DOI: 10.17117/na.2015.10.03.297

Поступила (Received): 30.10.2015

<http://ucom.ru/doc/na.2015.10.03.297.pdf>**Ячный И.В.****Автоматизированные средства системы безналичных расчетов на основе бесконтактных карт MIFARE****Yachny I.V.****Automated means of cashless payment system based on contactless cards mifare**

В данной работе приведены основные типы бесконтактных пластиковых карт MIFARE, описаны основные зоны применения карт в повседневной жизни. Рассказывается о структуре карты. Также показаны перспективы развития бесконтактных карт MIFARE в системах безналичных расчетов

Ключевые слова: карта MIFARE, система безналичных расчетов, структура карты

In this work is shown the main types of contactless cards MIFARE, describes the main areas of using cards in daily life. The author tells about the structure of the card. Also shown are the prospects for the development of contactless MIFARE card in the clearing system

Key words: MIFARE card, clearing system, card structure

Ячный Иван Викторович

Инженер

Томский государственный университет систем управления и радиоэлектроники

г. Томск, пр. Ленина, 40

Yachny Ivan Victorovich

Engineer

Tomsk state university of control systems and radioelectronics

Tomsk, Lenina ave., 40

Бесконтактные пластиковые карты с каждым годом расширяют сферу своего применения. Благодаря современным микрочипам, встроенным в корпус, пластиковые карты могут хранить большое количество информации и использоваться в различных областях деятельности.

Для бесконтактных карт на сегодняшний день существуют два основных международных стандарта:

- ISO 14443 – описывает частотный диапазон, метод модуляции и протокол обмена бесконтактных карт ближнего радиуса действия (до 10 см) на магнитосвязанных индуктивностях;

- ISO 15693 – описывает частотный диапазон, метод модуляции и протокол обмена бесконтактных карт дальнего радиуса действия (более 10 см) на магнитосвязанных индуктивностях.

Среди многообразия предлагаемых видов бесконтактных карт, наиболее распространенными, надежными и удобными считаются бесконтактные карты технологии MIFARE, использующие стандарт ISO 14443.

Область применения этих карт может быть разнообразной:

- идентификация владельца карты в системах контроля доступа;
- использование карт для систем безналичного расчета.
- оплата за проезд в общественном транспорте;
- оплата парковки;
- система расчётов на территории учебного заведения.

На сегодняшний день существуют следующие виды микросхем для смарт-карт MIFARE:

MIFARE Ultralight;
MIFARE Ultralight C;
MIFARE Ultralight EV1;
MIFARE Classic 1K, MIFARE Classic 4K;
MIFARE Classic EV1 1K, MIFARE Classic EV1 4K;
MIFARE Plus 2K, MIFARE Plus 4K;
MIFARE DESFire EV1;
MIFARE DESFire EV2.

Основные преимущества радио-карт технологии MIFARE:

- высокая скорость обмена информацией между модулем карты и считывающим устройством;
- карты MIFARE обладают высоким уровнем защиты от взлома и подделок;
- бесконтактные карты MIFARE имеют широкий набор используемых функций и достаточно большой объем энергонезависимой памяти (до 4 Кбайт).

Бесконтактные MIFARE карты состоят из чипа и антенны. На рисунке 1 приведен вид и структура карты.

Рис. 1. Бесконтактная MIFARE карта

Бесконтактные карты MIFARE используют радиочастотный интерфейс, который обеспечивает взаимодействие карты и считывающего устройства на расстоянии до 10 см.

Рассмотрим структуру карты MIFARE, объемом памяти 1 Кбайт. Вся память карты поделена на 16 энергонезависимых, отдельных, одинаковых по размеру секторов. Каждый сектор разбит на 4 блока по 16 байт каждый. Каж-

дый третий блок сектора хранит в себе ключи аутентификации и правила доступа к сектору. Внутренняя структура карты приведена на рисунке 2.

Sector	Block	Byte Number within a Block																Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Key A				Access Bits				Key B								Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A				Access Bits				Key B								Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A				Access Bits				Key B								Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A				Access Bits				Key B								Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Рис. 2. Структура карты MIFARE

Нулевой сектор карты MIFARE отличается от всех остальных. Он содержит в себе служебную информацию, записываемую при производстве – уникальный неизменяемый 4-х или 7-и байтный серийный номер карты (зависит от типа карты) и данные производителя. Доступ к этому сектору открыт для чтения всегда, в то время как другие блоки требуют пароль аутентификации, в том числе и для чтения сектора. Бесконтактная карта MIFARE имеет встроенную криптографическую защиту данных. Для защиты данных используется лицензионный криптоалгоритм Crypto-1.

Использование бесконтактных карт технологии MIFARE в системах безналичного расчета является перспективным направлением развития данной области. Благодаря разбиению памяти карты на энергонезависимые отдельные сектора, на одной карте MIFARE могут находиться различные приложения (бонусные, дисконтные и др.). А уникальность серийного номера, встроенное шифрование данных, а также дорогостоящий и сложный механизм создания полного клона карты сводит к минимуму возможность ее подделки.