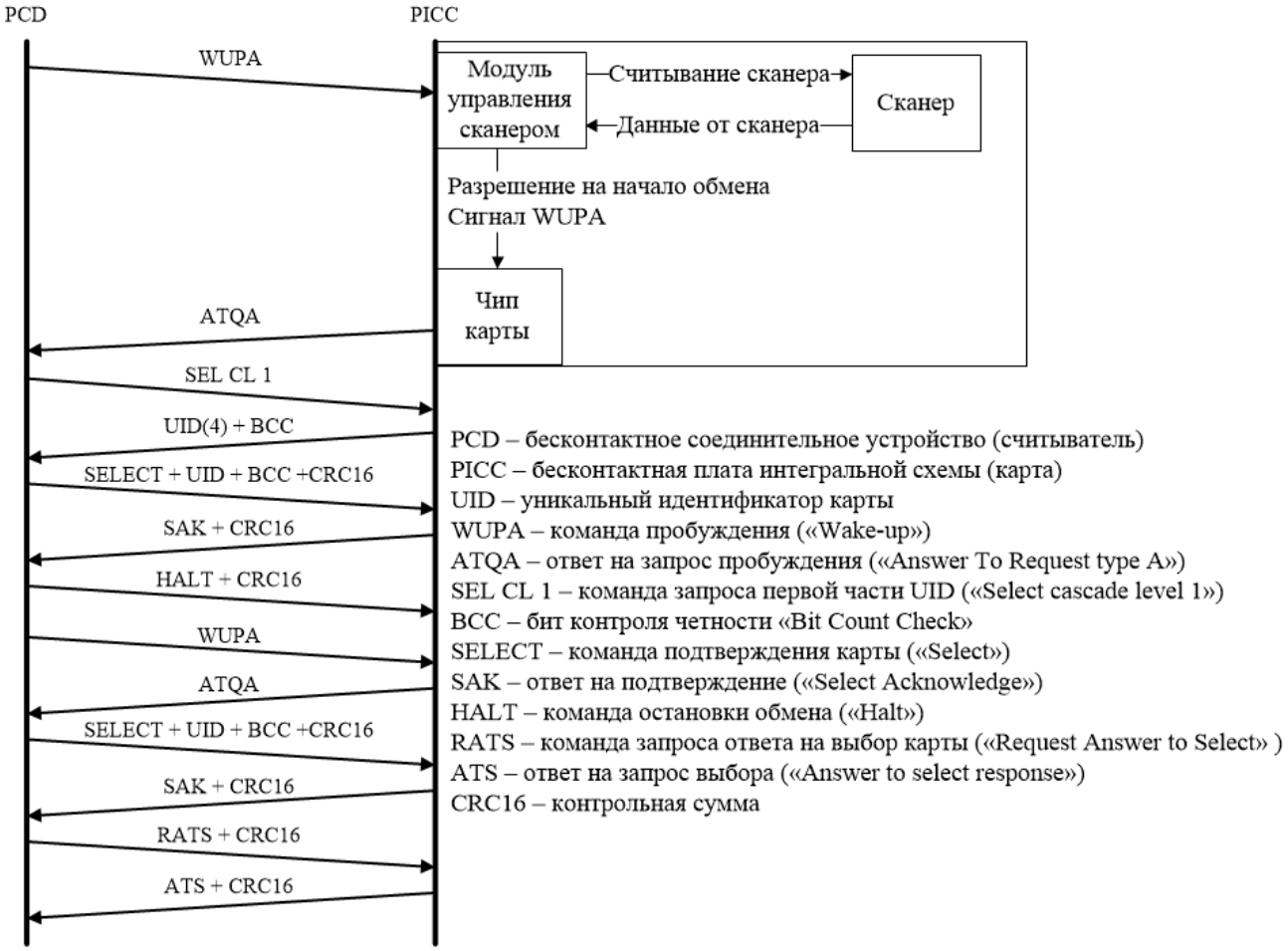

Рис. 3. Процесс инициализации карты

Сферы применения

Сферами применения данной разработки могут быть:

1. Системы контроля и управления доступом;
2. Средства доверенной загрузки;
3. Банковская сфера.

В первой сфере применения данная разработка позволит получить двухфакторную аутентификацию с полным сохранением существующей инфраструктуры предприятия.

Во второй сфере применения данная разработка позволит еще сильнее противостоять несанкционированному доступу к ЭВМ путем создания еще одного фактора проверки.

В третьей сфере применения данная разработка позволит осуществлять подтверждение транзакций не по PIN-коду, а по отпечатку пальцев, что позволяет исключить компрометацию PIN-кода в процессе его ввода.

Концепт изделия

Примерный вид разрабатываемой RFID-карты для банковской и остальных сфер применения представлен на рис. 4.

