**УДК 665.3**

# ЗАХИСТ СИСТЕМ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ ЗА ДОПОМОГОЮ ІМПЕДАНСУ

В.Б. Дудикевич, І.С. Собчук, Л.М. Ракобовчук, П.І. Гаранюк, І.П.Гаранюк

*1. Національний університет "Львівська політехніка", УКРАЇНА, м. Львів, вул. С.Бандери, 12*

*В статті розглянуто можливість використання імпедансу для захисту RFID–карток від несанкціонованого зчитування інформації. Проведено аналіз літературних джерел з проблеми захисту RFID-систем, а також проведено дослідження імпедансу RFID-міток та її елементів в частотному діапазоні 50-250кГц. Показані імпедансні спектри RFID–тегів, чіпів та антен для різних карток.*

***Ключові слова –*** *RFID, безконтактна радіочастотна ідентифікація, RFID-технологія, RFID-мітки, теги, чіп, анетна(контур), імпеданс, комплексний опір, імпедансні спектри, залежність імпедансу від температури.*

**Постановка проблеми.** RFID (Radio Frequency Identification – радіочастотна ідентифікація) – це технологія безконтактної автоматичної ідентифікації об'єктів за допомогою радіочастотного каналу зв'язку. За своїми функціональними можливостями RFID-технологія дуже близька до використовуваної в даний час технології штрих - кодів. Поряд з цим дана технологія має суттєві переваги [1]. **У** наш час безконтактні ключі стали витісняти з світового ринку контактні, оскільки вони набагато дешевші і простіші у виробництві. Картки доступу, на базі безконтактних ключів, працюють за принципом RFID-технологій. Безконтактні картки, які працюють на частотах 120-200 кГц (технологія EM-Marine) знайшли широке застосування в Україні. Їх основними перевагами є можливість персоналізації і відносно низька вартість порівняно з іншими безконтактними картками (MIFARE, HID).

Але система захисту безконтактних карт сьогодні є недостатньою. Для несанкціонованого зчитування конфіденційної інформації з банківської карти, оснащеної радіочіпом RFID, використовується недороге обладнання загальною вартістю декілька сотень доларів[2]. Окрім зчитування існують інші види атак на RFID-мітки[3,4].

**Аналіз останніх досліджень та публікацій.** Здебільшого активні мітки надійніші і забезпечують найвищу точність зчитування на максимальній відстані [5]. Пасивні RFID-мітки мають практично необмежений термін експлуатації. RFID-мітка може використовуватися для виконання інших завдань, крім функції носія даних [6].

Різні типи карток є вразливими для зчитування інформації. Механізми безпеки RFID-картки є недостатніми. Зокрема, для поширених карток MIFARE Classic виявлені слабкі місця в механізмі автентифікації [7-9]. Група Digital Security виявила серйозний недолік безпеки алгоритму шифрування CRYPTO1 для безконтактних смарт-карток MIFARE Classic [10]. Можливість використання портативних пристроїв зчитування для клонування RFID-картки досліджено в роботах [11-13].

Протягом останніх років активно проводились дослідження безпеки криптографічних механізмів 64-бітніх ключів, що використовуються в поширених безконтактних смарт-картах – iClass[14] та Hitag2[15]. Дослідження карток CryptoRF, які використовуються в системах контролю доступу та платіжних системах, показало, що вони мають підвищену, але недостатню безпеку, продуктивність та цілісність даних[16,17].

**Мета статті** – дослідження можливості використання імпедансних властивостей RFID–карток для підвищення захищеності від несанкціонованого зчитування інформації.

**Вразливості RFID - систем.**

Порушення нормальної роботи системи. Для цього використовується метод, що нагадує DoS-атаку: в навколишньому середовищі створюється маса сигналів, які імітують сигнали міток. RFID-зчитувачі першого покоління, тобто пасивні, не мають можливості зчитувати дані з карти. Нові інтерактивні зчитувачі, як показали досліди, також не можуть нормально працювати.

Несанкціоноване отримання інформації. Як правило, інформація, яка зберігається в RFID–картах є приватною. Це можуть бути паролі користувача, номери кредитних карт, біометричні дані (нові паспорти зберігають біометричну інформацію про власника) та багато іншого. Виробники використовують різні методи захисту даних, які базуються на відомих методах шифрування і аутентифікації. Але інформація з RFID-картки може бути зчитана без дозволу власника. Існує серйозна проблема в тому що RFID-мітки мають обмежені ресурси, які не дають можливості реалізувати об'ємні за ресурсами механізми захисту.

Незаконне відстеження місця розташування. У багатьох випадках RFID-мітки використовуються з метою визначення місця розташування об'єкта в просторі. Це може бути актуальним при доставці ліків або при відстеженні місця розташування домашньої тварини. Але існує більша небезпека - несанкціоноване стеження за місцеположенням людини або важливого носія інформації.

Клонування. Клонування мітки є однією з найпоширеніших атак на RFID-мітки. Це означає, що в областях застосування RFID-технології можуть почастішати випадки шахрайства. Виробники карт впроваджують заходи для захисту від клонування, таких як, наприклад унікальний ID для кожної карти, застосування ключів доступу, що залежать від унікальних параметрів карти, застосування шифрування. Однак, на практиці, існує велика кількість способів обходу цих методів захисту.

Proxmark дозволяє перехоплювати потік даних між зчитувачем та картою. За допомогою proxmark'а, який має компактні розміри, зловмисник може не-

помітно клонувати proximity-карту. Модифікований proxmark вміє працювати з більшістю 125KHz і деякими 13,56MHz RFID-мітками, а також клонувати VeriChip, який вважається виробниками найбільш надійним[18].

Перехоплення сигналу. Ще однією небезпекою використання технології RFID є можливість перехоплення сигналу від RFID-мітки до приймача RFID з подальшим повтором даного сигналу. Таким чином зловмисник може змінити дані, які зберігаються на карті (наприклад, збільшити свій банківський баланс). Такі перехоплення можуть, як наслідок, привести до численних випадків шахрайства.

Як правило карти мають вбудовані механізми розмежування прав доступу до даних, які реалізуються методами шифрування і аутентифікації. Але RFID-мітки мають обмежені ресурсів, що не дозволяє застосувати більш захищені системи шифрування.

Відмова в обслуговуванні. Здійснити атаку - відмови в доступі можна не тільки стандартними методами, перевантаженням мережі, але і специфічними для даної технології способами, як, наприклад, перехопленням сигналів, наведенням перешкод. Наслідки такої атаки можуть бути серйозними[18].

**Дослідження імпедансних спектрів елементів RFID – систем.**

При нормальній роботі зчитувачі безконтактних карт створюють магнітне поле. Коли RFID–тег попадає в поле дії цього випромінювання, то в ньому виникає індукційний струм, який необхідний для генерування сигналу (коду) в мікропроцесорі, після чого він передається через антену (обмотку) на зчитувач. Цей сигнал складається з 16 частин по 4 біти в кожній, в яких розміщена інформація про власника картки і його персональний ідентифікатор. Для зловмисника отримати доступ до таких карт не складає великих проблем. Отримати доступ до картки буде проблематично, якщо рідер буде доповнений імеданснім зчитувачем. Тобто отримати доступ до картки буде неможливо навіть за наявності оригінального ключа, якщо немає імеданснього. Мікропроцесор зчитувача програмується таким чином, що сигнал зчитування, буде доступним після того, як мікропроцесор обробить інформацію про імпеданс.

Нами проведені дослідження імпедансних властивостей тегів, чіпів та антен безконтактних карток в різних температурних режимах, оскільки вони в реальних умовах, працюють при різних температурах.

Експеримент проводився в лабораторних умовах, тобто для експерименту були підготовлено RFID-мітки, контури та чіпи. Для підтримування сталої температури був створений спеціальний контейнер, який працює за принципом термосумки. Експеримент проводився в трьох температурних режимах: при 0, 10, а також при 23°C. Картки поміщалися в контейнер, в якому через отвір виводились контакти, до яких під'єднували щупи універсального імпедансного спектрометра. Протягом 15хв пристрій зчитував всю інформацію з мітки, після чого видавав результат.

На рис.1-3 подані результати вимірювання(точки) та апроксимовані криві імпедансу RFID–мітки та її елементів при різних температурах. При збільшені

температури збільшується комплексний опір RFID–мітки. Максимальний опір спостерігається в межах 110-145 кГц для температури - 0°С, 115-140 кГц для температури - 10°С та 120-140 кГц для температури - 23°С.

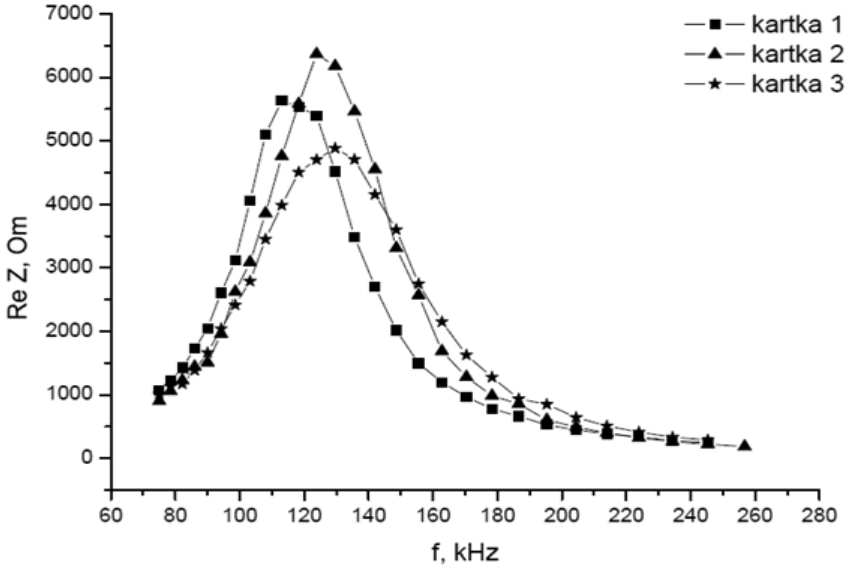


Рис 1. Експериментальні імпедансні спектри тегів(мітки) за температури 0° С

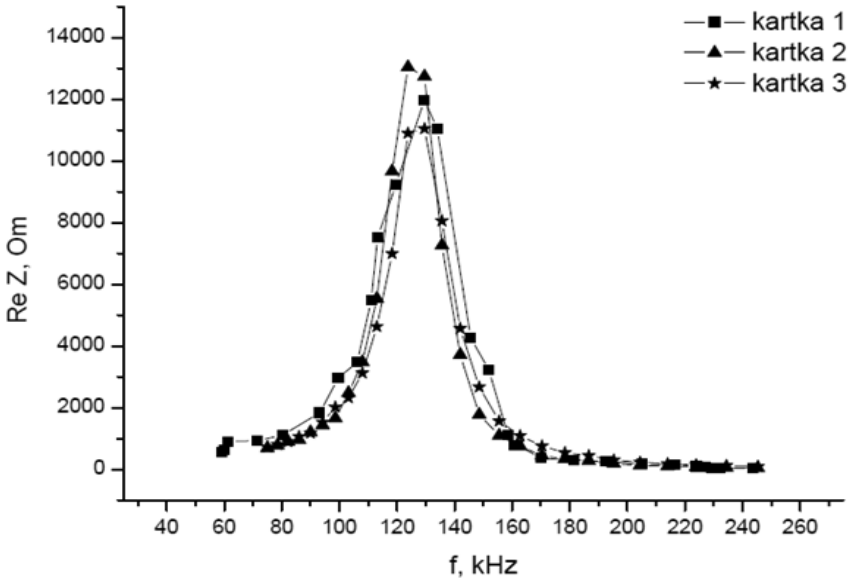


Рис 2. Експериментальні імпедансні спектри тегів(мітки) температури 10° С

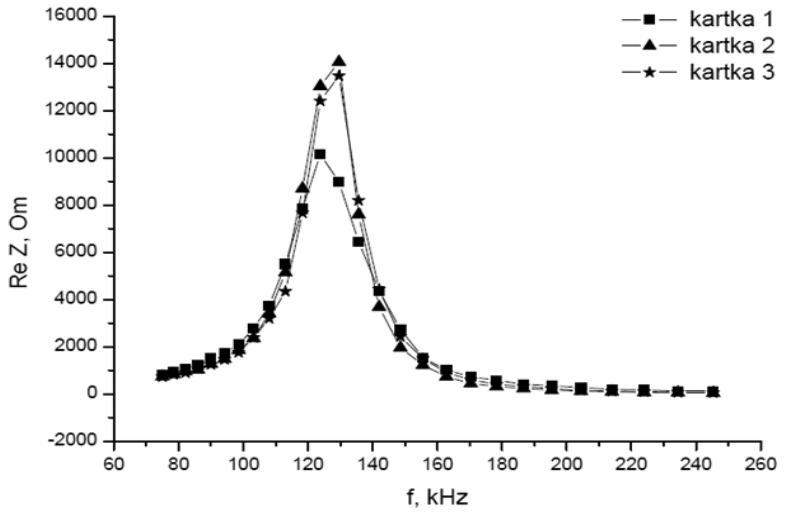


Рис 3. Експериментальні імпедансні спектри тегів(мітки) за температури 23° С

