

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

**ГУМЕНЮК ВЛАДИСЛАВ ДМИТРОВИЧ**

Допускається до захисту:

Завідувач кафедри інформаційних  
технологій,

кандидат технічних наук, доцент

\_\_\_\_\_ Т. В. Нескородева

« \_\_\_\_ » \_\_\_\_\_ 2021 року

**СКІМІНГ NFC КАРТОК НА ВИЩІЙ ГАРМОНІЇ**

Спеціальність 125 Кіберзахист

**Кваліфікаційна (бакалаврська) робота**

Керівник:

Чернов Д. В., доцент кафедри  
інформаційних технологій,  
кандидат технічних наук

\_\_\_\_\_

підпис

Оцінка: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

( бали за шкалою ЄКТС / за національною шкалою )

Голова ЕК: \_\_\_\_\_

(підпис)

Вінниця – 2021

## АНОТАЦІЯ

**Гуменюк В.Д. Скімінг NFC карток на вищій гармоніці. Спеціальність 125 Кіберзахист. Донецький національний університет імені Василя Стуса, Вінниця, 2021.**

У кваліфікаційній роботі досліджено роботу технологію та безпеку безпроводних карток. Проведений аналіз різноманітних атак на безконтактні NFC картки за допомогою вищих гармонік. За результатами аналізу була створена антена для скімінгу з ціллю збільшення діапазону атаки.

Ключові слова: NFC, вищі гармоніки, скімінг, цифрова валюта.

Рис. 10. Бібліогр.: 33.

**Humeniuk Vladyslav.NFC cards skimming on higher harmonics.Specialty 125.Cybersecurity. Vasyl Stus' Donetsk National University, Vinnytsia, 2021.**

**The work, technology and security of cards equipped with NFC are researched in this qualification work.The analysis of different attacks on contactless NFC cards with the help of higher harmonics.According to the analysis results, a skimming antenna was found in order to increase the attack range.**

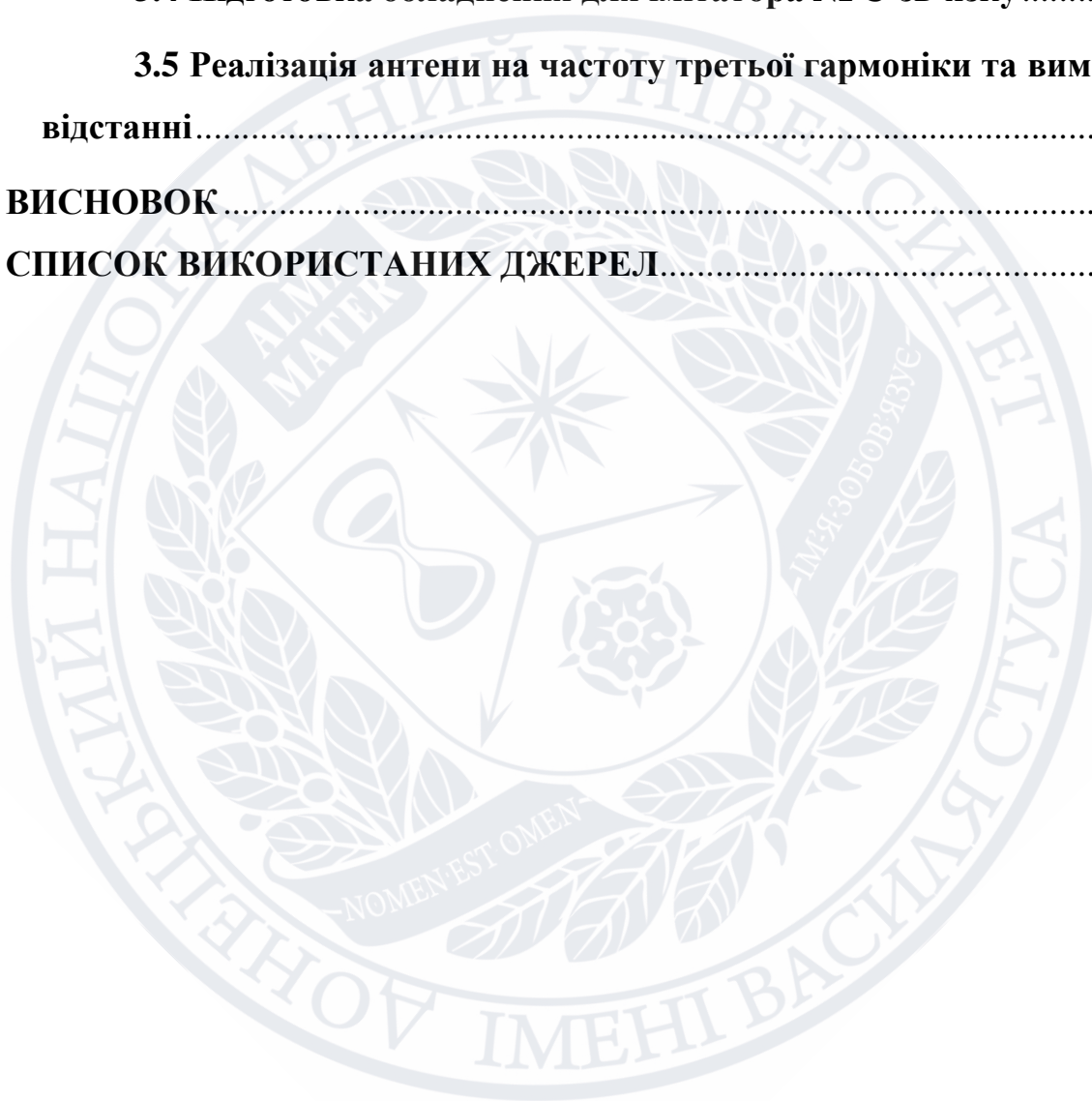
**Keywords: NFC,higher harmonics,skimming,digital currency.**

**Drawings 10, Bibliography 33.**

## ЗМІСТ

<b>РОЗДІЛ 1. ЩО ТАКЕ NFC ТА ПРИНЦИП ЙОГО ДІЇ.</b>	<b>8</b>
1.1. Що таке NFC?	8
1.2. Як працює NFC?	9
1.3. Використання NFC-міток	11
1.3.1. Обмін даними	11
1.3.2. Читання і запис даних	12
1.3.3. Емуляція роботи смарт-карт.	12
1.4. Архітектура NFC	13
1.5. Типи частот на якій працюють RFID/NFC	14
1.6. APDU	15
1.7. Клонування безконтактних карт	15
<b>РОЗДІЛ 2. СКІМІНГ. ЙОГО ПОНЯТТЯ ТА ПРИНЦИП ДІЇ</b>	<b>17</b>
2.1. Скімінг	17
2.2. Скімінг безконтактних NFC та RFID приладів	17
2.3. Робота безконтактної оплати	18
2.4. Реалізація безпеки безконтактної банківської карти. Чому її неможливо скопувати?	20
2.5. Процес емулявання карти мобільним телефоном	21
2.6. Зчитування даних безконтактних карток	23
2.7. Вразливість у банківських карток, які використовують NFC технологію	23
2.8. Види атаки	24
2.9. Види захисту проти хакерської атаки на безконтактну картку	24
2.10. Що безпечніше: смартфон або карта?	25

<b>РОЗДІЛ 3.....</b>	<b>28</b>
<b>3.1. Збільшення відстані атаки .....</b>	<b>28</b>
<b>3.2. Збільшення діапазону атаки на RFID або NFC приладів за допомогою вищої гармоніки .....</b>	<b>28</b>
<b>3.3 Несанкціоноване отримання даних .....</b>	<b>29</b>
<b>3.4 Підготовка обладнання для імітатора NFC-зв'язку .....</b>	<b>30</b>
<b>3.5 Реалізація антени на частоту третьої гармоніки та вимірювання відстанні.....</b>	<b>31</b>
<b>ВИСНОВОК.....</b>	<b>33</b>
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....</b>	<b>34</b>





## ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

NFC - Near Field Communication.

