УДК 621.391.5: 004.056.53 **DOI:10.30837/rt.2021.1.204.11**

В.Г. КРИЖАНОВСЬКИЙ, д-р техн. наук, С.П. СЕРГІЄНКО, канд. физ.-мат. наук,
Д.В. ЧЕРНОВ, канд. техн. наук, В.В. КРИЖАНОВСЬКИЙ, канд. техн. наук

ПІДСЛУХОВУВАННЯ NFC-ЗВ'ЯЗКУ НА ЧАСТОТАХ ВИЩИХ ГАРМОНІК

Вступ

Широке використання технологій близько польової комунікації (near field communication – NFC) спонукає розглядати різні аспекти удосконалення апаратури та безпеки її використання [1 – 4]. Безпека стосується таких застосувань NFC (та RFID – radio frequency identification device) як безконтактні банківські транзакції, біометричні паспорти та багато іншого. В останній час додалась ще й безпека зарядки електромобілів [5].

У роботі [3] розглянуто різні види атак на NFC-зв'язок, в [4] детально аналізуються можливості збільшення відстані, на якій можливо або підслухати або здійснити звернення до пристроїв з NFC-зв'язком. У роботах [6, 7] розглядається можливість здійснення доступу до NFC картки (RFID пристрою) з використанням прийому сигналу на вищих гармоніках частоти збудження. Аналіз процесу збудження та реєстрації сигналів у цих роботах є доволі детальним, але складність всього комплексу проблем є великою і відпрацювання методики вимірювання та вивчення можливостей впливу на випромінювання та прийом сигналу за цим побічним каналом є актуальною задачею.

Метою даної роботи є аналіз та експериментальне дослідження залежностей відстані, на якій можливо підслуховувати NFC зв'язок з використанням приймача на частотах вищих гармонік частоти 13,56 МГц.

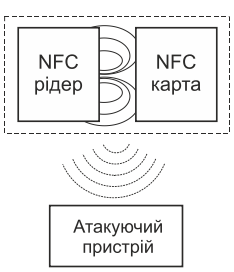
Аналіз стану проблеми та використовуваного обладнання

Зв'язок у близькому полі (NFC) є індуктивним зв'язком близько розташованих котушок індуктивності, пов'язаних спільним магнітним полем [1, 2]. Відповідно напруженість поля зменшується з відстанню за законом $1/r^3$, і на порівняно невеликих відстанях зв'язок стає неможливим, що є передумовою збереження конфіденційності транзакцій. Довжина електромагнітної хвилі на частоті 13,56 МГц складає 22,11 м, і елементи рідера не здатні скласти ефективну антену, але на частоті третьої гармоніки 40,68 МГц довжина хвилі у вільному просторі вже 7,37 м, тому можливе випромінювання цього сигналу пов'язаними провідниками. У роботі [6] такою антеною слугував USB кабель, який з'єднував комп'ютер і рідер. Тому вивчення, в тому числі експериментальне, джерел генерації та випромінювання вищих гармонік несучої частоти обміну інформації у системах NFC та RFID важливе для практики захисту інформації.

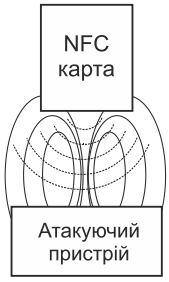
Є два основні варіанти несанкціонованого отримання даних з тегу (карти чи іншого пристрою RFID) – це підслуховування (рис. 1, *а*) чи скіммінг («зняття вершків» у вільному перекладі, рис. 1, *б*). У першому випадку здійснюється отримання інформації зі штатного процесу обміну легального рідеру та безконтактної картки, у другому – зловмисник генерує сигнал, яким запитує від картки інформацію, і потім приймає її без відома власника. Для цього можуть використовуватися збільшенні розміри антенних систем та використовуватися прийом на частотах вищих гармонік [4, 6 – 9]. Відстані, на яких це можливо здійснити, дають можливість розташувати антенні системи у стиснених умовах непомітно для власника картки.

Імітатор NFC-зв'язку. Для виконання експерименту потрібно мати передавач, який зв'язується з тегом на частоті 13,56 МГц. Використання різних реальних систем (смартфон з NFC та картка для сплати за проїзд) має той недолік, що процес встановлення зв'язку неперіодичний, і це ускладнює вимоги до апаратури, яка повинна реєструвати випромінювання

на частоті гармоніки. Тому було використано простішу схему зчитувача (рідера), побудованого на базі процесора Arduino Nano, та пристрою RFID-RC522 (рис. 2).



