

**Шпортко Олександр Володимирович**, к.т.н., доцент, доцент кафедри інформаційних систем та обчислювальних методів, **Мушин Марія Михайлівна**, студентка 1 курсу спеціальності «Інженерія програмного забезпечення» (Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука), ITShportko@ukr.net

## МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПОВЕДІНКИ РУХОМИХ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ NFC

Технологія безконтактної оплати смартфоном впевнено увійшла в наше життя. Найчастіше вона використовується в торгівлі та при оплаті послуг громадського транспорту. На основі цієї ж технології, що має назву NFC, працюють розумні банківські картки [1], а також багато інших пристроїв Інтернету речей.

NFC (Near Field Communication, комунікації ближнього поля) – це технологія безпроводного зв'язку малого радіуса дії. Вона працює на відстані до 10 см з частотою 13,56 МГц за допомогою електромагнітного поля [2]. Цей вид безпроводного зв'язку відрізняється від Wi-Fi та Bluetooth надшвидким встановленням з'єднання [3] та меншим радіусом дії [2], що зменшує ймовірність перехоплення сигналу [4].

NFC-зв'язок може працювати у двох режимах. У режимі активного зв'язку (перший режим) як ініціатор, так і цільовий пристрій взаємодіють по черзі генеруючи власне поле. Пристрій дезактивує своє радіочастотне поле під час очікування відповіді. У цьому режимі як ініціатор, так і ціль, як правило, повинні мати джерело живлення [2]. При пасивному зв'язку (другий режим) пристрій-ініціатор створює електромагнітне поле, а цільовий – відповідає на нього. У даному режимі цільовий пристрій може отримати свою робочу потужність з електромагнітного поля, наданого ініціатором, після чого відповісти йому на іншій частоті.

Зазвичай взаємодія відбувається між двома пристроями. Якщо їх більше, то пристрій-ініціалізатор обирає одну ціль з усіх доступних і тільки вона відповідає на його сигнал. З'єднання можуть проходити хіба що по черзі [4]. Саме тому безконтактна оплата можлива лише між двома пристроями, що підтримують технологію NFC. Ініціатором проведення оплати може виступати банківська картка, смартфон, телефон, планшет або смарт-годинник, а реагує на запит термінальний пристрій. Операція здійснюється завдяки вбудованому чіпу без використання камери, дротів,

сканерів чи введення спеціальних кодів захисту. NFC не розряджає батарею та не потребує обслуговування з боку користувача [1].

Також ця технологія використовується для організації взаємодії з пасивним фізичним NFC-тегом. Ним може бути радіочастотний RFID-ярлик або брелок. У цих пристроях міститься електросхема, куди можуть бути записані прості команди, які активуються при фізичному контакті. Таким чином автоматизуються відкриття заданої інтернет-адреси, введення паролю, розблокування електронних замків, послідовний запуск встановлених на смартфон додатків тощо. Команди для них обираються зі встановленого спеціального додатка на смартфоні [5].

NFC використовується також для безпроводної зарядки невеликих пристроїв Інтернету речей, таких як гарнітура Bluetooth, фітнес-трекер або смарт-годинник. При цьому потужність зарядки становить 1 В. Також, використовуючи NFC, два пристрої можуть обмінюватися даними. Для цього застосовується протокол однорангової мережі Peer-to-Peer і в передачі даних беруть участь два пристрої, які між собою рівноправні та можуть як отримувати, так і відправляти файли. У цьому випадку не використовується сервер, на якому би тимчасово зберігалися дані, а їх відправлення відбувається безпосередньо [1]. Так можна здійснювати обмін різною інформацією, наприклад, віртуальними візитками або цифровими фотографіями. Для передачі даних великого розміру краще спочатку встановити зв'язок між пристроями через NFC, оскільки це відбудеться швидко та без додаткових введень паролів, а після цього вже передати керування Bluetooth або WiFi, адже це забезпечить вищу швидкість передачі даних [2].

Технологію комунікацій ближнього поля використовують також при розробці багатокомпонентних систем. Наприклад, NFC-теги використовують для боротьби з торгівлею підробленими товарами шляхом створення захищеного цифрового ідентифікатора та зчитуванні вмісту тегу. В компанії «Touch and Discover» автоматизували управління персоналом готелю. Тепер клієнти записують у NFC-теги свої прохання персоналу, який може їх виконати, незважаючи навіть на мовний бар'єр [1].

Розглянемо ще один приклад. EWaterPay – це смарт-технологія розумного контролю дозатору подачі води. Основною її перевагою є відстеження доходу за обслуговування. У ній використовуються NFC-теги для замовлення води за мобільні гроші та в кредит. Вона дозволяє дарувати кошти на воду віддаленим користувачам [6]. Є й інші розробки з використанням NFC [1].

Технологія NFC підпорядковується міжнародним стандартам з метою забезпечення сумісності та працездатності пристроїв, що її підтримують [7]. Підтримкою технології займаються різні організації [1; 7].

Наведений опис технології NFC засвідчує, що вона дозволяє фіксувати положення рухомих об'єктів в момент взаємодії з пристроєм, що здійснює контроль. Причому навіть в місцях скупчення багатьох об'єктів NFC може ідентифікувати їх послідовно. Це дає змогу моделювати траєкторії руху цих об'єктів між моментами фіксації та прогнозувати їх подальші переміщення.

Узагальнюючи сказане, приходимо до висновків, що технологія комунікацій ближнього поля NFC є актуальною, спрощує та пришвидшує встановлення мережевих зв'язків, дозволяє автоматизувати повторювані дії, широко застосовується сьогодні, має перспективи розвитку в майбутньому та може ефективно використовуватися для математичного моделювання поведінки рухомих об'єктів.

### **Список використаних літературних джерел**

1. NFC Forum. [nfc-forum.org](https://nfc-forum.org): офіційний сайт. URL: <https://nfc-forum.org> (дата звернення: 08.12.2019).
2. Ecma International. [ecma-international.org/activities/Communications/2004tg19-001.pdf](https://www.ecma-international.org/activities/Communications/2004tg19-001.pdf) (дата звернення: 08.12.2019).
3. Исхаков А. Ю. Недостатки NFC-меток при аутентификации. *Ползуновский вестник*. 2013. № 2. С. 267–269.
4. Haselsteiner E., Breitfuß K., Philips Security in Near Field Communication (NFC). Strengths and Weaknesses. Workshop on RFID Security, 2006.
5. Wakdev. [Wakdev.com](https://www.wakdev.com/en/apps/nfc-tools/faq-nfc-tools-english.html): офіційний сайт. URL: <https://www.wakdev.com/en/apps/nfc-tools/faq-nfc-tools-english.html> (дата звернення: 09.12.2019).
6. Ewaterpay. [ewaterpay.com](https://www.ewaterpay.com/how-it-works/): офіційний сайт. URL: <https://www.ewaterpay.com/how-it-works/> (дата звернення: 08.12.2019).
7. Gsma. [Gsma.com](https://www.gsma.com/digitalcommerce/wpcontent/uploads/2012/03/gsmarequirementsforswpnfchandsetsv4.pdf): офіційний сайт. URL: <https://www.gsma.com/digitalcommerce/wpcontent/uploads/2012/03/gsmarequirementsforswpnfchandsetsv4.pdf> (дата звернення: 09.12.2019).