RFID - Radio frequency identification device

EMV - міжнародний стандарт для операцій з банківських карток з чипом.

Банк емітент - це банк, який випустив вашу карту.

POS-термінал (Point of Sale) - пристрій продавця, який зчитує карту і ініціює платіж.

Банк еквайєр - банк, який видає продавцям POS-термінали і обробляє платежі з них.

Транспондер - це приймально-передавальний пристрій, що надсилає сигнал у відповідь на прийнятий сигнал, наприклад: автоматичний пристрій, що приймає, підсилює і передає сигнал далі на іншій частоті.

Платіжна система - центральна ланка між банком еквайєром і банком емітентом, через неї проходять абсолютно всі платежі, і вона знає який банк скільки повинен перевести грошей.

EEPROM - постійний запам'ятовувач, що програмується та очищується за допомогою електрики, один з видів енергонезалежної пам'яті. Пам'ять такого типу може очищуватися та заповнюватися інформацією декілька десятків тисяч разів.

## ВСТУП

Інтернет технології з кожним днем удосконалюються, задля поліпшення життя звичайних людей. Банки та різноманітні компанії впроваджують ці системи, але немає нічого неперевершеного, тому кіберзлочинність розвивається на такому ж самому рівні, як і інтернет технології.

З моменту появи технологій NFC и RFID, які взаємодіють з ISO / IEC 14443 та пристрої, що використовують ці технологію, широко використовуються у галузях фінансових транзакцій, логістиці, біомедицинських застосуваннях та інших. Оскільки пасивні мітки ISO / IEC 14443 призначені для роботи на максимальній відстані близько 10 см, усе це заставляє розглядати різні аспекти їх використання, у тому числі і безпеку передачі даних як від спотворення, так і перехоплення.

З точки зору інформаційної безпеки основні слабкості і недоліки NFC та RFID пристроїв пов'язані з тим, що стек протоколів безконтактних пристроїв не передбачає криптографії при передачі. У роботі ми розглянемо технічні характеристики NFC, RFID пристроїв, та способи скімінгу безконтактних платіжних карт.

У цій роботі ми розглянемо проблеми безпеки NFC, RFID технологій, які застосовуються при ідентифікації клієнта, наприклад посвідчення особи, або у якості електронного ключа, але найчастіше ця технологія використовується для безконтактної оплати .

**Метою роботи** є виявлення потенційної можливості прийому сигналу вищої гамоніки, сгенерованої у NFC RFID картці.

**Об'єкт дослідження** – процеси генерації вищих гармонік на нелінійних пристроях.

**Предмет дослідження** — характеристики розповсюдження вищих гармонік, сгенерованих у NFC RFID картці.

**Завдання дослідження :**

- проаналізувати типи безконтактних карток, та визначити їх сильні та слабкі сторони;
- ознайомитись з видами реалізації безпеки у безконтактних картках;
- виміряти характеристику відносного рівня третьої гармоніки на відстані від NFC смарт-карти.



## РОЗДІЛ 1. ЩО ТАКЕ NFC ТА ПРИНЦИП ЙОГО ДІЇ.

### 1.1. Що таке NFC?

*Nfc* - це технологія безконтактного зв'язку, яка працює на відстані до 10см. Вона розшифровується як NFC - Near Field Communication.

Для роботи даної технології потрібен як мінімум один передавальний і один пристрій для прийому сигналу.

NFC поділяються на пасивні та активні пристрої.

Активні пристрої можуть як відсилати і одержувати дані, так і контактувати один з одним. Сучасні смартфони є найбільш поширеною формою активного NFC-пристрою. Зчитувачі карт (валідатори) в громадському транспорті і безконтактні платіжні термінали також є хорошими прикладами цієї технології.

Активні NFC встановлюють в:

- -ігрових приставках
- -аудіотехніці
- -фотоапаратах і відеокамерах
- -платіжних терміналах
- -розумних годинниках і фітнес-браслетах
- -смартфонах, планшетах

Пасивні пристрої NFC мають вже записану інформацію, і вони створені задля відправлення цієї інформації, найчастіше такі пристрої не потребують власного джерела живлення, проте вони не вміють обробляти інформацію, відправлену з інших джерел, і не можуть підключатися до інших пасивних пристроїв. До прикладу можна взяти ситуацію : на художній виставці встановлені NFC мітки на кожній картині, після зчитування яких телефоном, отримуємо усю інформацію щодо даної картини .

Пасивні чіпи встановлюють у:

- -проїзні квитки;



- -брелок;
- -банківські картки.

## 1.2. Як працює NFC?

NFC - новий стандарт для бездротової передачі даних, який працює за принципом передачі інформації по радіохвилях. Технологія NFC заснована на ідеї RFID (радіочастотна ідентифікація), у передачі інформації якої використовувалася електромагнітна індукція.

RFID-мітки повинні відповідати певним численним стандартам в області технологій радіочастотної ідентифікації. Перерахуємо деякі з них: ISO 11784/85, ISO 15693, ISO 14443, ISO 18000-6C / B, ISO 18000-3. Відповідність тому чи іншому стандарту визначає різні характеристичні мітки:

- Робоча частота: 125 кГц, 134,2 кГц (LF), 13,56 МГц (HF), 860-960 МГц (UHF)
- Швидкість передачі даних
- Тип кодування
- Наявність перезаписуваної пам'яті
- Наявність унікального неперезаписуваного ідентифікатора
- Наявність алгоритмів, що забезпечують безпеку даних

Найголовніша відмінність між NFC, WiFi, Bluetooth є те, що для пасивних пристроїв NFC, які можуть нести певну інформацію, не потрібно джерело живлення, оскільки вони отримують живлення від електромагнітного поля створюваного активним NFC-пристроєм, коли він входить у зону дії.

Частота передачі даних по NFC становить 13,56 МГц, при якій дані відправляються зі швидкістю 106, 212 або 424 кілобіт на секунду.

Щоб визначити яким типом інформації будуть обмінюватися між собою пристрої, стандарт NFC в цей час має три різних режими роботи: пристрій читання / запису ; одноранговий зв'язок ; емуляція карти.

### 1) P2P (Peer-to-peer) режим

Робочий режим дозволяє двом пристроям з підтримкою NFC взаємодіяти один з одним для обміну інформацією та файлами, щоб користувачі пристроїв з підтримкою NFC могли швидко обмінюватися контактною інформацією та іншими файлами одним дотиком. Наприклад, користувачі можуть обмінюватися параметрами налаштування з'єднання Bluetooth або Wi-Fi або поширювати дані, такі як віртуальні візитні картки або фотографії.

## 2) Режим читання / запису

Режим читання / запису дозволяє пристроям з підтримкою NFC зчитувати інформацію, що зберігається в NFC-тегах (або мітках), вбудованих у інтелектуальні плакати і дисплеї, або взаємодіяти з іншими NFC-пристроями в режимі читання / запису. Пристрій, який ініціює, може зчитувати дані з іншого пристрою або записувати дані на нього.

## 3) Режим емуляції карти

Режим емуляції карт дозволяє пристроям з підтримкою NFC працювати як смарт-карти.

У режимі емуляції карт пристрій з підтримкою NFC обмінюється даними із зовнішнім зчитувачем як звичайна безконтактна смарт-карта. Наприклад, при виконанні платежу за допомогою пристрою з підтримкою NFC.

Можливо, найбільш поширене використання в смартфонах – це режим тимчасового зв'язку. Це дозволяє двом пристроям з підтримкою NFC обмінюватися різною інформацією один з одним. У цьому режимі обидва пристрої перемикаються між активним при відправленні даних, і пасивним при отриманні.

Стандарт NFC має ряд переваг, тому виробники активно впроваджують його у життя людей. Відмітні переваги:

- -NFC відрізняється невисокою вартістю, тому зараз активно встановлюється виробниками навіть у бюджетні моделі телефонів.
- Можливість здійснення обміну даних з іншими смартфонами.
- Низька витрата заряду батареї.
- Малі розміри чіпа.

- Час налаштування і установки чіпа займає усього декілька секунд.
- Час встановлення з'єднання не перевищує 0,1 с.
- Різноманітна реалізація цього стандарту.

За рахунок малих розмірів і знижених енерговитрат NFC може використовуватися навіть у мініатюрних пристроях. Чіп зазвичай закріплюється всередині задньої панелі або на кришці відсіку батареї. Щоб користувач знав, яким місцем потрібно прикладати телефон для передачі даних, місце установки чіпа NFC позначається спеціальною наклейкою.

### **1.3. Використання NFC-міток**

Мітка NFC - це пристрій NFC, який працює в режимі пасивної комунікації.

Такі чіпи зберігають невеликий обсяг даних, в якості яких може служити контактна інформація, адреси веб-сторінок або навіть команди, які виконуються пристроєм при зчитуванні. Перерахуємо ряд завдань, які можна закодувати за допомогою таких міток:

- Параметри екрану;
- Налаштування звуку;
- Налаштування інших інтерфейсів, наприклад, Wi-Fi і Bluetooth;
- Повідомлення;
- Дзвінки;
- Додатки та безліч інших функцій.

Оскільки технологія NFC достатньо дешева, вона монтується практично в усі мобільні пристрої, вироблені лідерами ринку.

Спочатку концепція технології представляла собою використання в якості віртуальної форми дебетових карток, але певним часом експлуатація цієї технології розширилась:

#### **1.3.1. Обмін даними**

Передача даних між пристроями (контакти, додатки, посилання, фотографії, або інші файли).



### **1.3.2. Читання і запис даних**

Читання міток зі спеціальною інформацією і зміна режимів / налаштувань / профілів пристрою, швидке сполучення з периферійними пристроями (наприклад, гарнітурами).

### **1.3.3. Емуляція роботи смарт-карт.**

Мається на увазі використання смартфона, як безконтактного пристрою оплати послуг типу платіжних карт, що використовуються для оплати.

Серед допоміжних корисних сфер використання, що з'явилися згодом - пропуск у різні установи та ідентифікація особистості. Допоміжне використання технології забезпечує можливість обміну файлами, посиланнями і іншим контентом. За допомогою програм вдається записувати інформацію і закладати її у спеціальні картки.

- Обмін даними.
- Читання і запис даних.
- Емуляція роботи смарт-карт.
- Ідентифікація особистості

Технологія NFC швидкими темпами проникає у різні сфери життя. Вже зараз NFC активно використовується:

- Як електронний ключ (NFC-технологія доступу до закритих даних)
- Як посвідчення особи (NFC-чіп з інформацією про власника)

Емуляція карт – NFC дуже добре підходить для здійснення електронних платежів і відповідно банків, оскільки вона підтримує так званий режим емуляції. Тобто за допомогою даної технології можна емулювати роботу добре відомої для всіх банківської карти. Користувачеві достатньо просто піднести свій смартфон з NFC-чіпом до терміналу і легко здійснити будь-яку транзакцію. За допомогою NFC можна створити свій власний електронний гаманець. Переваги заключаються у тому, що технологію можна впровадити практично у будь-який пристрій. Як приклад можна привести роботу технології PayPass. Її суть



заключається у наступному. Якщо у користувача є телефон з чіпом NFC і його банківська карта активована в SIM-меню, то він може підійти до будь-якого терміналу, який підтримує функцію платіжної системи MasterCard PayPass, піднести до нього телефон на потрібну відстань (1-8 сантиметрів) і платіж буде оброблений. Не потребується навіть взаємодія з платіжним терміналом. Звуковий та світловий сигнали стануть підтвердженням, що кошти списані з банківського рахунку. Все, що необхідно людині для реалізації такого рішення – мати на телефоні NFC-чіп та дані про банківські рахунки.

#### 1.4. Архітектура NFC

В архітектурі NFC є кілька рівнів. Найнижчий з них - фізичний, який реалізований ЦПУ і іншим апаратним комплексом, через який відбувається взаємодія. Усередині знаходяться дані про пакети та транспортний рівень, потім формат даних рівнів, і в кінці програмне забезпечення.



Рис. 1.1. Архітектура NFC

На фізичному рівні NFC працює за алгоритмом, який описаний в ГОСТ для RFID (ГОСТ ISO / IEC 14443-2-2014), де йдеться про малопотужні радіосигнали з частотою 13,56 МГц. За ним рівень, який описує розбивку потоку даних на фрейми (ГОСТ ISO / IEC 14443-3-2014). Будь-які радіоконтролери, які використовуються в телефоні, планшеті або приєднуються до комп'ютера або мікроконтролеру, є окремими апаратними компонентами. Вони взаємодіють з головним процесором за допомогою одного або декількох стандартних

послідовних протоколів між пристроями: універсальний асинхронний приймач (UART), послідовний периферійний інтерфейс (SPI), послідовна шина даних для зв'язку інтегральних схем (I2C), або універсальна послідовна шина (USB).

Над цим знаходиться декілька протоколів команд RFID, що базуються на двох специфікаціях. NFC читання і запис міток базується на оригінальному RFID ДСТУ ISO / IEC 14443A. Протоколи Philips / NXP Semiconductors Mifare Classic і Mifare Ultralight і NXP DESFire сумісні з ДСТУ ISO / IEC 14443A. Обмін даними P2P NFC базується на ДСТУ ISO / IEC 18092.

### **1.5. Типи частот на якій працюють RFID/NFC**

Типи частот на якій працюють RFID/NFC системи діляться на:

- низькі частоти (НЧ або LF-125 кГц);
- високі частоти (ВЧ або HF-13,56 МГц);

LF (low frequency) - низькочастотні, робоча частота 125 КГц. Рідко це може бути 134,2 КГц. Відстань передачі інформації – від 1 до 50 см. LF мітки вважаються старим форматом, оскільки вони абсолютно не захищені і при запуску цієї технології використовувались тільки як теги. У низькочастотних картах не передбачено безпеку. Якщо вони потрапляють в електричне поле на низькій частоті, то модулюють постійний сигнал, який завжди передає завжди, яке можна списати і записати на іншу балванку, таким чином ми можемо отримати клон карти.

HF (high frequency) - високочастотне обладнання, робоча частота 13,56 МГц. Як і LF обладнання, відстань передачі сигналу і отримання відповіді від мітки може бути не більше 10 см. Перевагою RFID мітки 13.56 МГц є незалежна пам'ять EEPROM з захищеною областю, доступною для перезапису. Це забезпечує додатковий захист даних і дозволяє використовувати мітки у складних системах аутентифікації, а саме:

- Ідентифікація персон
- Платіжні системи
- Електронні ключі у готелях

- Авторизація користувача
- Посвідчення особи (паспорт)
- Підключення до wi-fi
- Карта для розрахунку за послуги
- Карти розрахунку в парках атракціонів, гральних автоматах

Високочастотні карти надійні, вони використовують APDU команди в залежності від стандарту, які використовують різні механізми для підтвердження будь-чого.

### 1.6. APDU

APDU (application protocol data unit) - це формат спілкування карти і терміналу. Термінал посилає Command APDU (C-APDU), а карта відповідає з Response APDU (R-APDU)

Для взаємодії з операційною системою Рутокен і його файловою системою є низькорівневий протокол, який реалізує підмножину стандарту ISO / IEC 7816-4 (Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange). Цей протокол оперує поняттям APDU (Application Protocol Data Unit) і складається з двох видів APDU: APDU-команда і APDU-відповідь. Ініціює обмін інформацією з токеном, відправляючи APDU-команду і чекаючи відповідь від іншого типу токена.

Інтерфейс рівня APDU забезпечує додаткам доступ до всіх функцій токенів. Саме додаток має виявляти токен, ініціювати транзакції, забезпечувати спільний доступ і т.д.

### 1.7. Клонування безконтактних карт

Це міф, який виник через те, що на початку інтегрування безпроводних технологій NFC/RFID у різноманітні прилади або у картки для перепусток, вони не призначались для інтегрування у банківські карти для оплати, тому їх стандарти та механізми роботи були дуже незахищеними, вони використовувались тільки як теги, але були присутні у різноманітних системах



контролю доступу. Вони до цих пір використовуються, оскільки ця технологія працює, але ніякої безпеки в ній не передбачено. Ці карти називаються картами старого формату, які працюють на низькій частоті і працюють від 120 КHz до 150 КHz. Низькочастотні карти вважають незахищеним, оскільки, при попаданні в електричне поле низької частоти, вони почнуть передавати усі данні, які записані на карті і ці дані можливо легко перезаписати на іншу безконтактну карту.

Високочастотні картки уже передбачали безпеку, і скопіювати їх було майже не можливо. До прикладу, популярний MifareClassic, який був провальною розробкою компанії NXP, через знайдену вразливість в RS втратах, яка дозволяла передбачити вихід генератора випадкових чисел, і саме через цю вразливість, можна було повністю скопіювати карту, оскільки маючи ключ, ми маємо доступ до пам'яті. Карта була досить прогресивною, оскільки використовувала нормальну схему аутентифікації, яка називається Challenge-response. І саме через це, з'явилася думка, що карти можна клонувати.



## РОЗДІЛ 2. СКІМІНГ. ЙОГО ПОНЯТТЯ ТА ПРИНЦИП ДІЇ

### 2.1. Скімінг

Скімінг - це вид кіберзагроз, який полягає в крадіжці банківських карт шляхом фізичного зняття інформації. З кожним роком технології стрімко розвиваються та інтегруються у роботу різноманітних сфер діяльності. Раніше скімінг представляв собою тільки крадіжку даних банківських карток, шляхом зняття даних через магнітну полосу на банківській карті, який давав змогу отримати усі необхідні її реквізити - ім'я власника, номер карти, термін закінчення терміну дії, CVV- і CVC-код, які шахрай використовує для своїх зловживань. Але з інтегруванням NFC технологій у банківські карти для безконтактної оплати, цей вид шахрайства розширився.

Безконтактні картки вважаються більш захищеними, оскільки відомості карти завжди залишаються при власникові, і їх непотрібно зчитувати, та вводити пін-код. Але у цьому криються і недоліки безпеки. Якщо користувач банку загубив свою карту, або її було викрадено, то зловмисник може оплачувати товари, не маючи жодної інформації про карту та її власника, але до тих пір, поки власник не заблокує карту. На даний момент потрібно вводити пін-код при оплаті вище 100 грн від MasterCard, та при платежі понад 500 грн системою Visa. Проте у більшості банківських додатків є налаштування щодо безконтактної оплати.

Оскільки при безконтактній оплаті карта підноситься впритул до терміналу, зчитати реквізити на відстані неможливо, тому це можна вважати ще одним рівнем захисту.

### 2.2. Скімінг безконтактних NFC та RFID приладів

Під час скімінг-атаки зловмисник таємно активує пасивний тег і спілкується з ним. Атака скімінгу завжди повинна бути активна, щоб антена генерувала частотне поле до тегу. Такий спосіб атаки обмежує максимальну відстань у порівнянні з атакою підслуховування. У скімінг-атаці потрібно знайти

баланс між поданням потужності сигналу для активації тега та дистанції відповіді. Це потрібно зробити по тій причині, що під час збільшення відстані активації тега, зменшується відстань його відповіді, оскільки під час збільшення активації тега генерується більше шумів сигналу, тому ускладнює виявлення реакції тегу.

Існує два види атак : активна та пасивна. Активна атака - скімінг пристрій має дві антени, де перша антена активує тег, а інша отримує відповідь від тега.

Пасивна атака реалізовується єдиною антеною, яка виконує тільки функцію підслуховування. Зловмиснику не доводиться жити тег, він лише слухає комунікацію.

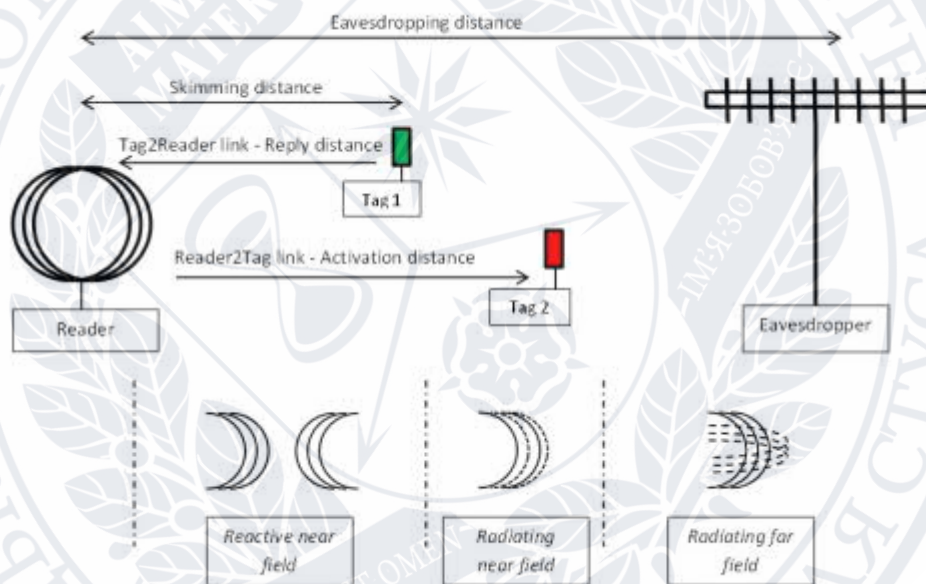


Рис. 2.1. Схема скімінг атаки

### 2.3. Робота безконтактної оплати

Чіпи NFC використовуються не тільки в мобільних пристроях в режимі емуляції карти, але і в самих пластикових картах, для можливості безконтактної оплати, і ще у понад десяти інших пристроях з можливістю емуляції вашої карти, типу кільця або браслета з вбудованим чіпом NFC.



Рис.2.2. Этапы прохождения платжной транзакції.

У разі використання контактної карти, в її чіп зашивається платіжний додаток банку-емітента, який через платіжну систему взаємодіє з банком-еквайєром продавця при проведенні платіжної транзакції, і персональні платіжні дані клієнта банку, на чие ім'я випущена карта. Дані зберігаються в зашифрованому вигляді криптоключа і захищені від перезапису або зміни.

Стандартна EMV транзакція проходить в кілька етапів, я опишу повний алгоритм взаємодії у разі контактної інтерфейсу, для безконтактного інтерфейсу алгоритм декілька скорочений:

- Як вибрати програму;
- Ініціалізація обробки додатка;
- Зчитування даних програми;
- Офлайн аутентифікація;
- Обробка обмежень;
- Перевірка власника картки;
- Ризик-менеджмент на стороні терміналу;
- Аналіз дій терміналу;
- Ризик-менеджмент на стороні карти;
- Аналіз дій карти;
- Процесинг в режимі on-line;
- Завершення операції.