а



б

Рис. 1

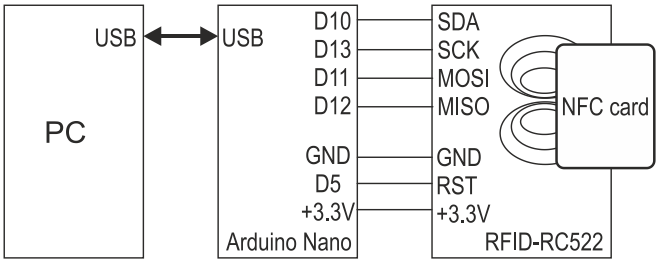


Рис. 2

Програма для Arduino Nano була складена на основі програми [10], вона дозволила проводити періодичне зчитування даних з картки, і тому на спектроаналізаторі можна було дослідити спектр передачі від картки до зчитувача. Спочатку було проведено вимірювання, яке підтвердило, що і в цьому випадку третя гармоніка переважно генерується NFC карткою (табл. 1). На рис. 3 показано спектри без картки (нижня частина) та з карткою (верхня спектрограма). На рис. 4 показана схема експерименту, де 1 – безконтактна картка, 2 – котушка зв'язку, використовувалась NFC антена зі смартфона, FPC1500 – спектроанализатор.

Таблиця 1

Спектр	1 гармоника, dBm	2 гармоника, dBm	3 гармоника, dBm
Без NFC карты	-33,5	-62,56	-73,97
С NFC картой	-31,68	-66,5	-62,7

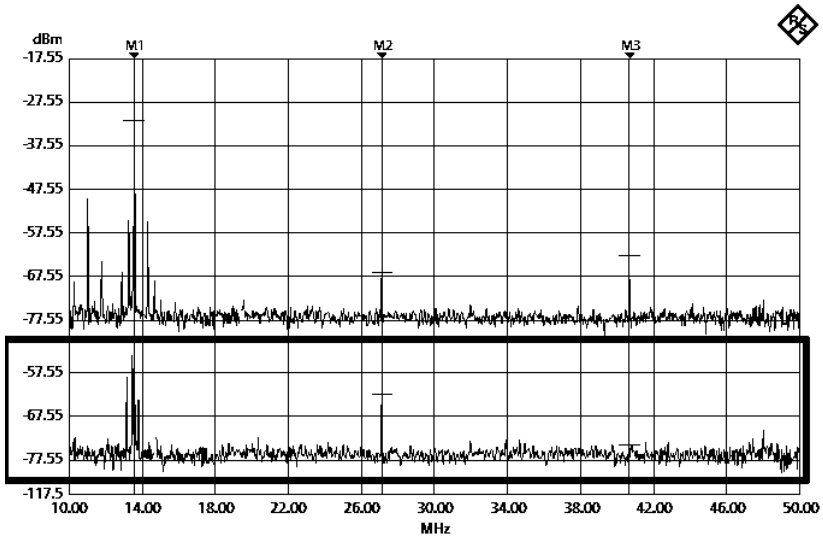


Рис. 3

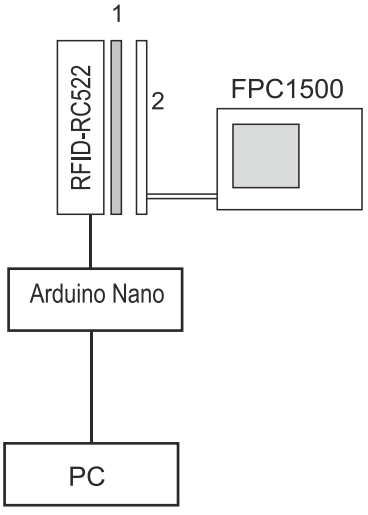


Рис. 4

Видно, що третя гармоніка сигналу значною мірою генерується у NFC картці, і сигнал цієї частоти можна використовувати для отримання інформації про картку.

