УДК: 004.056.53
PACS: 84.40.Ua, 84.90.+a
DOI: 10.24144/2415-8038.2018.44.165-174

В.В. ГУСТІ, Т.В. МАТЬОВКА
Ужгородський національний університет, вул. Волошина, 54, Ужгород, 88000, Україна,
e-mail: vlad.husty@gmail.com

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ДЛЯ ЗАХИСТУ RFID-МІТОК БАНКІВСЬКИХ БЕЗКОНТАКТНИХ ПЛАТІЖНИХ КАРТОК НА БАЗІ ТЕХНОЛОГІЙ PAYPASS (MASTERCARD) ТА PAYWAVE (VISA) ВІД НЕСАНКЦІОНОВАНОГО ЗЧИТУВАННЯ

На основі аналізу процесу проведення транзакції з безконтактною банківською платіжною карткою встановлено способи та момент можливого викрадення даних з RFID-міток з використанням саморобних RFID-рідерів. Розроблено програмно-апаратний комплекс на базі платформи Arduino UNOR3 для захисту RFID-міток банківських безконтактних платіжних карток на базі технологій PayPass (Mastercard) та PayWawe (Visa) від несанкціонованого зчитування.
Ключові слова: RFID, PayPass, PayWave, RFID-мітка, безконтактні платежі.

Вступ

На сьогодні радіочастотна ідентифікація (RFID) є технологією, що динамічно розвивається [1-5]. Це пов’язано з широким використанням різних безконтактних систем реєстрації об’єктів у комерційних та технологічних процесах. Не обійшлася без використання RFID і банківська система [6]. Поява банківських платіжних карток з технологією безконтактної оплати – це серйозний крок вперед. Але, на кожне нововведення з'являється людина, яка спробує зробити на ньому гроші. Як правило, це або бізнесмени, або шахраї. Через останніх прогрес може сприйматися досить негативно – люди просто бояться за свої гроші.

Безконтактні банківські платіжні картки – це по суті вже знайомі і звичні для людей шматочки пластику, з тією лише різницею, що в них вбудована антена для передачі інформації по радіоканалу (RFID-мітка), яка використовує радіоканал, щоб передавати повідомлення про платежі.

Найпоширенішими їх видами є VISA PayWave і Mastercard PayPass [7]. Відрізнити такі карти можна за відповідним символом у вигляді хвилі в кутку і назвою безконтактної технології поряд з логотипом платіжної системи. Для оплати покупки всього лише треба піднести таку карту до платіжного терміналу, оснащеного спеціальним радіоприймачем. І все – платіж здійснено. Ніяких вводів PIN-кодів і залишення «автографів».

Зловмисники мають можливість віддалено викрадають гроші з банківських карт, оснащених RFID чіпами, використовуючи саморобні безконтактні рідери, здатних сканувати такі банківські карти. По суті, хакери створили саморобні аналоги легальних безконтактних PoS-терміналів.

Відстань в 5-20 сантиметрів, здавалося б, невелика, навряд чи хакер зможе підібратися так близько. Але в натовпі або в громадському транспорті провернути подібний трюк цілком можливо. Людина може навіть не помітити «злодійства». Отримані дані шахраї наносять на карти-клони - для подальших операцій.

Незважаючи на захист технологій PayPass і PayWave, з таких карт можна витягти номер картки і дату закінчення терміну її обслуговування - цього деколи

буває досить для проведення транзакцій і виготовлення клону з магнітною смугою. Крім того, хакерам стає доступною історія операцій по карті, в тому числі точні суми і дати списань.

Методики експерименту

Для реалізації проекту були використані наступні складові: Arduino UNO R3; RFID-модуль RC522; картка з RFID-чіпом; макетна плата на 400 точок; набір макетних проводів; RFID-модуль з підвищеним радіусом дії; банківська платіжна картка з підтримкою безконтактних платежів.