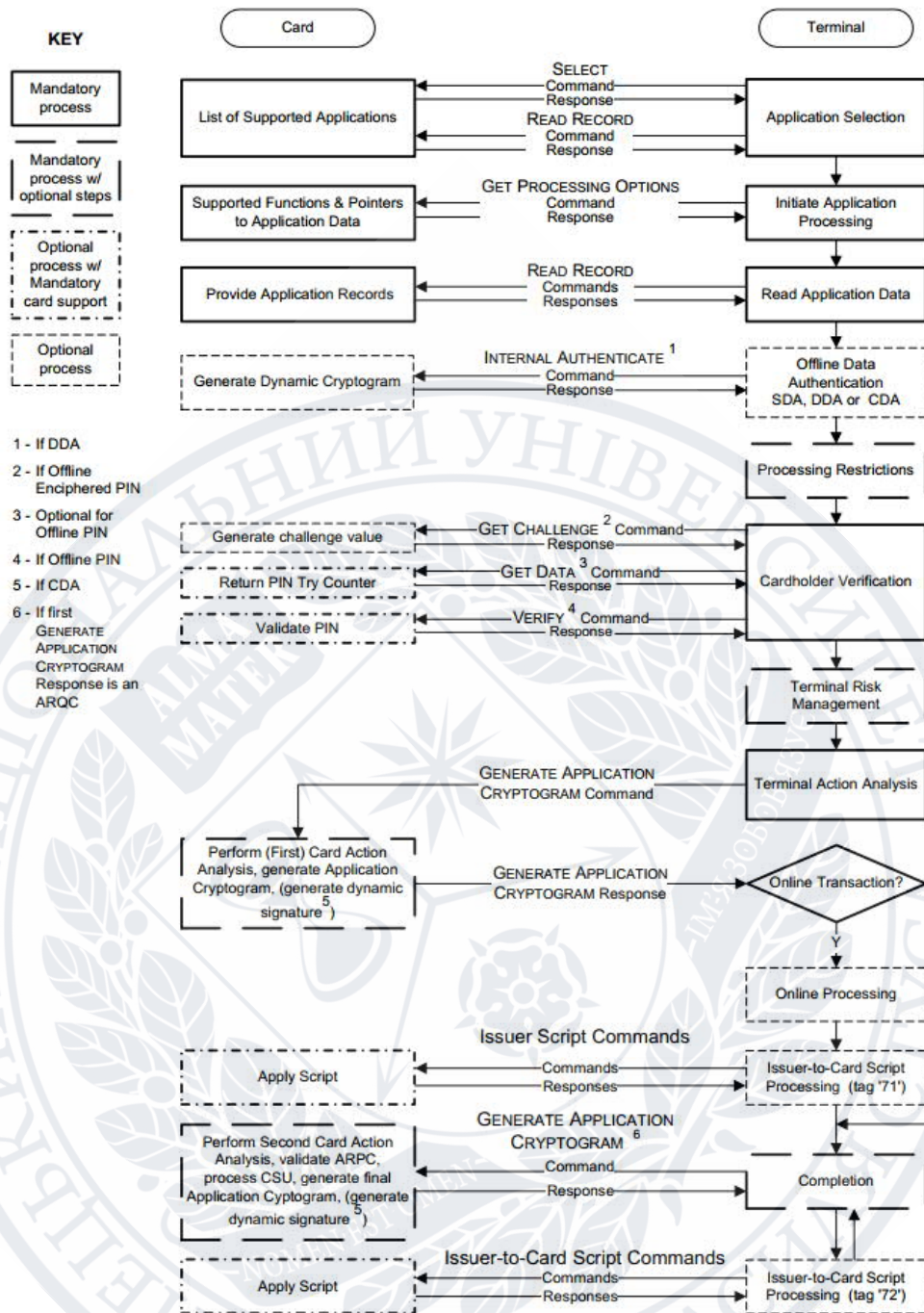


Рис 2.3. Етапи Проходження оплати за допомогою безконтактної банківської карти

## 2.4. Реалізація безпеки безконтактної банківської карти. Чому її неможливо скопувати?

EMV стандарт працює від APDU протоколу, в карті знаходиться чіп, який являє собою маленький комп'ютер, цей комп'ютер може здійснювати кількість обмежених операцій, і в основному це стосується криптографії. Чіп генерує пару



RSA і приватний ключ, який зберігається всередині чіпа та ніколи його не покидає, коли карту випускає банк, він запускає операцію генерування цих ключів, та запис деякої мета-інформації, після чого витягує публічний ключ, і цей публічний ключ, підписує своїм центром сертифікації, після чого підписаний вже сертифікат карти, зберігається на саму карту. Це потрібно для того, щоб термінали, які володіють публічним ключем банку емітента карти могли перевіряти первинні операції з карти не звертаючись в мережу, тобто, у них є публічні ключі банківського СА, тому вони можуть це робити.

Коли до терміналу прикладають карту, він живить її енергією, після чого, він починає перебирати платіжну систему з якою працює карта, цей процес називається вибір додатка. У кожної карти свій AID з єдиним форматом, але це в тому випадку, якщо ми говоримо про стандарт EMV. Після того як термінал підтвердив, що він працює з цією платіжною системою на картці, вони починають спілкування, у цей час, термінал формує подол, це об'єкти, схожі на данні типу JSON або XML, але там свій бінарний формат, вони описують ідентифікатори:

- Суму;
- Валюту;
- Деяку інформацію про термінал, та клієнта картки.

Після чого карта повинна його підписати. Платіж заключається не в передачі якоїсь інформації, або перерахунку коштів, а це по суті операція цифрового підпису, і там нічого не можна перехопити при спілкуванні, оскільки приватний ключ карту ніколи не покине, ніяких можливостей скопіювати її немає, все що передається - це подол, який не являється нічим секретним. Коли термінал отримує підписаний подол, він відправляє його через екваєр банк емітент і вже там відбувається підтвердження операції.

## **2.5. Процес емулявання карти мобільним телефоном**

Що ж відбувається в разі емулявання карти мобільним телефоном. Щоб не записувати на чіп SE в мобільному пристрої платіжні додатки всіх

банківських карт, якими користується власник пристрою, які до того ж треба персоналізувати, тобто передати дані про випущених картах і зберігати їх в захищеному вигляді, була сформульована роль TSM (Trusted Service Manager), який об'єднує з одного боку постачальників послуг (Service Provider TSM), а з іншого боку чіпи Secure Element (Secure Element Issuer TSM).

TSM - Trusted Service Manager - унікальний посередник, який володіє ключами. Це апаратно-програмний комплекс, що надає технологічні відносини між операторами зв'язку і постачальниками послуг.

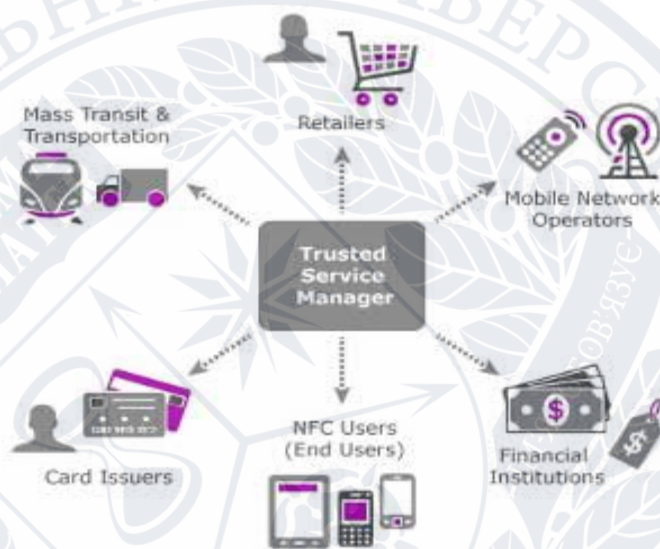


Рис. 2.3. . Trusted Service Manager

Trusted Service Manager або TSM - довірений постачальник послуг. Виконує захищену завантаження і менеджмент контенту захищеного елемента (SE) для транспортних додатків, магазинів, мобільних операторів, банківських додатків, конфіденційні дані власника картки.

Термін скімінгу передбачає собою знаття дублікату магнітної смужки, який зловмисник таємно зчитує інформацію на магнітній смужці, а потім можна зробити її копію, яку неможливо відрізнити від оригіналу. Для тегів RFID або NFC, зловмисник не може створити скімінг-атаку, Оскільки ця технологія використовує певну форму відповіді. Але через вразливість EMV, можна отримати певні реквізити карти, які в майбутньому можна використовувати для зловживань.

## **2.6. Зчитування даних безконтактних карток**

Зчитування даних EMV можливо тільки через безконтактні банківські карти, оскільки вони відкрито надають інформацію через специфікацію стандарту EMV.

Достатньо завантажити додаток "Зчитувач банківських карт" у Плей Маркеті, аби провести експеримент зі зчитування даних. Різницею між цілеспрямованими пристроями для зчитування даних карт є те, що найчастіше у пристрої встановлені додаткові антени для сканування більшої дистанції даних.

Сканувати дані віртуальної картки з телефона - неможливо, оскільки система передачі даних працює більш в закритому доступі. Віртуальні карти на смартфонах з NFC, набагато безпечніше використовувати, оскільки:

- Не дозволяє зчитувати данні до авторизації
- Не розриває дані про власника
- Авторизовує лише одну транзакцію

Не дозволяє зчитувати дані до авторизації, коли телефон з додатком для оплати потрапляє в поле дії зчитувача (13,56 МГц), користувачеві пропонується авторизуватися, і тільки після успішної авторизації телефон починає виявлятися як безконтактна картка. До цього моменту зчитувач не бачить нічого.

## **2.7. Вразливість у банківських карток, які використовують NFC технологію**

Оскільки стандарт EMV допускає зберігання в пам'яті чіпа карти даних в незашифрованому вигляді, до таких даних можуть додаватися номер карти, термін її дії, кілька останніх здійснених операцій і т.д. Яка саме інформація і як зберігається у чіпі, визначають платіжна система і банк-емітент. Ці дані можна вважати навіть за допомогою звичайного смартфона, встановивши на нього цілком легальне додаток (наприклад, Banking card reader NFC). Незважаючи на те, що ця відкрита, здавалося б, інформація не ставить під загрозу безпеку карти, реальність така, що все частіше багато інтернет-магазини перестали вимагати CVV2 / CVC2-код карти, який потрібно для онлайн-покупки.



## **2.8. Види атаки**

Так, у першому випадку зловмисники крадуть кошти через шахрайський мобільний POS-термінал або спеціальний пристрій, який створить фейковий покупку і «змусить» карту жертви її оплатити. Однак такий спосіб має деякі обмеження, наприклад, зловмисникові потрібно мати рахунок в банку, оформлений на юрособу, і платіжний термінал, зареєстрований в податковій інспекції. Крім того, через скарги клієнтів рахунок найімовірніше заблокують до того, як шахраї встигнуть отримати гроші.

Другий спосіб - зчитування даних карти, її номера та терміну дії спеціальних NFC-скімерів (пристрій для зчитування даних з безконтактних карт) для подальшої спроби шахрайства з операціями без карти.

## **2.9. Види захисту проти хакерської атаки на безконтактну картку**

Найпростіший і найдієвіший спосіб захисту карти від безконтактного рідера - носити її разом з іншими безконтактними картами, наприклад, з транспортної карткою або навіть інший банківською карткою. При спробі зчитування даних апарат шахраїв не зможе правильно скопіювати інформацію, так як вхідний сигнал буде направлятися одночасно з декількох карт і він буде опрацьовано некоректно.

Також можна придбати спеціальне портмоне blocking RFID wallet з захистом від зчитування. Також рекомендується підключити СМС-повідомлень або PUSH-повідомлень вашого банку, для моніторингу транзакцій. Як варіант можна ще зменшити розмір суми, яку можна використовувати при оплаті картою без вказівки PIN-коду.

Більш безпечнішим спосіб вважається використання безконтактної оплати через телефон. Оскільки функція безконтактної оплати доступна, коли в смартфоні активна система Розрахуватись через телефон, можна буде тільки після того, як користувач авторизується в систему.



Смартфон як засіб платежу - ще один спосіб захисту від NFC-шахрайства. Це коли замість картки використовують телефон, тобто мобільне програмне додаток, прив'язане до рахунку карти. З еї допомогою мобільного пристрою з підтримкою безконтактних платежів передає дані про платіжну операції через канал, захищений за допомогою шифрування. Дані зберігаються в пам'яті смартфона або планшета. Така модель значно знижує ймовірність симуляції NFC-платежу і перехоплення даних зловмисниками. Якщо користувач не розблокував смартфон і не активував мобільний додаток, до якого прив'язана карта, атака з використанням ретрансляції неможлива. Хоча і носії NFC теж уразливі, адже самі по собі гаджети не захищені. Не гарантують 100% безпеки і приймають пристрою: POS-термінали, банкомати, які також можуть бути заражені шкідливим програмним забезпеченням. Всі перераховані загрози стосуються не тільки найпопулярніших карткових NFC-технологій PayWave і PayPass від платіжних систем Visa і MasterCard, а й систем, випущених на ринок мобільними операторами, таких як Vodafone Pay і "Смарт-гроші" ( "Київстар"), а також програмних рішень Apple Pay і Google Pay (G Pay), які отримали останнім часом широке поширення.

## **2.10. Що безпечніше: смартфон або карта?**

Оплата безконтактною картою і смартфоном практично однакова. Різниця полягає в невеликих технологічних відмінності, що стосуються реалізації NFC (ближня безконтактна зв'язок - ред.) в телефоні.

Оплата смартфоном навіть безпечніше, оскільки для кожного платежу в цьому випадку генеруються одноразові платіжні дані, і справжній номер вашої банківської карти не передається на банківський термінал. Але потрібно бути уважними, адже в разі втрати телефону, що не захищеного паролем, у його нових власників з'являється шанси отримати як інформацію, збережену на ньому, так і ваші гроші», - попереджає експерт.

Утім, за її словами, і платіжні сервіси, і банки, і виробники терміналів, смартфонів дбають про безпеку проведення транзакцій. Так, наприклад, на iPhone не можна провести безконтактну оплату без введення пароля.

Сьогодні реальність така, що навіть незважаючи на технологію з хорошою багатофакторної захистом, 100% гарантію захисту грошових коштів ніхто не дасть. Занадто багато все залежить ще й від додаткових налаштувань торгових точок, а також від персоналу, який приймає картки для платежів, не дотримуючись інструкції з безпеки.

Смартфон як засіб платежу - ще один спосіб захисту від NFC-шахрайства. Це коли замість картки використовують телефон, тобто мобільне програмне додаток, прив'язане до рахунку карти. З еїї допомогою мобільного пристрою з підтримкою безконтактних платежів передає дані про платіжну операції через канал, захищений за допомогою шифрування. Дані зберігаються в пам'яті смартфона або планшета. Така модель значно знижує ймовірність симуляції NFC-платежу і перехоплення даних зловмисниками. Якщо користувач не розблокував смартфон і не активував мобільний додаток, до якого прив'язана карта, атака з використанням ретрансляції неможлива. Хоча і носії NFC теж уразливі, адже самі по собі гаджети не захищені. Не гарантують 100% безпеки і приймають пристрою: POS-термінали, банкомати, які також можуть бути заражені шкідливим програмним забезпеченням. Всі перераховані загрози стосуються не тільки найпопулярніших карткових NFC-технологій PayWave і PayPass від платіжних систем Visa і MasterCard.

Підсумовуючи, зараз можна говорити, що сучасні технології частіше перемагають шахраїв. Також, суттєво знизився відсоток неписьменності самих користувачів, проте фахівці стверджують, що це заслуга гаджетів і встановлених додатків. Саме лінь користувачів стали в цьому питанні двигуном прогресу, адже прикласти до зчитувача смартфон набагато простіше, ніж шукати карту, забивати дані, перевіряти реквізити.

Сьогодні реальність така, що навіть незважаючи на технологію з хорошою багатофакторним захистом, 100% гарантію захисту грошових коштів ніхто не

дасть. Занадто багато все залежить ще й від додаткових налаштувань торгових точок, а також від персоналу, який приймає картки для платежів, не дотримуючись інструкції з безпеки.



## РОЗДІЛ 3.

### 3.1. Збільшення відстані атаки

Одним з обмежуючих факторів для досягнення більших відстаней зв'язку є необхідну потужність для картки. Картки пасивні, тобто вони не мають акумулятора, тому їм потрібне сильне колювання магнітного поля для живлення. Але а потужна антена для активації картки на великій відстані генерує багато шуму, що ускладнює отримання відповіді картки. Тут ми досягаємо головного вдосконалення, використовуючи резонансну котушку як 3-ю гармонічну антену для прийому.

У роботі розглянемо різні види атак на NFC та RFID приладів, та детально проаналізуємо можливості збільшення відстані, на якій можна буде підслухати, або здійснити активацію пристрою з NFC-зв'язком.

### 3.2. Збільшення діапазону атаки на RFID або NFC приладів за допомогою вищої гармоніки

В середині смарт-картки є діодний міст, який в свою чергу складається з нелінійних діодів. Будь-який нелінійний пристрій генерує вищу гармоніку сигналу, який на нього надходить. Оскільки обмін даних проходить на частоті 13.56 МГц, то можна реалізувати підсилення сигналу на вищій гармоніці.

Порядок гармонік - це число раз, в яке частота гармонічної складової перевищує значення основної частоти: 1,2,3,4,5. Порядок може бути визначений як відношення частоти гармонік ( $n$ ), до основної частоти.

Обмежуючим фактором при спілкуванні RFID/NFC мітками є її не активація, а отримання його відповіді. Оскільки більша потужність приводить до зменшення індексу модуляції, та сигналу до шуму (SNR), що призводить до



меншого впливу отримання сигналу. Тому для роботи використовується дві антени:

- 1) для активації мітки
- 2) друга для прийому відповіді.

За допомогою двох різних антен, які налаштовані на дві різні частоти, можна розробити скімер. Перша антена працює на частоті 13.56 мГц і виконує роль активації мітки. Друга антена налаштована на частоту 40.68 мГц, яка підсилює відповідь 3-ю гармоніки і отримує відповідь.

### 3.3 Несанкціоноване отримання даних

Є два основні варіанти несанкціонованого отримання даних з тегу (картки чи іншого пристрою RFID) – це підслуховування (рис. 1, а) чи скімінг

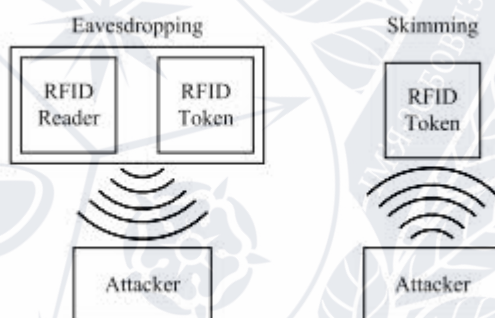


Рис. 3.1. атака скімінгу та прослуховування

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. Відстані, на яких це можливо здійснити, дають можливість розташувати антенні системи у стиснених умовах непомітно для власника картки.

### 3.4 Підготовка обладнання для імітатора NFC-зв'язку

Для реалізування рідера були вибрані пристрої такі як, Arduino Nano (рис.3.2.), та RFID-RC522 (Рис. 3.3.)

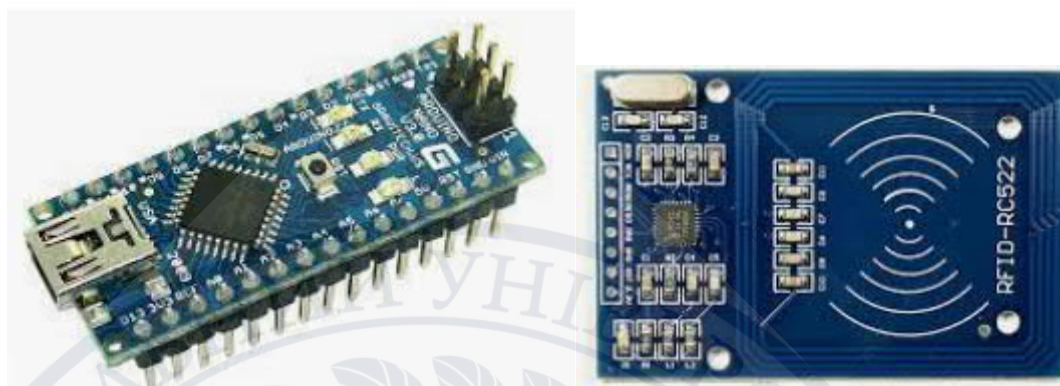


Рис. 3.2 Arduino Nano та Рис. 3.3 RFID-RC522.

Для Arduino Nano була використана програма [1], яка могла взаємодіяти з пристроєм RFID-RC522, та могла працювати з картками Mifare Classic (1k, 4k, mini). Рідер міг 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. На (рис. 3.4.), показано спектри без картки (нижня частина) та з карткою (верхня спектрограма), тому і сигнал цієї частоти можна використовувати для отримання інформації про картку.

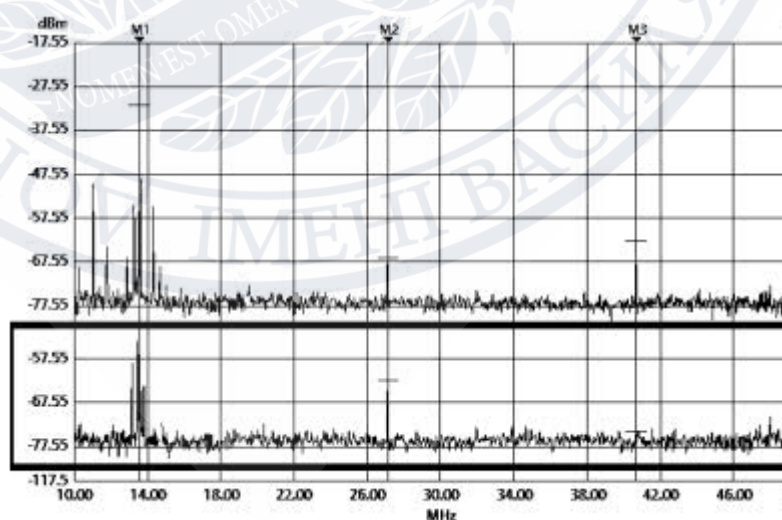


Рис. 3.4. Спектри з карткою та без

Роботи проводились з картою NXP MIFARE Classic 1k, яка працювала по стандарту ISO 14443-3A. Оскільки 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 за кодовані 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. Зворотний канал повинен бути в діапазоні 424 кГц, зосередженим близько 847,5 кГц. Прямий канал амплітудно модулюється на 13,56 МГц з індексом модуляції 100 %, тоді як зворотний канал має індекс модуляції 8 - 12 %.

### 3.5 Реалізація антени на частоту третьої гармоніки та вимірювання відстані

Для скімінг пристрою була виготовлена резонансна магнітна антена у вигляді кільцевого вібратора, для прийому сигналу на частоті 40,68 МГц. Антена навантажується навантажений на ємність та узгоджується з лінією

50 Ом за допомогою гамма-узгодження. Антена має діаметр 77 см та виготовлена з алюмінієвого обручу (рис.3.5.).