В роботі використовувалась картка стандарту ISO 14443-3A з криптографічним алгоритмом NXP MIFARE Classic 1k, як це визначено за результатами тестування за допомогою смартфона Sony Xperia Z5 Premium. За стандартом ISO 14443A зчитувач передає кодовані дані з кодом Міллера 106 кбіт/с за допомогою імпульсів 3 мкс. Отже, дані прямого каналу повинні знаходитись у перших 330 кГц спектру. Картка передає закодовані кодом Манчестер 106 кбіт/с дані, які модулюються ASK на піднесучій частоті 847,5 кГц. Зворотний канал повинен бути в діапазоні 424 кГц, зосередженим близько 847,5 кГц. Прямий канал амплітуд-

но модулюється на 13,56 МГц з індексом модуляції 100 %, тоді як зворотний канал має індекс модуляції 8–12 % [2]. На рис. 5 показана спектрограма обміну інформацією між зчитувачем та карткою, видно складові модуляції біля основної частоти $f_0 = 13{,}56$ МГц та біля піднесучих $f_0 \pm f_M$, де $f_M = f_0/16 = 0{,}8475$ МГц, використовувався багатофункціональний спектроаналізатор R&S FPC1500. На рис. 6 показано спектр сигналу біля третьої гармоніки основної частоти – 40,68 МГц за вимірюваннями за допомогою рамочної антени. Для показу основних характеристик сигналу виконувалось усереднення сигналу за останні 10 вимірювань. Також було збільшено полосу ВЧ фільтру до 100 кГц та відеофільтру до 1 МГц. Видно, що найбільша бокова складова знаходиться на відстані ±848 кГц. Це свідчить про те, що третя гармоніка основної частоти модулюється безпосередньо частотою піднесучої, а не утворюється за рахунок потроювання складових спектру, що передається карткою. Тому інформацію, яку передає картка до зчитувача, можна відстежувати на частотах 40,68±0,8475 МГц.

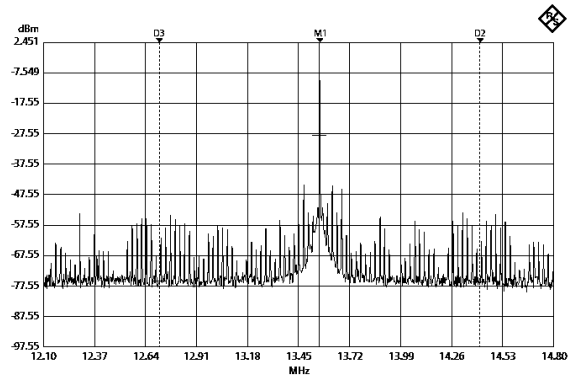


Рис. 5

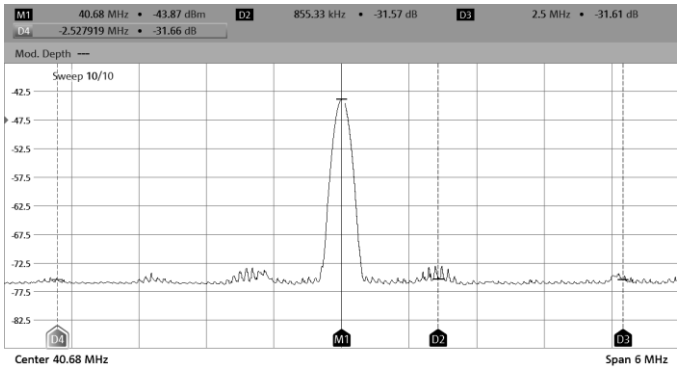


Рис. 6

Для попереднього експерименту було досліджено можливість використання картки без ініціювання її відповіді на запит від рідера. Для цього використовувалася схема рис. 7, де сигнал від картки на частотах 13,56±0,8475 МГц було замінено на подачу АМ сигналу з таким самим спектром; моделювання у часовій області показало, що і в такому режимі картка повинна генерувати частотні складові $3f_0 \pm f_M$ (рис. 8). При цьому мікросхема картки не вмикалась на передачу даних, і сигнал третьої гармоніки генерувався за рахунок нелінійності діодів мостової схеми, як і в штатному режимі роботи. Але при цьому сигнал, що приймався, був стаціонарним і було легше його вимірювати. Передавальна котушка індуктивності L_1 разом з ємністю C_1 утворювали резонансний контур, який пропускав частоти $f_0 \pm f_M$ але послаблював частоти $3f_0 \pm f_M$, це разом з опційним фільтром нижніх частот (ФНЧ) (рис. 7) робило випромінювання схеми живлення картки на частотах третьої гармоніки низьким, і відповідно спостерігалось переважно випромінювання самої картки.

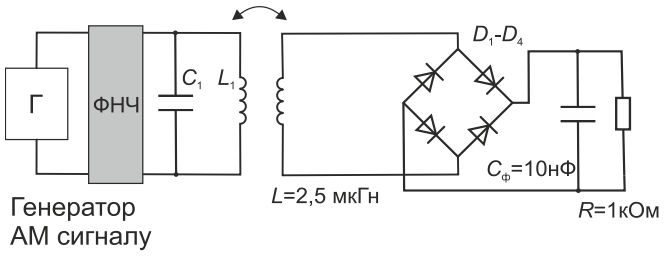


Рис. 7

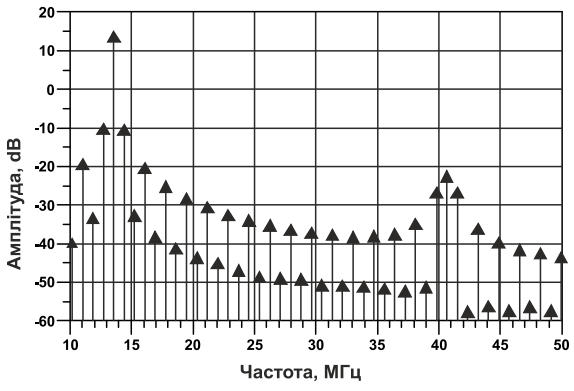


Рис. 8

Перевагою такого рішення є безперервна передача сигналу та більш точне вимірювання спектральних складових прийнятого сигналу. Маючи такі способи генерації тестового сигналу, можна виміряти відстань, на якій можливо зареєструвати сигнал на частоті третьої гармоніки.

Антена на частоту третьої гармоніки та вимірювання відстанні. Аналогічно роботі [7] для прийому сигналу на частоті 40,68 МГц була використана резонансна магнітна антена у вигляді кільцевого вібратора, який навантажений на ємність та узгоджується з лінією 50 Ом за допомогою гамма-узгодження. Антена має діаметр 77 см та виготовлена з алюмінієвого обручу (діаметр трубки 16 мм), рис. 9. КСВН антени показано на рис. 10. Антена має вузьку смугу частот, де вона узгоджена, до того ж узгодження залежить від оточуючих предметів, тому налаштування антени постійно перевірялось при зміні умов експерименту.

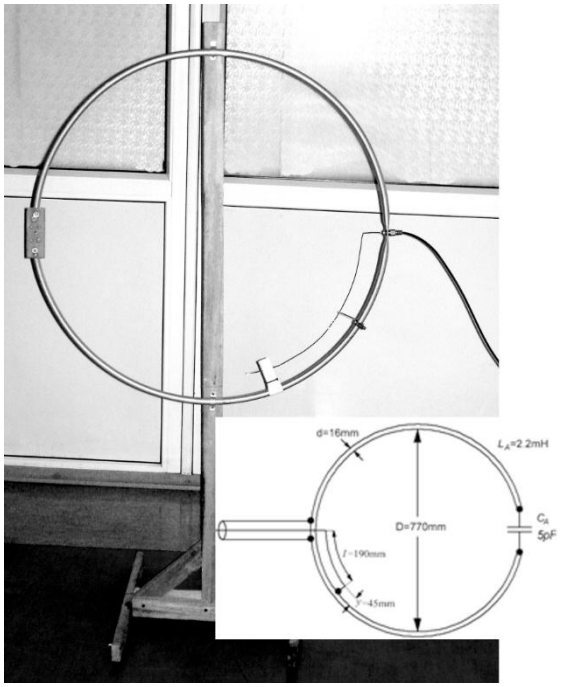


Рис. 9

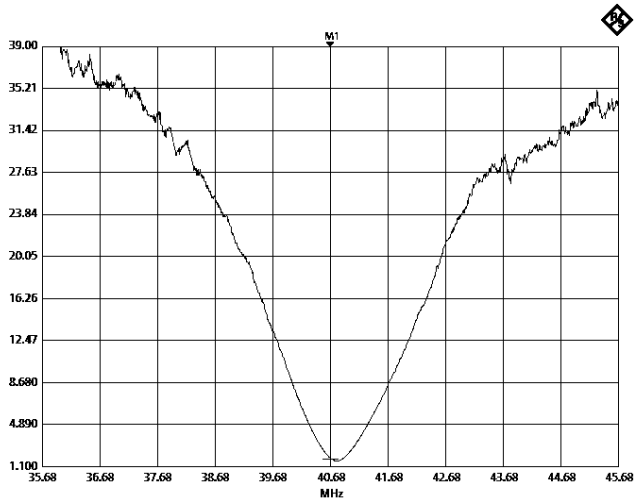


Рис. 10

Використовуючи цю антену, за схемою рис. 7 виміряли залежність сигналу картки в діапазоні частоти третьої гармоніки від відстані між карткою та приймальною антеною. Картка та антена були розташовані на одній горизонтальній осі. Залежність показана на рис. 11, вимірювання проводились при подачі на котушку L_1 змінної напруги 13,56 МГц з 10 %-ю амплітудною модуляцією прямокутним сигналом частотою f_M. Показано залежності для двох значень амплітуди основного сигналу – 6 та 8 В. Картка при цьому не передавала даних, і спостереження проводилось за спектральними складовими на частотах $3f_0$ та $3f_0 \pm f_M$. Результат свідчить про те, що рівень сигналу модуляції знаходиться на рівні шуму спектроаналізатору. В режимі вимірювання аналогової модуляції аналізатор FPC1500 здатен виявити сигнал модуляції на частоті f_M тільки при відстані між карткою и приймальною антеною біля 2 см.

При вимірюванні за схемою рис. 4, коли картка працює в періодичному режимі «запит-відповідь» з живленням від стандартного зчитувача, рівень сигналу на частоті третьої гармоніки при тій же відстані трохи вищий, але так само досягає рівня шумів. Залежність на рис. 12 отримана як результат усереднення 10 вимірювань на кожній відстані, кожне вимірювання є результатом усереднення спектроаналізатором 10 розгорток у часі. Спектрограма

кожного вимірювання має вигляд рис. 6, відповідно можна зробити висновок про наявність сигналу, але складно здійснити детектування сигналу від картки. Для розширення діапазону потрібно розшити полосу частот приймальної антени та удосконалити приймач сигналів. На додаток можна зауважити, що розглянута схема підслуховування може бути використана і у складі більш складних атак на безконтактні картки [4, 11].

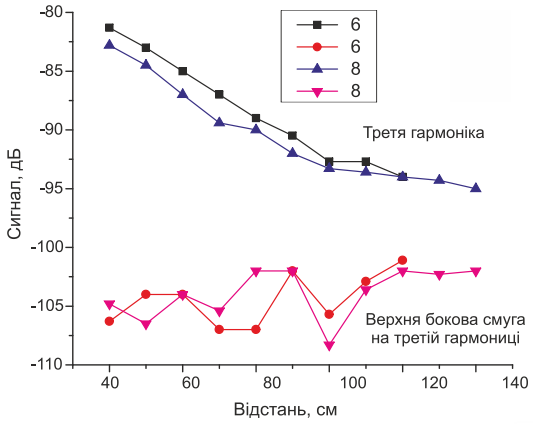


Рис. 11

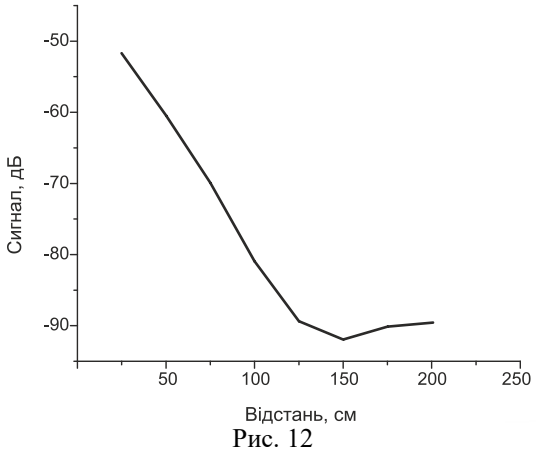


Рис. 12

Висновки

Розроблено обладнання та запропоновано методи вимірювання випромінювання вищих гармонік, які генеруються у безконтактних картках NFC-зв'язку з основною частотою 13,56 МГц. Підтверджено можливість збільшити відстань прийняття сигналу третьої гармоніки від картки, разом з тим при використанні резонансних приймальних антен демодуляція інформативного сигналу викликає складнощі, оскільки рівень бокових складових значно послаблюється і на вході приймача знаходиться на рівні шуму. Для можливості підслуховування сигналу потрібно використовувати відносно широкосмугові антени та підсилювачі з низьким рівнем шуму.

Список літератури:

1. Чернов Д.В., Крыжановський В.Г. Усилитель класса Е в составе трансивера системы ближнеполевой коммуникации // Технічна електродинаміка. Тем. вип. Силова електроніка та енергоефективність. 2011. Ч. 1. С. 293-298.

2. Finkenzeller K. RFID handbook: fundamentals and applications in contactless smart cards and Identification. ; 2nd ed. John Wiley & Sons Ltd, 2003. 427 p.

3. Bolhuis M. Using an NFC-equipped mobile phone as a token in physical access control. Thesis… University of Twente, 2014. 129 p. http://essay.utwente.nl/65419/1/thesis_nfc_martijn_bolhuis_ final.pdf

4. Hancke G. P. Practical eaves dropping and skimming attacks on high-frequency RFID tokens // J. Comput. Security. Mar. 14, 2011. Vol. 19, no. 2, pp. 259–288,

5. Van den Broek F., Poll E., Vieira B. (2015). Securing the Information Infrastructure for EV Charging // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 61–74.

6. Engelhardt M., Pfeiffer F., Finkenzeller K. and Biebl E. Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics // Smart SysTech 2013; European Conference on Smart Objects, Systems and Technologies, Erlangen/Nuremberg, Germany, 2013, pp. 1-8.

7. Habraken R., Dolron P., Poll E & De Ruiter J. 2015 An RFID Skimming Gate Using Higher Harmonics // S Mangard & P Schaumont (eds), Radio Frequency Identification. Security and Privacy Issues. vol. 9440, Lecture Notes in Computer Science, vol. 9440, Springer, pp. 122-137, 11th Workshop on RFID Security, New York, United States, 23/06/15.

8. Ilan Kirschenbaum, Avishai Wool. How to Build a Low-Cost, Extended-Range RFID Skimmer. 15th Security Symposium Security 06. Vancouver, B.C. Canada, 07/2006 https://documen.site/download/how-to-build-a-low-cost-extended_pdf.

9. Brown T. W. C., Diakos T. and Briffa J. A. Evaluating the eavesdropping range of varying magnetic field strengths in NFC standards // 2013 7th European Conference on Antennas and Propagation (EuCAP), Gothenburg, Sweden, 2013, pp. 3525-3528.

10. MFRC522 library https://github.com/miguelbalboa/rfid (ПО для МС)

11. Oren Y., Schirman D., Wool A. Range extension attacks on contactless smart cards // Crampton, J., Jajodia, S., Mayes, K. (eds.) Computer Security – ES-ORICS 2013, LNCS, vol. 8134, pp. 646–663. Springer (2013).

Надійшла до редколегії 28.01.2021

Відомості про авторів:

Крижановський Володимир Григорович – д-р техн. наук, професор, професор кафедри радіофізики та кібербезпеки; Донецький національний університет імені Василя Стуса (м. Вінниця); Україна; email: v.krizhanovski@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-2685-9740

Сергієнко Сергій Петрович – канд. техн. наук, доцент, доцент кафедри радіофізики та кібербезпеки; Донецький національний університет імені Василя Стуса (м. Вінниця); Україна; email: s.serhiienko@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-5515-8946

Чернов Дмитро Вікторович – канд. техн. наук, доцент кафедри радіофізики та кібербезпеки; Донецький національний університет імені Василя Стуса (м. Вінниця); Україна; email: d.chernov@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-7173-0842

Крижановський Володимир Володимирович – канд. техн. наук, Synic Solution Co., Ltd, 37, Hwangsaeul-ro 258 beon-gil, Seongnam-si Republic of Korea; email: vlad@synic.co.kr; ORCID: https://orcid.org/0000-0003-1989-1483