Ардуіно і Ардуіно-сумісні плати [8] спроектовані таким чином, щоб їх можна було при необхідності розширювати, додаючи в пристрій нові компоненти («shields»). Ці плати розширень підключаються до Ардуіно за допомогою встановлених на них штирових роз'ємів. Існує ряд уніфікованих плат, що допускає конструктивно жорстке з'єднання процесорної плати та плат розширення в стопку через штирові лінійки [9]. Крім того, випускаються плати зі зменшеним (наприклад, Nano, Lilypad) і спеціальним (для задач робототехніки) форм-фактором.

У концепцію Ардуіно не входять корпусні і монтажні деталі. Розробник вибирає метод установки і механічного захисту процесорних плат та компонентів розширення самостійно.

Нами використовувався RFID-модуль RC522 з частотою 13.56 МГц з SPI-інтерфейсом, оскільки такий модуль може бути використаний для різних радіоаматорських та комерційних застосувань, в тому числі контролю доступу, автоматичної ідентифікації, робототехніки, відстеження речей, платіжних систем і т.д [10]. Його основними характеристиками є: напруга живлення: 3.3V; струм: 13-26mA; робоча частота: 13.56MHz; дальність зчитування: 0 ~ 60 мм; Інтерфейс: SPI, максимальна швидкість передачі 10Мбіт/с; розмір: 40мм x 60мм; читання і запис RFID-міток.

Програма для роботи апаратної частини була написана в середовищі розробки для Arduino – ArduinoIDE. Як мова програмування за замовчуванням для платформи Arduino є мова програмування C^{++}.

Результати

Для початку роботи було зібрано апаратну частину на базі платформи Arduino Uno за схемою, як показано на рис.1.

Написано програму для зчитування даних з RFID-карток (Додаток 1).

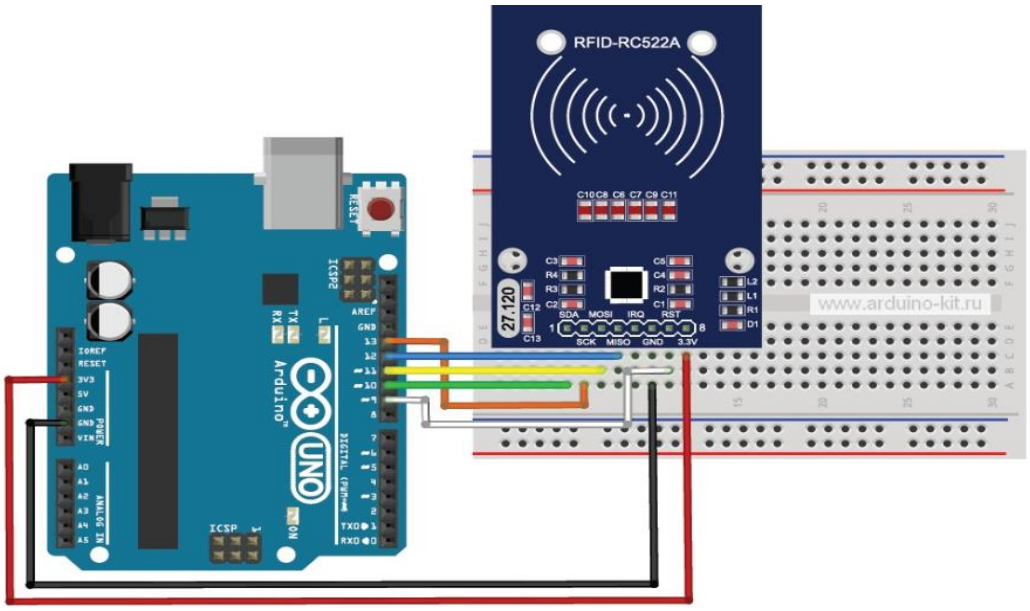

Рис.1. - Схема підключення RFID-модулю до плати ArduinoUNOR3.

В результаті роботи даного RFID-рідера стає можливим зчитати HEX-код безконтактної картки в якому міститься інформація номеру картки, CVV та терміну дії. При її розшифруванні ці дані можна записати на пусту картку, створивши дублікат, що і роблять шахраї. RFID-мітка зберігає свої дані в 16 секторах, кожен з яких складається з 4 блоків, а в свою чергу, кожен блок містить 16 байт даних [11]. Вигляд зчитаних даних показано на рис. 2.

