Офіційно/

Пенсійний фонд НБУ працює стабільно

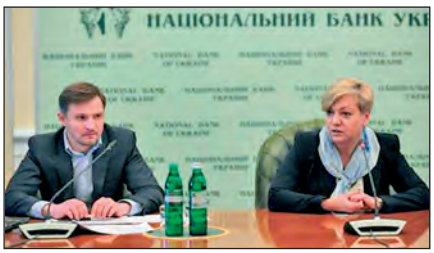
The NBU Pension Fund operates stably

Останнім часом у Національному банку України проводиться масштабна реорганізація, яка торкнулася й Корпоративного недержавного пенсійного фонду НБУ (КНПФ), зокрема нещодавно тут змінилося керівництво. Водночас у деяких засобах масової інформації з'явилися публікації, в яких колишні керівники фонду вважають нинішню його діяльність неефективною. Це викликало підвищений інтерес громадян до ситуації навколо найбільшого в Україні недержавного пенсійного фонду. У зв'язку з чим 13 березня в НБУ за участі Голови Національного банку Валерії Гонтаревої відбулася зустріч учасників фонду з директором департаменту з управління діяльністю Корпоративного недержавного пенсійного фонду Національного банку України Олегом Курінним, на якій було дано роз'яснення щодо нинішнього становища КНПФ.

The National Bank of Ukraine is going through the large-scale reorganization these days. The NBU Corporate Non-State Pension Fund (CNSPF) also underwent some changes; in particular, its authorities were changed. In some mass media, there appeared publications, in which the former authorities described Fund's operation as inefficient. This aroused interest of citizens in the situation around the largest non-state pension fund in Ukraine. In this connection, on 13 March 2015, there was held a meeting of the Fund participants with Director of the Department of NBU Corporate Non-State Pension Fund Management Oleh Kurinnyi, where the situation around the CNSPF was clarified. NBU Governor Valeriia Gontareva also participated in the meeting.

Відкриваючи зустріч, **Валерія Гонтарева** зазначила, що Корпоративний недержавний пенсійний фонд Національного банку України є найбільшим та найнадійнішим недержавним пенсійним фондом в Україні. Нині керівництво фонду докладає всіх зусиль для подальшої стабілізації роботи установи та підвищення її ефективності. (При цьому варто зауважити, що НБУ підтримує відкриття Службою безпеки України кримінального провадження за фактами розтрати та легалізації грошових коштів колишніми службовими особами КНПФ. – **Ред.**). Валерія Гонтарева також приділила увагу питанням оплати праці співробітників Національного банку, наголосивши на необхідності розробки нової – зрозумілої і транспарентної її системи на ринковій основі.

Директор департаменту з управління діяльністю Корпоративного недержавного пенсійного фонду Національного банку України **Олег Курінний** розповів, що колишнє керівництво фонду, вкладаючи кошти пенсіонерів, не проводило належного аналізу економічного, фінансового, ринкового стану емітентів, а також інвестиційних оцінок їхньої діяльності, тож вони часто інвестувалися в заздалегідь неліквідні облігації. Також приймалися рішення щодо розміщення коштів фонду на депозити в комерційних банках без попереднього аналізу їхнього фінансового стану та рівня ліквідності, зокрема у деяких випадках за такими розміщеннями не було навіть потрібної застави за депозитом. Тому фонду довелося списати частину активів, пов'язаних із втратою коштів, розміщених на депозитах у банках, які перебувають на стадії ліквідації, а також у зв'язку зі знеціненням коштів, укладених попереднім керівництвом у так звані "сміттєві цінні папери". Нині КНПФ активно працює над якнайшвидшим поверненням заставного майна для відшкодування активів фонду та відновленням платоспроможності емітентів облігацій, якими він володіє.



Олег Курінний і Валерія Гонтарева під час зустрічі з учасниками фонду.

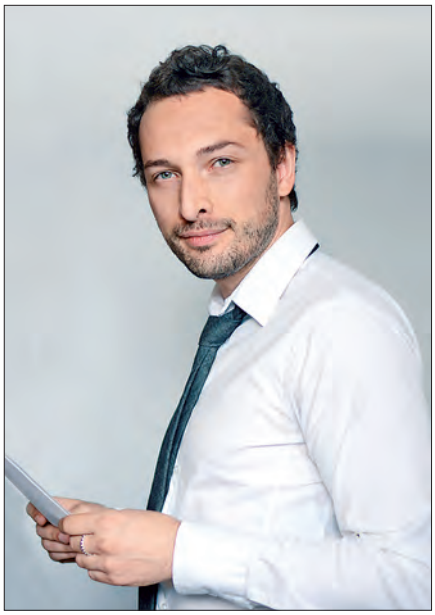
Щодо нинішньої ситуації у фонді, то Олег Курінний запевнив присутніх, що наразі його роботу стабілізовано, зокрема завдяки заходам, які проводяться з метою повернення заставного майна для відшкодування активів та відновлення платоспроможності емітентів облігацій, якими він володіє. Для подальшої оцінки реальної вартості активів фонд запросив одну з найбільших світових аудиторських компаній KPMG, яка здійснить оцінку справедливої вартості інвестиційного портфеля КНПФ. При цьому згідно з уже проведеною попередньою переоцінкою активів вони є достатніми та дають змогу фонду виконувати всі необхідні зобов'язання перед його учасниками. Відповідно до результатів фінансової діяльності фонду за три останні місяці основний дохід установа отримала за рахунок переоцінки вартості валюти, оренди, виплат за державними цінними паперами та депозитами у національній та іноземних валютах у державних банках. Олег Курінний навів дані щодо поточної фінансової ситуації у фонді, а також результати інвестиційної діяльності та роботи з адміністрування цієї установи. Зокрема з грудня 2014-го до лютого 2015 року здійснено пенсійні виплати і переведення до інших фінансових установ 2 050 учасникам фонду на суму понад 43 млн. грн.

При цьому керівник КНПФ наголосив, що надалі за рішенням Ради фонду установа дотримуватиметься консервативної інвестиційної політики – кошти розміщуватимуться виключно на депозитах у державних банках та інвестуватимуться в державні цінні папери строком обігу до трьох років. Завдяки вжитим заходам ліквідність фонду збережено та буде збільшено, отже, він і надалі залишатиметься флагманом свого сегмента і найбільш привабливим та надійним інструментом збереження пенсійних нагромаджень співробітників Національного банку України. Олег Курінний відповів також на численні запитання учасників фонду.

❐

За матеріалами управління інформації та громадських комунікацій Національного банку України.

By materials given by the Information and Public Relations Office of the National Bank of Ukraine.



Інновації/

■ ***Станіслав Широчин***
Stanislav Shyrochyn

Директор департаменту технологій роздрібних платежів Національного банку України, кандидат технічних наук

Ph.D. (Engineering), Director of the Retail Payment Technologies Department of the National Bank of Ukraine

E-mail: SShyrochyn@gmail.com

■ ***Роман Гартінгер***
Roman Hartinger

Начальник відділу забезпечення діяльності Національної системи масових електронних платежів департаменту роздрібних платежів Національного банку України, кандидат економічних наук

Ph.D. (Economics), Head of the Division for NSMEP Support of the Retail Payments Department of the National Bank of Ukraine

E-mail: Rmn.Hartinger@gmail.com

Платежі в мережі Інтернет: у пошуках "срібної кулі"

Internet payments: in search of a "silver bullet"

У статті авторами розглядається можливість використання QR-коду як одного з інструментів для здійснення безпечних платежів в мережі Інтернет. Запропонована технологія, на думку авторів, має право на існування як один із додаткових продуктів Національної системи масових електронних платежів (НСМЕП).

Протягом 2014 року платежі в мережі Інтернет залишались одним із найпоширеніших об'єктів, щодо яких вчинялися шахрайські дії. Тенденція до постійного збільшення показників кібершахрайства в Інтернеті характерна не лише для українського ринку, а й для більшості країн світу. Наприклад, за даними Банку Франції, платежі в Інтернеті з використанням платіжних карток у цій країні становили 7% від загальної кількості карткових операцій. Водночас саме на інтернет-платежі припадає 65% від загальної кількості шахрайських операцій з використанням платіжних карток.

Причина цього полягає насамперед у незахищеності даних, які передаються під час здійснення так званих "card not present" -операцій. Вони не потребують фізичного використання платіжної картки, достатньо лише її реквізитів (номера картки (PAN), терміну дії (expired), в окремих випадках – контрольного коду CVV2/CVC2). Як свідчить практика, ймовірність несанкціонованого перехоплення цієї інформації досить висока. Отримавши реквізити платіжної картки, злочинець може скористатися ними для шахрайських платежів ще декілька разів. Крім того, деякі інтернет-торговці зберігають дані про платіжні картки покупців на власних серверах. У разі злому шахраями такого серверу відбувається крадіжка відразу всіх карткових даних.

The article considers the possibility of using the QR-code as one of instruments for safe internet payments. The suggested technology, by authors' opinion, has a right to exist as one of additional products of the National System of Mass Electronic Payments (NSMEP).

During 2014, internet payments were one of the most widespread objects suffering from fraud. A tendency towards a gradual growth in cyber fraud indicators on the Internet was characteristic of not only Ukrainian market but of the majority of world countries. For example, by Bank of France data, internet payments with the use of payment cards in the country made up 7% of the total number of payment card operations. At the same time, internet payments are accounted for 65% of the total number of fraud operations with the use of payment cards.

Unprotected data being transferred during card-not-present transactions are the main factor causing the above-mentioned problems. The transactions do not require the physical use of a payment card; it is sufficient to write its identification data viz. the payment account number (PAN), expiration date, and in some cases, the check code CVV2 (Card Verification Value) or CVC2 (Card Verification Code). As practice shows, the probability of the unauthorized

data interception is rather high. Having gained the identification data, a fraudster can use them during its fraud payments some more times. Moreover, some internet-traders save the identification data of buyers on their own servers. In case of backing the server the fraudsters steal the identification data of all the payment cards at once.

ПