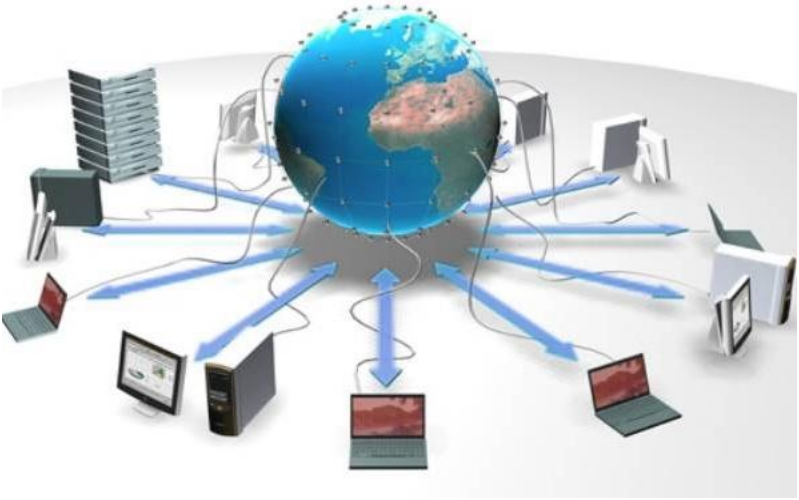
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ І УПРАВЛІННІ»

ЗБІРНИК НАУКОВИХ СТУДЕНТСЬКИХ ПРАЦЬ

ВИПУСК 5



Одеса
2023

БЕЗПЕКА NFC-ТРАНЗАКЦІЙ В УМОВАХ ЗРОСТАЮЧОГО ПОПИТУ НА БЕЗКОНТАКТНІ ПЛАТЕЖІ

Маркова О.[1], Гострик О. М.[2]

1 – студентка 4 курсу 48 гр., факультет економіки та управління підприємництвом,
2 – канд. екон. наук, професор, кафедра економічної кібернетики та інформаційних технологій
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Маркова О., Гострик О. М. ***Безпека NFC-транзакцій в умовах зростаючого попиту на безконтактні платежі.*** *Стаття присвячена безпеці NFC-транзакцій в умовах зростаючого попиту на безконтактні платежі. Висвітлено проблеми безпеки безконтактних платежів та технологію, що лежить в основі цих платежів. Показано розвиток технологій, що сприяють зростанню популярності безконтактних платежів у всіх їх формах, та зручність їх використання.*
Ключові слова: *NFC, безконтактні платежі, транзакція, безпека, автентифікація, токенізація.*

Markova O., Hostryk O. ***Security of NFC transactions in the face of growing demand for contactless payments.*** *The article is devoted to the security of NFC transactions in the context of growing demand for contactless payments. The security problems of contactless payments and the technology underlying these payments are highlighted. The development of technologies that contribute to the growing popularity of contactless payments in all their forms and the convenience of their use are shown.*
Keywords: *NFC, contactless payments, transaction, security, authentication, tokenization*.

Маркова О., Гострик О. М. Безпека NFC-транзакцій в умовах зростаючого попиту на безконтактні платежі. *Інформаційні технології в економіці і управлінні* : зб. наук. студ. праць. Одеса : ОНЕУ, 2023. Вип. 5. С. 131–136.

Постановка проблеми у загальному вигляді. Розвиток технології Near Field Communication (NFC) уможливив появу платіжних послуг з використанням мобільних телефонів. Крім того, ця технологічна інновація започаткувала постійну еволюцію платіжних операцій. Компанії та дослідники прогнозують, що основна функція кредитних карток буде поступово замінена мобільними пристроями.

Аналіз досліджень і публікацій останніх років. Аналіз наукової літератури показав, що проблеми безпеки безконтактних платежів були розглянуті в наукових публікаціях таких вчених, як: В. В. Гірняк, Т. Р. Кулик, В. Некрасов, О. Постіпух, Е. Філатова та ін. Серед закордонних вчених, що займалися цієї проблемою: Паскаль Урієн, Чен Сі, Вакар Анвар, Дейл Ліндског, Рон Руль, Янг Чен та ін.