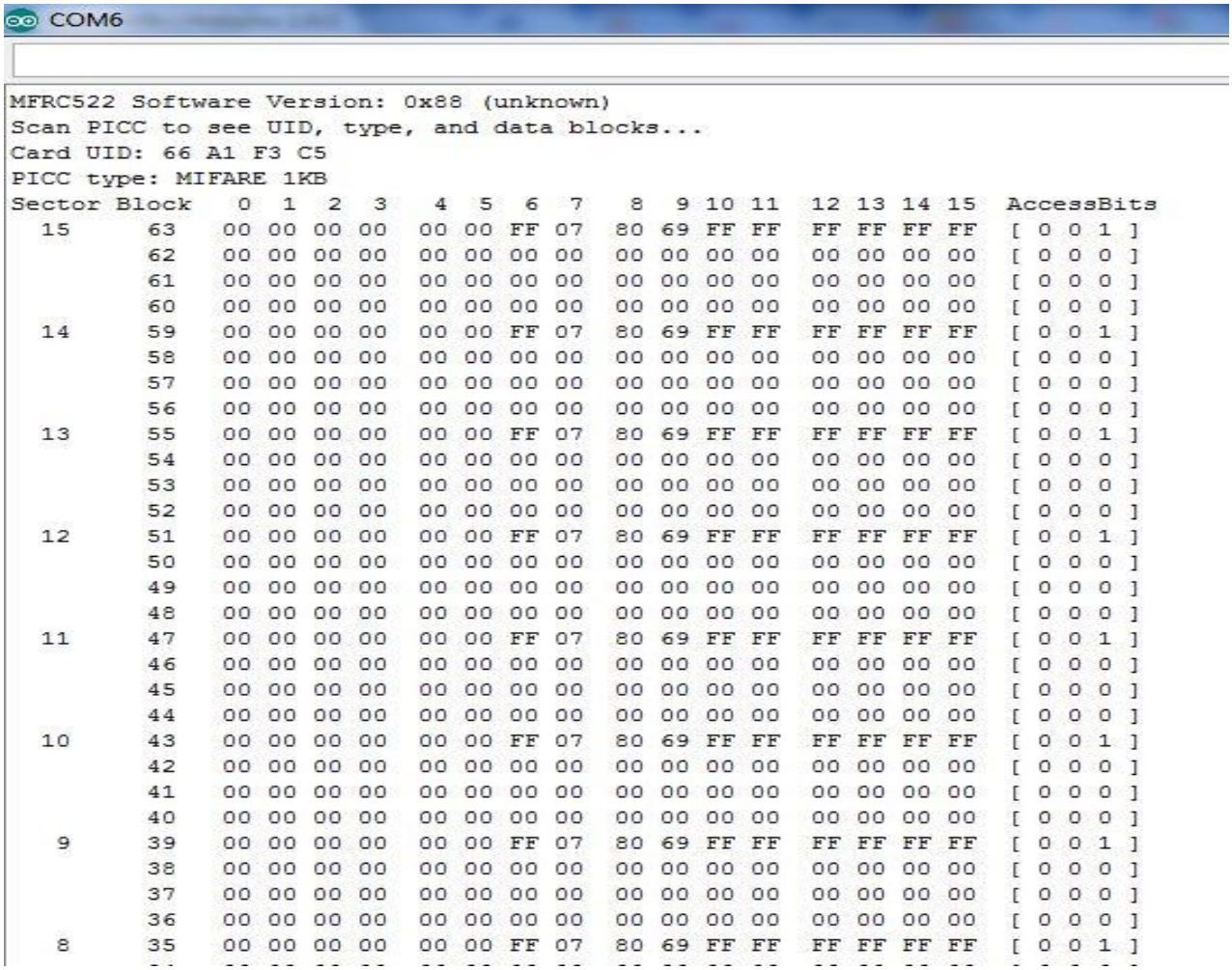

Рис. 2. – Зчитаний HEXкод RFID-мітки.

Для цього нам потрібно ще одну програму, за допомогою якої ми будемо записувати дану інформацію на пусту картку (Додаток 2).

Розробка картки із функцією блокування несанкціонованого зчитування даних безконтактних карток. Проаналізувавши вразливість банківських платіжних карток для безконтактних платежів та основні способи використання даних вразливостей зловмисниками було прийнято рішення розробити картку із функцією блокування несанкціонованого зчитування даних з RFID-міток. Прототип даної картки не відрізняється фізичними параметрами від захищеної картки, одною відмінністю є його товщина, яка в 1.5 разів більша в порівнянні із звичайною банківською платіжною карткою.

Принцип роботи прототипу полягає в тому, що завдяки посиленій антені та RFID-мітці, яка працює на частоті 13.56 МГц (на такій же частоті працюють RFID-мітки банківських платіжних карток) [12], вона перехоплює сигнал від рідера, який направлений на зчитування RFID-мітки банківської картки, чим блокує зчитування останньої.

Прототип виконує роль бар’єру для всіх карток в радіусі 14 см. (рис. 4).

COM6

```
Scan a MIFARE Classic PICC to demonstrate read and write.
Using key (for A and B): FF FF FF FF FF FF
BEWARE: Data will be written to the PICC, in sector #1
Card UID: 66 A1 F3 C5
PICC type: MIFARE 1KB
Authenticating using key A...
Current data in sector:
   1      7   00 00 00 00  00 00 19 67  8E 00 00 00  00 00 00 00  [ 0 1 1 ]
          6   EC FF FF FF  13 00 00 00  EC FF FF FF  06 F9 06 F9  [ 1 1 0 ]  Value=0xFFFFFFEC Adr=0x6
          5   02 00 00 00  FD FF FF FF  02 00 00 00  05 FA 05 FA  [ 1 1 0 ]  Value=0x2 Adr=0x5
          4   01 01 01 01  01 01 01 01  08 09 FF 0B  0C 0D 0E 0F  [ 0 0 0 ]

Reading data from block 4 ...
Data in block 4:
 01 01 01 01 01 01 01 01 08 09 FF 0B 0C 0D 0E 0F

Authenticating again using key B...
Writing data into block 4 ...
 01 02 03 04 05 06 07 08 08 09 FF 0B 0C 0D 0E 0F

Reading data from block 4 ...
Data in block 4:
 01 02 03 04 05 06 07 08 08 09 FF 0B 0C 0D 0E 0F
Checking result...
Number of bytes that match = 16
Success :-)

Current data in sector:
   1      7   00 00 00 00  00 00 19 67  8E 00 00 00  00 00 00 00  [ 0 1 1 ]
          6   EC FF FF FF  13 00 00 00  EC FF FF FF  06 F9 06 F9  [ 1 1 0 ]  Value=0xFFFFFFEC Adr=0x6
          5   02 00 00 00  FD FF FF FF  02 00 00 00  05 FA 05 FA  [ 1 1 0 ]  Value=0x2 Adr=0x5
```

Рис. 3. – Процес запису даних на RFID-мітку.