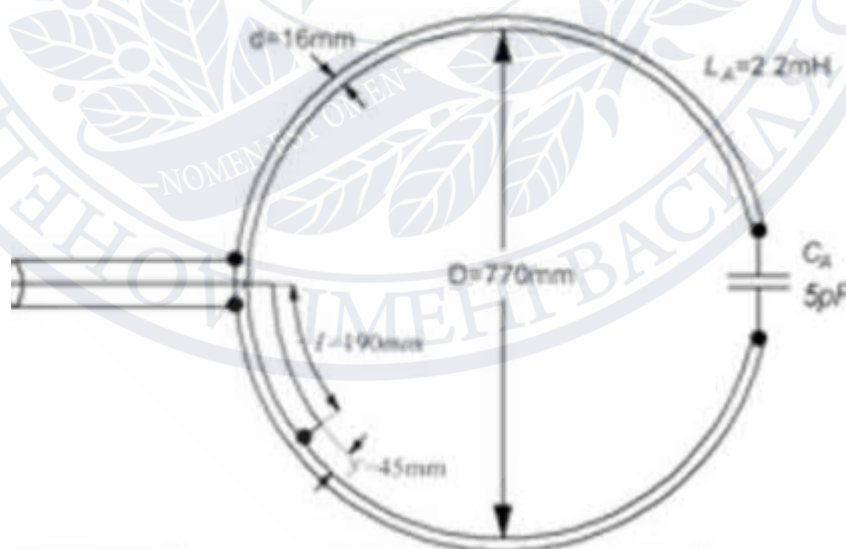


Рис. 3.5. Схема антени

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. При експлуатації антени, завжди виміряли залежність сигналу картки в діапазоні частоти третьої гармоніки від відстані між картою та приймальною антеною. Карта та антена були розташовані на одній горизонтальній осі.

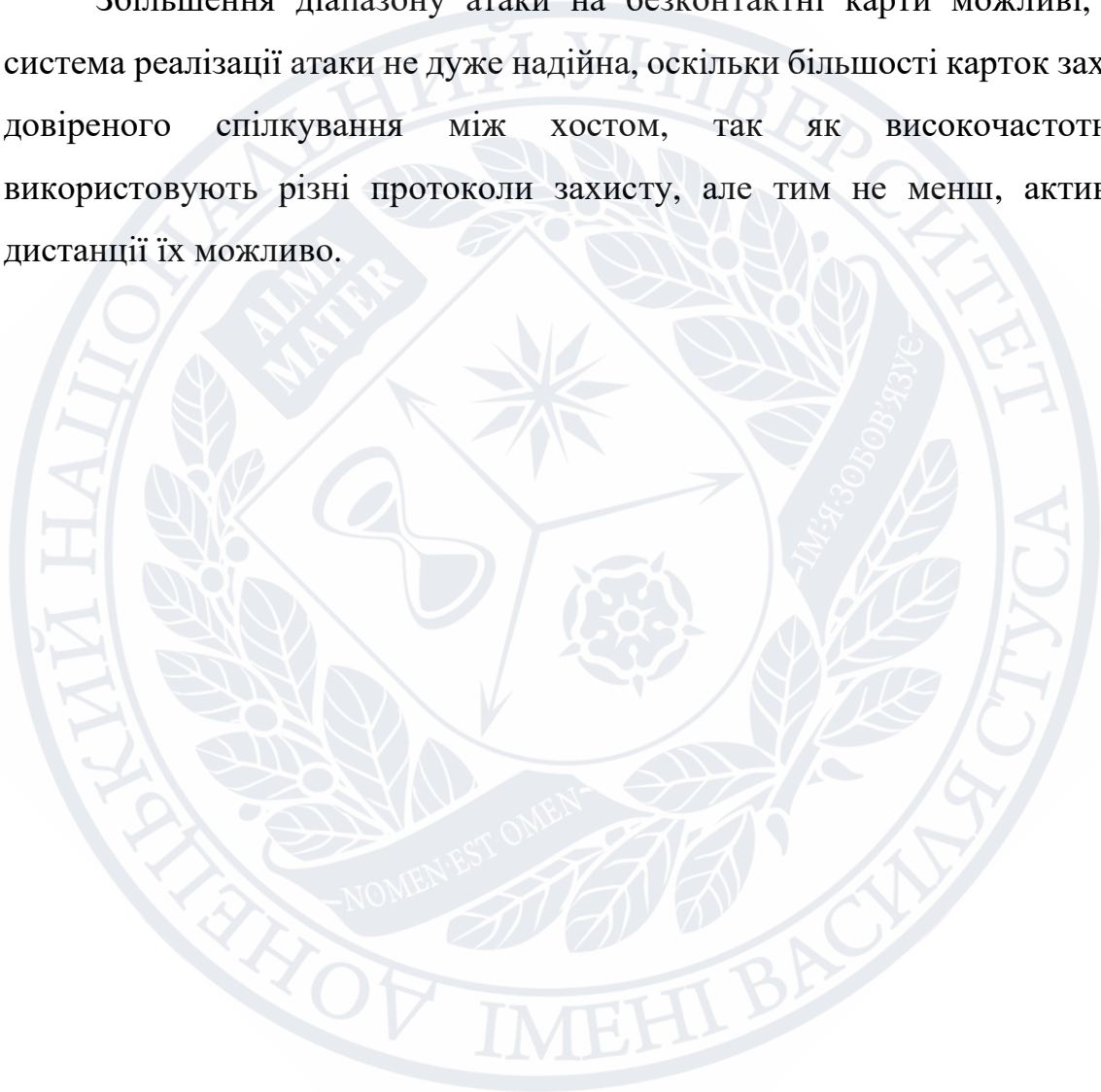




## ВИСНОВОК

Безконтактні платіжні системи досить надійно захищені. Незважаючи на теоретичну можливість шахрайства, на практиці вона виявляється нерентабельна і вкрай важко здійснена. Немає ніякої причини боятися безконтактних карт або взлому антени в карті.

Збільшення діапазону атаки на безконтактні карти можливі, але сама система реалізації атаки не дуже надійна, оскільки більшості карток захищені від довіреного спілкування між хостом, так як високочастотні карти використовують різні протоколи захисту, але тим не менш, активувати на дистанції їх можливо.



## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hancke, G.P.: Practical attacks on proximity identification systems. In: IEEE Symposium on Security and Privacy (S&P'06). pp. 328–333. IEEE (2006)
2. Hancke, G.P.: Practical eavesdropping and skimming attacks on high-frequency RFID tokens. J. Comput. Secur. 19(2), 259–288 (2011)
3. ISO/IEC: ISO/IEC 14443-3:2011, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision (2011)
4. NFC в телефоні [Електронний ресурс] – Режим доступу до ресурсу: <https://www.moyo.ua/ua/news/nfc-v-smartfone-chto-eto-i-kak-rabotaet-3-glavnykh-sekreta-tekhnologii.html>.
5. Що таке NFC [Електронний ресурс] – Режим доступу до ресурсу: <https://marketer.ua/ua/what-is-nfc-and-how-to-use-this-technology/>
6. Як працює NFC [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.easypay.ua/uk/shho-take-nfc-i-yak-tse-pratsyuue/>.
7. Зчитувач RFID [Електронний ресурс] – Режим доступу до ресурсу: [https://arduino-kit.ru/blogs/blog/project\\_28](https://arduino-kit.ru/blogs/blog/project_28).
8. Радіочастотна ідентифікація [Електронний ресурс] – Режим доступу до ресурсу: <https://www.pharmencyclopedia.com.ua/article/6776/radiochastotna-identifikaciya>.
9. Захист даних RFID [Електронний ресурс] – Режим доступу до ресурсу: <https://lockers.com.ua/scho-take-rfid-i-jak-zahistiti-svoji-dani-i-groshi-vid-shahrajiv/>
10. ФНК [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: <https://football.kulichki.net/>.
11. MIFARE Classic® EV1 1K - 4K [Електронний ресурс] – Режим доступу до ресурсу: [https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-classic/mifare-classic-ev1-1k-4k:MF1S50YYX\\_V1](https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-classic/mifare-classic-ev1-1k-4k:MF1S50YYX_V1).

12. Слабкий захист карт [Електронний ресурс] – Режим доступу до ресурсу: <https://www.neftocard.ru/articles/mifare/zayavlenie-o-slabosti-zashchity-kart-mifare-classic.php>.