Виділення невирішених раніше частин загальної проблеми. Не зважаючи на кількість наукових досліджень з приводу цього питання, ця тема залишається актуальною, адже існує проблема безпеки безконтактних платежів. З'являються нові методи, способи та тенденції більшого впровадження системи безконтактних платежів як в повсякденне життя, так і на підприємствах.

Мета статті. Головною метою статті є дослідження проблеми безпеки безконтактних платежів та технології, що лежить в їх основі.

Виклад основного матеріалу дослідження. Безконтактні платежі являють собою популярний вид платіжних технологій, який робить розрахунки готівкою або проведенням картками по терміналу, застарілими. На касі клієнт може здійснити безконтактну транзакцію, доторкнувшись карткою або мобільним пристроєм до платіжного терміналу.

Щоб приймати безконтактні транзакції, торговець повинен мати сумісні POS-системи з підтримкою NFC. Крім того, продавці можуть використовувати рішення SoftPOS. Встановивши додаток SoftPOS, власники бізнесу можуть перетворити власні смартфони в POS-термінали і приймати безконтактні платежі.

Незважаючи на те, що в процесі безконтактної оплати беруть участь кілька сторін (банки-еквайрингові компанії, платіжні схеми та банки-емітенти), платіжний термінал дозволяє всім їм підключатися, і транзакція завершується за лічені секунди. Весь процес має на меті зменшити черги, покращити досвід касового обслуговування як для споживача, так і для продавця, а також зменшити передачу COVID-19, оскільки немає необхідності торкатися готівки.

Форми безконтактних платежів включають в себе безконтактні платежі картками, що використовують технологію RFID та безконтактні мобільні платежі, які потребують наявність мобільного пристрою – смартфона, смарт-годинника або іншого пристрою з підтримкою NFC. В їх основі лежить технологія зв'язку ближньої дії. Пристрої з підтримкою NFC можуть зв'язуватися один з одним за допомогою радіочастот та обмінюватися даними.

Ліміти безконтактних платежів були підвищені в 29 європейських країнах, що охоплюють більшу частину регіону. Нові ліміти варіюються в залежності від країни, частково через різні валюти, але більшість з них прийняли ліміт від 40 до 60 євро [5].

Одною з потенційних небезпек можна виділити крадіжку банківських карток (в середньому 4 з 10 крадіжок пов`язані з крадіжкою банківських

карток). Клієнтам рекомендується обирати більш безпечні безконтактні мобільні платежі. Вони вимагають або верифікації PIN-коду, або біометричної ідентифікації, тому стають марними в разі крадіжки. В Україні понад 90% громадян користуються смартфонами.

Впровадженню безконтактних платежів також перешкоджає стійке сприйняття того, що мобільні гаманці недостатньо безпечні. Майже половина американських споживачів вважають, що якщо зловмисник заволодіє їхнім телефоном, вони втратять свою конфіденційну інформацію. Провайдери платіжних послуг повинні докладати більше зусиль, щоб запевнити споживачів, що мобільні гаманці є безпечнішими, ніж традиційні банківські інструменти.

Ще одне занепокоєння у споживачів викликає те, що мобільні платежі не працюють, коли вони потрібні, і багато людей (41%) вважають за краще носити з собою вторинні варіанти оплати, такі як готівка або фізичні картки.

Нарешті, велике занепокоєння споживачів викликає те, що безконтактні платежі не приймаються там, де вони здійснюють покупки. Краще інформування про переваги мобільних платежів могло б переконати малий та місцевий бізнес забезпечити більш широке прийняття, в тому числі безконтактних платежів.

Рішенням деяких проблем може стати надійніша автентифікація клієнтів. Надійна автентифікація клієнтів (SCA) має на меті додати рівень захисту до онлайн-платежів споживачів. Вона працює завдяки тому, що користувачі підтверджують свою особу щоразу, коли вони здійснюють транзакцію. Безконтактні транзакції також повинні проходити через процес SCA [9]. До цього регуляторного кроку все, що потрібно було зробити, це доторкнутися до своєї картки та здійснити транзакцію. Надійна автентифікація покликана підвищити безпеку платежів за допомогою двофакторної автентифікації. Цей метод автентифікації вимагає наявності двох з трьох факторів – знання, володіння та приналежність – для підтвердження транзакції. Наприклад, використання чіпа та PIN-коду на касовому терміналі, де чіп відповідає володінню, а PIN-код – знанню.

Технологія, яка стоїть за безпекою безконтактних платежів – токенізація платіжних даних. Токенізація працює шляхом заміни конфіденційної інформації (наприклад, номер банківського рахунку) на неконфіденційну заміну, відому як токен. Токен не має реальної цінності або значення, оскільки він складається з випадкового рядка даних. Токен зберігає всі релевантні дані без шкоди для їх безпеки.

На відміну від систем шифрування, які можна розшифрувати за допомогою секретного ключа, токенізація зберігає оригінальні дані, але не пропонує жодного способу розшифрувати токен для виявлення оригіналу.

Приклад налаштування токенізації мобільних платежів може виглядати такми чином: торговець впроваджує (купує, розробляє, маркує)

спеціальний додаток для прийому платежів. Додаток може використовуватися в магазині та/або в інтернеті, споживач встановлює додаток та вбудовує свою платіжну картку. Саме тут відбувається токенізація даних картки: реквізити картки зберігаються у вигляді токену, який зберігається в застосунку та використовується для обміну платіжною інформацією. Кожного разу, коли споживач має здійснити платіж на користь продавця, він списується через додаток за допомогою токена, без необхідності кожного разу вводити дані картки / платежу. Аутентифікація клієнта здійснюється за допомогою смартфону через розпізнавання обличчя, біометричні дані або інші відповідні заходи безпеки. Приклади токенізації платежів наведені в табл. 1.

Таблиця 1

Види та технології платежів

Вид платежу	Опис технології
Оформлення замовлення в один клік	Електронна комерція та традиційний бізнес можуть використовувати зручність оплати в один клік на свою користь, безпечно зберігаючи дані клієнта, та надаючи йому можливість завершити транзакцію одним кліком миші.
Періодичні платежі	Моделі оплати за підпискою. Токенізація дозволяє компаніям впроваджувати регулярні платежі, зберігаючи токен, що представляє картку клієнта, і використовуючи його для подальших платежів.
Позапланові періодичні платежі	Незаплановані періодичні платежі дозволяють торговцям визначати, коли стягувати плату з клієнтів. Застосовується до потокових сервісів, таких як Netflix або Spotify, тренажерних залів або інших постачальників послуг на основі підписки.

Джерело: розроблено авторами на основі [6]

Отже, завдяки токенізації клієнти можуть отримати вигоду від більш персоналізованої платіжної процедури, зберігаючи свої платіжні вподобання для майбутніх покупок. У разі витоку даних, клієнт не втратить конфіденційну інформацію про свій рахунок, оскільки інформація про його картку є токенізованою.

З приводу світової ситуації можна сказати, що Європа та Китай лідирують у світі безконтактних платежів. За даними Financial Times (FT), Швеція та Фінляндія ділять п’єдестал з Китаєм, коли мова йде про суспільства, найбільш близькі до безготівкових розрахунків. Китай лідирує у світі електронної комерції завдяки наявності відповідної платіжної екосистеми для розвитку технологій електронної комерції. Також, FT повідомляє, що Швеція є найбільш агресивною європейською країною

у своїй місії стати безготівковою. Лише 2 з 10 шведських транзакцій здійснюються за допомогою готівки.

Тенденції показують, що поведінка споживачів постійно змінюється і вимагає від постачальників послуг подальших інновацій. Цифрові гаманці є популярним способом оплати онлайн-транзакцій. Люди, які не мають банківських рахунків або мають їх недостатньо, користуються цифровими гаманцями, надсилаючи та отримуючи гроші від друзів та родичів.

Крім того, безконтактні способи оплати різко зросли, оскільки популярність смартфонів стрімко пішла до гори. Mastercard повідомила, що кількість платежів карткою Tap-and-Go в аптеках і продуктових магазинах подвоїлася у порівнянні з безконтактними платежами в період між 2020 і 2022 роками. Visa випустила власну опцію Tap-to-Pay на Android, щоб дозволити торговцям і малому бізнесу використовувати рішення SoftPOS (перетворити свої смартфони в безконтактні POS-системи) [8].

У травні 2022 року Mastercard запровадила програму «Біометричний касовий апарат». Ця послуга дозволяє здійснювати біометричні платежі. Помахом руки або просто посмішкою цей тип особистої оплати можна використовувати для розрахунку на касі у великих ритейлерів або малих підприємств.

Згідно з дослідженням FIS, споживачі, торговці та емітенти виграють від безконтактних платежів. Переваги для споживачів полягають у зручності, простоті використання та швидкості, а для торговців та емітентів – у скороченні часу проведення транзакцій, збільшенні обсягів платежів за картками, зниженні операційних витрат та збільшенні проникнення на ринок готівкових платежів. Зростання безконтактних платежів стимулює розвиток інших ніш та форм розрахунків.

Висновки з даного дослідження. Розвиток технологій та зручність використання сприяють зростанню популярності безконтактних платежів у всіх їх формах. У близькому майбутньому нові пристрої та пункти прийому платежів замінять ті, до яких ми звикли. Банкам та бізнесу важливо відповідати цій тенденції, інвестуючи в більш інноваційні та безпечні платіжні технології. Альтернативою інвестування є партнерство з постачальником послуг, який вже має необхідні технології та сертифікати. Варіант партнерства є швидшим та гарантує (у разі правильного вибору партнера), що роботу виконують люди, які є експертами у цій сфері.

ЛІТЕРАТУРА

1. Гладких Д. М. Банківська безпека держави в умовах розвитку інформаційної економіки (трансформації банківських операцій) : монографія. К. : НУОУ, 2019. 393 с.

2. Головченко О. М., Гострик О. М., Степаненко О. А. Методи прогнозування ймовірності виплат при наданні факторінгових послуг банківськими установами. *Збірник наукових праць Уманського національного університету садівництва*. 2016. Вип. 89, Ч. 2:

Економічні науки. С. 191–202. URL: http://dspace.oneu.edu.ua/jspui/handle/123456789/5075 (дата звернення: 18.11.2022).

3. Гострик О. М. Програмні засоби бізнес-аналізу та їх застосування для оцінки розвитку бізнес-середовища. *Економіко-правові аспекти господарювання: сучасний стан, ефективність та перспективи* : матеріали VIII Міжн. наук.-практ. конф. (Одеса, 23-24 вересня 2022 р). Одеса, 2022. С. 372–373.

4. Загарій В. П. Монетарні важелі досягнення фінансової безпеки: досвід розвинених країн. *Бізнес-інформ.* 2014. № 4. С. 400–404.

5. Платежные предпочтения жителей разных стран мира. URL: https://psm7.com/news/payment-preferences-of-different-countries.html (дата звернення: 18.11.2022).

6. Chen Xi (2014). Terminal Security of Mobile Finance.*Thoughts Contending*. № 4. pp. 106–110.

7. Pascal Urien (2014). A secure cloud of electronic keys for NFC locks securely controlled by NFC smartphones.*Consumer Communications and Networking Conference.* № 1. pp. 1120–1124. URL: https://ieeexplore.ieee.org/document/6994415 (дата звернення: 18.11.2022).

8. Ян Чен, Ян Цзянь-цзюнь. Дослідження технічної системи та стандартизації забезпечення безпеки мобільних платежів. *Інформаційні технології та стандартизація*. 2017. № 7. С. 17–20.

9. Ву І-мін, Хе Цзя-жун. Розробка та впровадження механізму безпеки SQlite на основі Android та віддаленого сервісу. *Журнал Гуандунського технологічного університету.* 2019. № 30. С. 49–52.