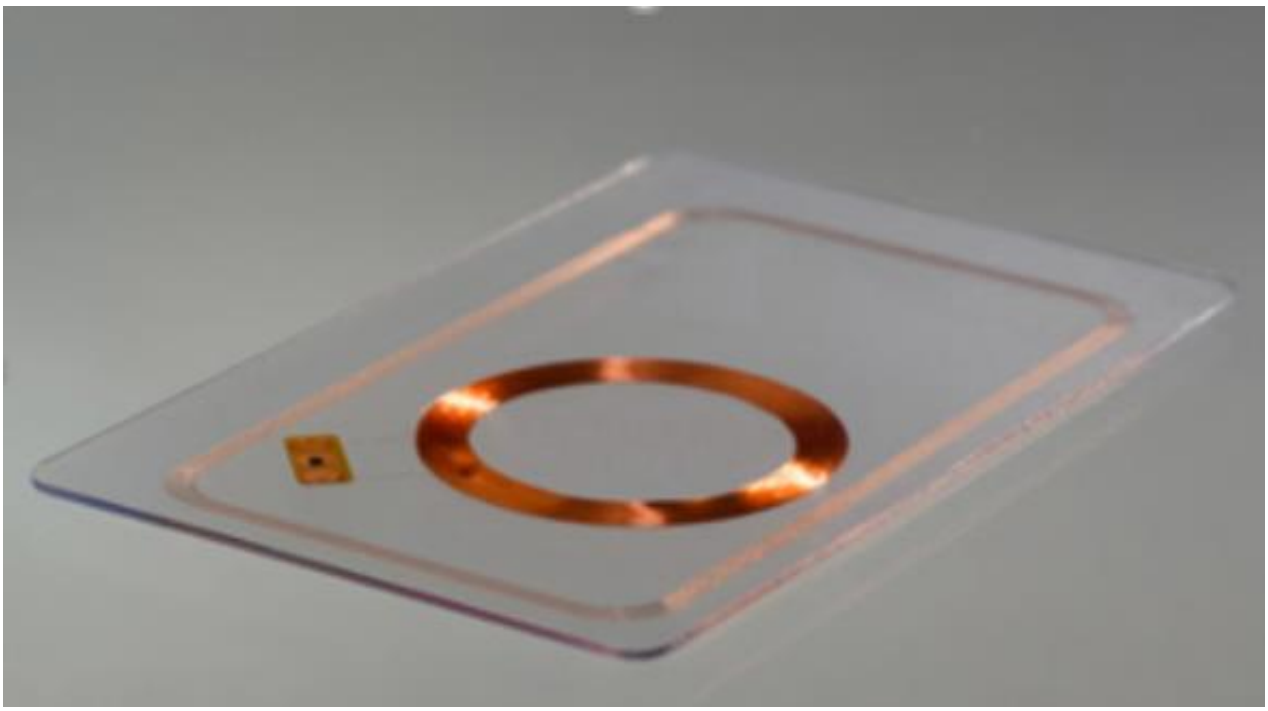

Рис. 4. – Прототип картки з посиленою антеною RFID-мітки.

Протестувавши процес проведення транзакції з банківською безконтактною платіжною карткою на програмно-апаратному комплексі на базі платформи Arduino UNO R3 з наявністю прототипу картки з посиленою антеною RFID-мітки та без нього, було встановлено ефективність роботи прототипу, який унеможливив процес несанкціонованого зчитування даних з RFID-мітки банківської безконтактної платіжної картки.

Висновки

Визначено основні загрози коректної роботи і шляхи несанкціонованого доступу до даних RFID-міток, а також методи захисту конфіденційності даних RFID-міток банківських платіжних карток на базі технології Visa Pay Wave та Mastercard Pay Pass.

Спроектовано та розроблено програмно-апаратний комплекс на базі ArduinoUnoR3 для демонстрації процесу отримання даних з RFID-міток.

Створено прототип картки з посиленою антеною RFID-мітки, наявність якої дає змогу убезпечити себе від викрадення коштів з банківських платіжних карток на базі технологій Visa Pay Wave та Mastercard Pay Pass.

Встановлено ефективність даного способу захисту на основі результатів тестування зчитування інформації з RFID-міток при наявності поруч прототипу картки з посиленою антеною RFID-мітки та за його відсутності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Agren, M., Hell, M., Johansson, T.: On hardware-oriented message authentication with applications towards RFID. In: Proceedings of International Workshop on Lightweight Security & Privacy (LightSec) (2011).
2. Das, M.L.: Strong security and privacy of RFID system for internet of things infrastructure. In: Security, Privacy, and Applied Cryptography Engineering, pp. 56–69. Springer, Berlin (2013).
3. Deng, H., Varanasi, M., Swigger, K., Garcia, O., Ogan, R., Kougianos, E.: Design of sensorembedded radio frequency identification (SE-RFID) systems. In: Proceedings of International Conference on Mechatronics and Automation (2006).
4. Mitrokotsa, A., Douligeris, C.: Integrated RFID and sensor networks: architectures and applications. RFID and sensor networks: architectures, protocols, security and integrations, pp. 511–535 (2009).
5. Nie, X., Zhong, X.: Security in the internet of things based on RFID: issues and current countermeasures. In: Proceedings of 2nd International Conference on Computer Science and Electronics.
6. Ruzzelli, A.G., Jurdak, R., O'Hare, G.M.P.: On the RFID wake-up impulse for multi-hop sensor networks. In: Proceedings of 1st ACM Workshop on Convergence of RFID and Wireless Sensor Networks and their Applications (SenseID) at the 5th ACM International Conference on Embedded Networked Sensor Systems [ACM SenSys 2007] (2007).
7. Sample, A.P., Yeager, D.J., Powledge, P.S., Smith, J.R.: Design of a passively-powered, programmable sensing platform for UHF RFID systems. In: Proceedings of IEEE International Conference on RFID, pp. 149–156 (2007).
8. Austin Lloyd J. Joint Publication (JP) 3-09 Joint Fire Support / Lloyd J. Austin. – United States of America, 2010. – III-20 p.
9. Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд. – М., 2006. – 197 с.
10. Стандарты и тенденции развития RFID-технологий [Електронний ресурс] // Компоненты и технологии. – 2008. – №1. – Режим доступу до журн.: http://www.kite.ru/assets/files/pdf/2006_01_108.pdf – Назва з екрану.

11. Hunt Daniel. A guide to radio frequency identification / Daniel Hunt, Mike Puglia, Albert Puglia. – WILEYINTERSCIENCE. – 2007. – С. 11-12 Research Trends in RFID Technology [Електроннийресурс] // Interdisciplinary Journal. – 2007. – №1. – С.68–82. – Режим доступу до журн.: http://www.lonworks.org.cn/en/RFID/RFIDResearchTrends.pdf.
12. Рынок RFID демонстрирует непрерывный рост [Електронний ресурс] // РСТ-Инвент. – 2013. – С. 1–2 – Режим доступу до журн.: http://www.rst-invent.ru/rfid-news/news/60/ – Назва з екрану.

Стаття надійшла до редакції 17.07.2018.

В.В. ГУСТИ, Т.В. МАТЁВКА
Ужгородский национальний университет, ул. Волошина, 54, Ужгород, 88000, Украина,
e-mail: vlad.husty@gmail.com

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ЗАЩИТЫ RFID-МЕТОК БАНКОВСКИХ БЕСКОНТАКТНЫХ ПЛАТЕЖНЫХ КАРТОЧЕК НА БАЗЕ ТЕХНОЛОГИЙ PAYPASS (MASTERCARD) И PAYWAVE (VISA) ОТ НЕСАНКЦИОНИРОВАННОГО ЧТЕНИЯ

На основе анализа процесса проведения транзакции с бесконтактной банковской платежной карточкой установлены способы и момент возможного похищения данных с RFID-меток с использованием самодельных RFID-ридеров. Разработан программно-аппаратный комплекс на базе платформы Arduino UNOR3 для защиты RFID-меток банковских бесконтактных платежных карт на базе технологий PayPass (Mastercard) и PayWawe (Visa) от несанкционированного считывания.
Ключевые слова: RFID, PayPass, PayWave, RFID-метка, бесконтактные платежи.