На рис.4. показані експериментальні(точки) та апроксимовані залежності комплексного опору від частоти досліджуваного чіпа при температурі 0° С, 10° С, та 23° С. Максимальне збільшення імпедансу в діапазоні частот від 50 до 135 кГц є спробами чіпа корекції побічних гармонік, на яких збуджується котушка, тобто чіп збільшує свій комплексний опір для придушення цих гармонік. Мінімальні значення імпедансу на графіку відповідають частоті бажаного резонансу антени. Зсув графіка по осі частот є наслідком корекції системи функції залежності частоти резонансу антени від температури навколишнього середовища.

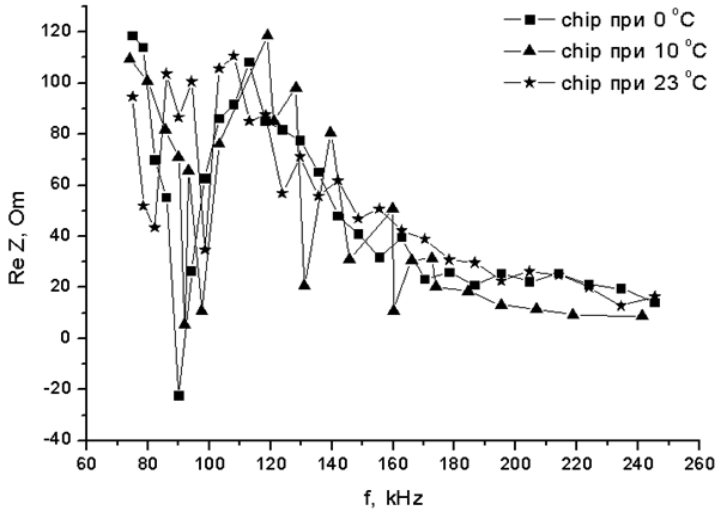


Рис.4. Експериментальні імпедансні спектри досліджуваного чіпа за температури 0° С, 10° С та 23° С.

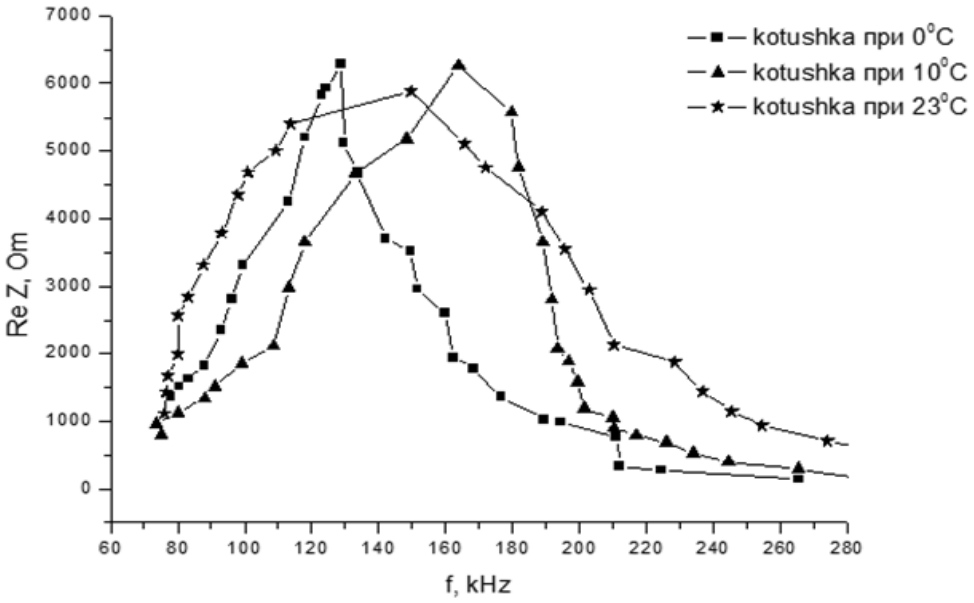


Рис.5. Експериментальні імпедансні спектри антени за температури 0° С, 10° С та 23° С.

Резонанс антени(котушки) спостерігається на частоті 120,140 та 170кГц(-див. рис.5), що є наслідком невеликої вхідної ємності вимірювальної системи.

Імпедансні частотні характеристики та діаграми Нейквіста досліджуваних елементів RFID–систем отримані за допомогою універсального імпедансного спектрометра в частотному діапазоні 50-250кГц. Вимірювання проводились за допомогою вимірювального комплексу “AUTOLAB” фірми “ECO CHEMIE” (Голандія) та програмного забезпечення FRA-2 та GPES та Origin 6.0.

**Висновки.** В результаті досліджень комплексного опору RFID–карток та їх елементів встановлено, що імпеданс для кожної картки та її елементів є індивідуальним. В цілому система є захищеною від побічних електромагнітних полів, тобто вона може самостійно реагувати на некоректні гармоніки. Добротність антени впливає на роботу системи, таким чином чим вища добротність тим вища амплітуда корисного сигналу і як наслідок більша дальність зчитування картки. Таким чином, імпедансні властивості RFID–карток можна використовувати для підвищення захищеності системи, не витрачаючи при цьому додаткової енергії самого пристрою.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стариковский А.В., Жуков И.Ю., Михайлов Д.М. Усовершенствованный протокол аутентификации бюджетных RFID-меток./ Спецтехника и связь, 2012. – № 1. – С. 25 – 27.
2. Дистанционный съём информации с RFID – карточки: ничего сложного. [Електронний ресурс] - Режим доступу: https://xakep.ru/2012/01/31/58208/

3. Roberti M. RFID Security: a Reality Check [Електронний ресурс] - Режим доступу: http//www.rfidjornal.com
4. Р.А. Юрьев. Методы и средства клонирования RFID-меток//Технология программирования и защиты информации. 2015- С.215.
5. Проблемы и их решения в RFID технологии [Електронний ресурс]. Режим доступу: http://www.itsec.ru/articles2/Inf_security.
6. Фролова Г. Технология RFID. Проблемы и решения / Г. Фролова // Журнал «Склад и техника», 2007. – № 1.
7. Nicolas T. Courtois. The dark side of security by obscurity - and cloning MIFARE Classic rail and building passes, anywhere, anytime. In 4th International Conference on Security and Cryptography (SECRYPT 2009), pages 331–338. INSTICC Press, 2009.
8. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the MIFARE Classic. In 8th Smart Card Research and Advanced Applications Conference (CARDIS 2008), volume 5189 of Lecture Notes in Computer Science, pages 267–282. Springer-Verlag, 2008.
9. Ronny Wichers Schreur, Peter van Rossum, Flavio D. Garcia, Wouter Teepe, Jaap-Henk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. Security flaw in MIFARE Classic. Press release, Digital Security group, Radboud University Nijmegen, The Netherlands, March 2008.
10. Ronny Wichers Schreur, Peter van Rossum, Flavio D. Garcia, Wouter Teepe, JaapHenk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. Security flaw in MIFARE Classic. http://www.sos.cs.ru.nl/applications/rfid/pressrelease.en.html, March 2008. Press release, Digital Security group, Radboud University Nijmegen, The Netherlands.
11. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly pickpocketing a MIFARE Classic card. In 30th IEEE Symposium on Security and Privacy (S&P 2009), pages 3–15. IEEE Computer Society, 2009.
12. Roel Verdult. Proof of concept, cloning the OV-chip card. Technical report, Radboud University Nijmegen, 2008.
13. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the MIFARE Classic. In 8th Smart Card Research and Advanced Applications Conference (CARDIS 2008), volume 5189 of Lecture Notes in Computer Science, pages 267–282. Springer-Verlag, 2013.
14. Martin Feldhofer, Manfred Josef Aigner, Michael Hutter, Thomas Plos, Erich Wenger, and Thomas Baier. Semi-passive RFID development platform for implementing and attacking security tags. In 2nd International Workshop on RFID/USN Security and Cryptography (RISC 2010), pages 1–6. IEEE Computer Society, 2010.
15. Roel Verdult, Flavio D. Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with Hitag2. In 21st USENIX Security Symposium (USENIX Security 2012). USENIX Association, 2012.
16. Josep Balasch, Benedikt Gierlichs, Roel Verdult, Lejla Batina, and Ingrid Verbauwhede. Power analysis of Atmel CryptoMemory - recovering keys from secure EEPROMs. In 12th Cryptographers' Track at the RSA Conference (CT-RSA 2012), volume 7178 of Lecture Notes in Computer Science, pages 19–34. Springer-Verlag, 2012.
17. Alex Biryukov, Ilya Kizhvatov, and Bin Zhang. Cryptanalysis of the Atmel cipher in SecureMemory, CryptoMemory and CryptoRF. In 9th Applied Cryptography and

Network Security (ACNS 2011), volume 6715 of Lecture Notes in Computer Science, pages 91–109. Springer-Verlag, 2011.
18. Roel Verdult. Security analysis of RFID tags. June 25, 2008.

## REFERENCES

1. Starykovskyy A.V., Zhukov Y.Yu., Mykhaylov D.M. (2012). Usovershenstvovannyy protokol autentyfykatsyy byudzhetnykh RFID-metok./ Spetstekhnyka y svyaz'– # 1. – S. 25 – 27. (in Russian)
2. Dystantsyonnyy siem ynformatsyy s RFID – kartochky: nycheho slozhnoho. [Elektronnyy resurs] - Rezhym dostupu: https://xakep.ru/2012/01/31/58208/(in Russian)
3. Roberti M. RFID Security: a Reality Check [Elektronnyy resurs] - Rezhym dostupu: http//www.rfidjornal.com (in English)
4. R.A. Yur'ev. (2015). Metody y sredstva klonyrovanyya RFID-metok//Tekhnolohyya prohrammyrovanyya y zashchyty ynformatsyy. - S.215. (in Russian)
5. Problemy y ykh reshenyya v RFID tekhnolohyy [Elektronnyy resurs]. Rezhym dostupu: http://www.itsec.ru/articles2/Inf_security. (in Russian)
6. Frolova G. (2007). Tekhnolohyya RFID. Problemy y reshenyya / H. Frolova // Zhurnal «Sklad y tekhnyka»– # 1. (in Russian)
7. Nicolas T. Courtois. (2009). The dark side of security by obscurity - and cloning MIFARE Classic rail and building passes, anywhere, anytime. In 4th International Conference on Security and Cryptography (SECRYPT 2009), pages 331–338. INSTICC Press. (in English)
8. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. (2008). A practical attack on the MIFARE Classic. In 8th Smart Card Research and Advanced Applications Conference (CARDIS 2008), volume 5189 of Lecture Notes in Computer Science, pages 267–282. Springer-Verlag. (in English)
9. Ronny Wichers Schreur, Peter van Rossum, Flavio D. Garcia, Wouter Teepe, Jaap-Henk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. (2008). Security flaw in MIFARE Classic. Press release, Digital Security group, Radboud University Nijmegen, The Netherlands, March. (in English)
10. Ronny Wichers Schreur, Peter van Rossum, Flavio D. Garcia, Wouter Teepe, JaapHenk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. Security flaw in MIFARE Classic. http://www.sos.cs.ru.nl/applications/rfid/pressrelease.en.html, March 2008. Press release, Digital Security group, Radboud University Nijmegen, The Netherlands. (in English)
11. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. (2009). Wirelessly pickpocketing a MIFARE Classic card. In 30th IEEE Symposium on Security and Privacy (S&P 2009), pages 3–15. IEEE Computer Society. (in English)
12. Roel Verdult. (2008). Proof of concept, cloning the OV-chip card. Technical report, Radboud University Nijmegen. (in English)
13. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. (2013). A practical attack on the MIFARE Classic. In 8th Smart Card Research and Advanced Applications Conference (CARDIS 2008), volume 5189 of Lecture Notes in Computer Science, pages 267–282. Springer-Verlag. (in English)
14. Martin Feldhofer, Manfred Josef Aigner, Michael Hutter, Thomas Plos, Erich Wenger, and Thomas Baier. (2010). Semi-passive RFID development platform for implementing

and attacking security tags. In 2nd International Workshop on RFID/USN Security and Cryptography (RISC 2010), pages 1–6. IEEE Computer Society. (in English)
15. Roel Verdult, Flavio D. Garcia, and Josep Balasch. (2012). Gone in 360 seconds: Hijacking with Hitag2. In 21st USENIX Security Symposium (USENIX Security 2012). USENIX Association. (in English)
16. Josep Balasch, Benedikt Gierlichs, Roel Verdult, Lejla Batina, and Ingrid Verbauwhede. (2012). Power analysis of Atmel CryptoMemory - recovering keys from secure EEPROMs. In 12th Cryptographers» Track at the RSA Conference (CT-RSA 2012), volume 7178 of Lecture Notes in Computer Science, pages 19–34. Springer-Verlag. (in English)
17. Alex Biryukov, Ilya Kizhvatov, and Bin Zhang. (2011). Cryptanalysis of the Atmel cipher in SecureMemory, CryptoMemory and CryptoRF. In 9th Applied Cryptography and Network Security (ACNS 2011), volume 6715 of Lecture Notes in Computer Science, pages 91–109. Springer-Verlag. (in English)
18. Roel Verdult. (2008). Security analysis of RFID tags. June 25. (in English)

**UDC 665.3**

## PROTECTION OF SYSTEMS OF RADIO FREQUENCY IDENTIFICATION BY IMPEDANCE

V.B. Dudykevych, I.S. Sobchuk, L.M. Rakobovchuk,
P.I. Haraniuk, I.P. Haraniuk.

*National University "Lviv Politechnic", 12, S.Bandera St., Lviv, Ukraine,*
*E-mail: Igorpolitech@gmail.com*

*The article considers the possibility of using an impedance to protect RFID cards from unauthorized reading of information. An analysis of literature sources on the protection of RFID systems has been conducted, as well as research on the impedance of RFID tags and its elements in the frequency range of 50-250 kHz. Impedance spectra of RFID tags, chips and antennas for different cards have been shown.*

*RFID (Radio Frequency Identification) is a technology for contactless automatic identification of objects using a radio frequency communication channel.*

*The purpose of the paper is to study the possibility of using RFID-impedance properties to increase the security against unauthorized reading of information.*

*As a result of the research of integrated impedance of RFID-cards and their elements, it has been established that the impedance for each card and its elements is individual. In general, the system is protected from adjacent electromagnetic fields, that is, it can independently respond to incorrect harmonics. The quality of the antenna affects the operation of the system, so the higher the quality factor, the higher the amplitude of the useful signal and as a result, the greater the range of reading the card. Thus, the impedance properties of RFID cards can be used*

*to increase the security of the system without wasting the additional energy of the device itself.*

***Keywords:*** *RFID, non-contact radio frequency identification, RFID technology, RFID tags, tags, chip, annetna (contour), impedance, complex impedance, impedance spectra, temperature dependence of impedance.*

*Стаття надійшла до редакції 14.02.2017*
*Received 14.02.2017*