Рис. 4. Вид разрабатываемых карт

Заключение

Таким образом, данная разработка, – RFID-карты со сканером отпечатка пальцев – описанная в ходе данной статьи, удовлетворяет выдвинутым требованиям: обладает всеми преимуществами стандартных карт и не нарушает функционирование существующей инфраструктуры, так как полностью опирается на структуру исходника и никак не изменяет иерархию работы стека протоколов. И в тоже время решает проблемы передачи карты третьим лицам и её ретрансляции или копирования. Подход, предложенный в статье, также универсален, так как опирается на протокол, используемый большинством существующих продуктов, и незначительно удорожает производство изделия благодаря правильному выбору типа сканера отпечатка пальцев.

Как итог, данная разработка подойдет компаниям, желающим улучшить свою безопасность с минимальными изменениями существующей инфраструктуры, и клиентам в банковской сфере, желающим дополнительно обезопасить использование своих банковских карт.

Список литературы

1. ГОСТ Р ИСО/МЭК 14443-1-2013 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 1. Физические характеристики. [Текст], взамен ГОСТ Р ИСО/МЭК 14443-1-2004; Введен 2015-01-01. М.: Стандартинформ, 2014. 10 с.

2. ГОСТ Р ИСО/МЭК 14443-2-2014 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 2. Радиочастотный энергетический и сигнальный интерфейс. [Текст]; Введен 2016-01-01. М.: Стандартинформ, 2015. 31 с.

3. ГОСТ Р ИСО/МЭК 14443-3-2014 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 3. Инициализация и антиколлизия. [Текст]; Введен 2016-01-01. – М.: Стандартинформ, 2015. 61 с.

4. Задорожный В.В. Идентификация по отпечатку пальцев. Часть 1 / В.В. Задорожный // PC Magazine/Russian Edition. 2004, №1. С. 13-18.

5. Куренкова П.Ю. Способы выбора сканера отпечатков пальцев/ П.Ю. Куренкова // Безопасные информационные технологии (БИТ-2016), 2016. С. 167-170.

6. Болл Р.М. Руководство по биометрии / Р.М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э.У. Сеньор. М.: Техносфера, 2007. 368 с.

7. Шарапиев Д.С Возникновение NFC технологии и её потенциал для развития / К.О. Атаджанов, В.Н. Звягинцев, В.А. Клесов, П.Д. Полищук, // Наука и бизнес: пути развития, 2019. №9. С. 71-74.

8. Бельский В. Безопасность RFID-систем / В. Бельский, Е. Грибоедова, К. Царегородцев, А. Чичаева // International Journal of Open Information Technologies, 2021. Т. 9, № 9. С. 1-20.

9. Жовнер П. Как украсть деньги с бесконтактной карты и Apple Play // habr.com: URL: https://habr.com/ru/post/422551/ (дата обращения: 01.11. 2022).

10. Субхо Г., Гупта А. Беспроводная связь ближнего радиуса действия (Near Field Communication, NFC) // SecurityLab.ru: URL: https://www.securitylab.ru/analytics/438097.php (дата обращения: 01.11.2022)

Тамбовский государственный технический университет
Tambov State Technical University

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 10.11.2022

Информация об авторах

Громов Юрий Юрьевич – д-р техн. наук, профессор, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru

Пушкин Павел Юрьевич – канд. техн. наук, заведующий кафедрой, МИРЭА - Российский технологический университет, e-mail: pushkin@mirea.ru

Карасев Павел Игоревич – канд. техн. наук, МИРЭА - Российский технологический университет, e-mail: karasev@mirea.ru

Гладышев Максим Алексеевич – студент, МИРЭА – Российский технологический университет, e-mail: 0362725@mail.ru

IMPROVING THE RFID CARD INITIALIZATION PROCESS USING A SCANNED FINGERPRINT IMAGE

Y.Y. Gromov, P.Y. Pushkin, P.I. Karasev, M.A. Gladyshev

The paper proposes the development of an improved high-frequency RFID card (NFC card) with a fingerprint scanner. The NFC protocol stack for various existing implementations of this technology and the choice of a suitable place for the implementation of fingerprint scanner controls are described. The process of initialization of cards based on the GOST R ISO/IEC 14443-3-2014 protocol is described. A comparative analysis of existing types of fingerprint scanners is carried out and a search for an acceptable solution regarding its use in development according to the parameters of cost, the proper level of security and the size of the sensor itself. A new algorithm for initializing the card after the introduction of a fingerprint scanner into its composition is presented, as well as the advantages of this approach in solving the problems of transferring cards to third parties, retransmitting or copying to the expended funds. The potential areas of application of this development and the advantages of its implementation in relation to the standard are proposed.

Keywords: RFID card, NFC card, biometrics, fingerprint scanner, information security.

Submitted 10.11.2022

Information about the authors

Yurii Y. Gromov – Dr. Sc. (Technical), Professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru

Pavel Y. Pushkin – Cand. Sc. (Technical), Head of Department, MIREA – Russian Technological University, e-mail: pushkin@mirea.ru

Pavel I. Karasev – Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru

Maksim A. Gladyshev – student, MIREA – Russian Technological University, e-mail: 0362725@mail.ru