V.V. HUSTI, T.V. MATYOVKA
Uzhhorod National University, Voloshyna str., 54, Uzhhorod, 88000, Ukraine,
e-mail: vlad.husty@gmail.com

SOFTWARE COMPLEX FOR PROTECTION OF RFID-TAG OF BANK CONTACTLESS PAYMENT CARD BASED ON PAYPASS (MASTERCARD) AND PAYWAVE (VISA) TECHNOLOGIES FROM UNPRECATED READING

Purpose. Develop protection against unauthorized reading of bank contactless payment cards based on PayPass (Mastercard) and PayWave (Visa) technologies.
Methods. The following components were used to implement the project: Arduino UNO R3; RFID module RC522; RFID chip card; model board for 400 points; set of model wires; RFID-module with increased radius of action; Bank payment card with support of contactless payments. These extension boards are connected to Arduino using their pin connectors mounted on them. There is a number of unified motherboards, which allows a constructively rigid connection of the processor board and expansion cards in a stack through the pin rods. In addition, boards with reduced and special form factors are issued. We used the RC522 RFID module with a

frequency of 13.56 MHz with an SPI interface, since such a module can be used for various radio amateur and commercial applications, including access control, automatic identification, robotics, speech tracking, payment systems, etc.
Results. Based on the analysis of the process of conducting a transaction with a contactless bank payment card, the methods and the moment of possible theft of data from RFID tags with the use of homemade RFID readers are established. The software-hardware complex on the basis of the Arduino UNOR3 platform was developed to protect the RFID tags of bank contactless payment cards based on PayPass (Mastercard) and PayWawe (Visa) technologies from unauthorized reading.
Conclusions. The main threats of correct operation and ways of unauthorized access to RFID-labeled data are determined, as well as methods for protecting the confidentiality of RFID-tags of bank payment card. The ArduinoUnoR3 software-hardware complex was designed and developed to demonstrate the process of obtaining data from RFID tags. A prototype card with RFID tagged antenna has been created, which allows it to protect itself against the theft of bank payment cards. The effectiveness of this method of protection has been established based on the results of testing the reading of information from the RFID tags in the presence of a nearby prototype of the card with a reinforced RFID tag antenna and in its absence.
Keywords: RFID, PayPass, PayWave, RFID tag, contactless payments.
PACS: 84.40.Ua, 84.90.+a

REFERENCES

1. Agren, M., Hell, M., Johansson, T .: On the hardware-oriented message authentication with applications towards RFID. In: Proceedings of International Workshop on Lightweight Security & Security (LightSec) (2011).
2. Das, M.L .: Strong security system. In: Security, Privacy, and Applied Cryptography Engineering, pp. 56–69. Springer, Berlin (2013).
3. Deng, H., Varanasi, M., Swigger, K., Garcia, O., Ogan, R., Kougianos, E .: Design of sensorembedded radio frequency identification (SE-RFID) systems. In: Proceedings of International Conference on Mechatronics and Automation (2006).
4. Mitrokotsa, A., Douligeris, S .: Integrated RFID and sensor networks: architectures and applications. RFID and sensor networks: architectures, protocols, security and integrations, pp. 511–535 (2009).
5. Nie, X., Zhong, X .: Security issues and current countermeasures.
6. Ruzzelli, A.G., Jurdak, R., O'Hare, G.M.P .: On the RFID wake-up impulse for multi-hop sensor networks. ACM Workshop on the ACM Workshop on the ACM International Conference on Embedded Networked Systems [ACM SenSys 2007] (2007).
7. Sample, A.P., Yeager, D.J., Powledge, P.S., Smith, J.R .: UHF RFID systems, programmable sensing platform for passively-powered, programmable sensing platform. In: Proceedings of the IEEE International Conference on RFID, pp. 149–156 (2007).
8. Austin Lloyd J. Joint Publication (JP) 3-09 Joint Fire Support / Lloyd J. Austin. - United States of America, 2010.
9. Sharfeld T. Low cost RFID systems / T. Sharfeld. - M., 2006. - 197 p.
10. Standards and trends in the development of RFID technologies [Electronic resource] // Components and technologies. - 2008. - №1. - Mode of access to the journal: http://www.kite.ru/assets/files/pdf/2006_01_108.pdf.
11. HuntDaniel. A guide to radio frequency identification / Daniel Hunt, Mike Puglia, Albert Puglia.- WILEYINTER SCIENCE. - 2007. - P. 11-12 5. Overview of the systems of radio frequency identification components and their use [Electronic resource] // Chip News Ukraine. - 2005. - №1 (41). - pp. 76–87.
12. Research Trends in RFID Technology [Electronic Resource] // Interdisciplinary Journal. - 2007. - №1. - P.68-82. - Mode of access to the journal: http://www.lonworks.org.cn/en/RFID/RFIDResearchTrends.pdf.

ДОДАТКИ

Додаток 1. Скетч для зчитування даних RFID

```
#include <SPI.h>
#include <MFRC522.h>
#define RST_PIN 9
#define SS_PIN 10
MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance.
MFRC522:MIFARE_Key key;
byte sector = 1;
byte blockAddr = 4;
byte dataBlock[] = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};
byte trailerBlock = 7;
byte status;
byte buffer[18];
byte size = sizeof(buffer);
void setup()
{
Serial.begin(9600);
SPI.begin();mfrc522.PCD_Init()
for (byte i = 0; i < 6; i++)
key.keyByte[i] = 0xFF;
}
void loop()
{
if ( ! mfrc522.PICC_IsNewCardPresent())
return;
if ( ! mfrc522.PICC_ReadCardSerial())
return;
Serial.print(F("Card UID:"));
dump_byte_array(mfrc522.uid.uidByte, mfrc522.uid.size);
Serial.println();
Serial.print(F("PICC type: "));
byte piccType = mfrc522.PICC_GetType(mfrc522.uid.sak);
Serial.println(mfrc522.PICC_GetTypeName(piccType));
Serial.print(F("Reading data from block "));
Serial.print(blockAddr);
Serial.println(F(" ..."));
Serial.print(F("Data for count ")); Serial.print(blockAddr);
Serial.println(F(":"));
dump_byte_array(buffer, 2); Serial.println();
```

```
Serial.println();
for (byte i = 0; i < 16; i++) // запись в buffer[]
dataBlock[i]=buffer[i];
int count1=(buffer[0]<<8)+buffer[1];
Serial.print("count1=");Serial.println(count1);
count1=count1+1; // инкремент счетчика
dataBlock[0]=highByte(count1);
dataBlock[1]=lowByte(count1);
Serial.println(F("Authenticating again using key B..."));
Serial.print(F("Writing data into block "));
Serial.print(blockAddr);
Serial.println(F(" ..."));
dump_byte_array(dataBlock, 2); Serial.println();
}
void dump_byte_array(byte *buffer, byte bufferSize)
{
for (byte i = 0; i < bufferSize; i++)
{
Serial.print(buffer[i] < 0x10 ? " 0" : " ");
Serial.print(buffer[i], HEX);}}
```

Додаток 2. Скетч для запису даних на RFID

```
#include
#include
#define NEW_UID {0xDE, 0xAD, 0xBE, 0xEF}
#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);
MFRC522::MIFARE_Key key;
void setup() {
	Serial.begin(9600);
	while (!Serial);
	SPI.begin();
	mfrc522.PCD_Init();
	for (byte i = 0; i < 6; i++) {
		key.keyByte[i] = 0xFF;
	}
}
void loop() {
	if ( ! mfrc522.PICC_IsNewCardPresent() || ! mfrc522.PICC_ReadCardSerial() ) {
	  delay(50);
	  return;
	}
	Serial.print(F("Card UID:"));
	for (byte i = 0; i < mfrc522.uid.size; i++) {
		Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
		Serial.print(mfrc522.uid.uidByte[i], HEX);
	}
	Serial.println();
	byte newUid[] = NEW_UID;
	if ( mfrc522.MIFARE_SetUid(newUid, (byte)4, true) ) {
	  Serial.println(F("Wrote new UID to card."));
	}
		mfrc522.PICC_HaltA();
	if ( ! mfrc522.PICC_IsNewCardPresent() || ! mfrc522.PICC_ReadCardSerial() ) {
		return;
	}

	Serial.println(F("New UID and contents:"));
	mfrc522.PICC_DumpToSerial(&(mfrc522.uid));
	delay(2000);
}
```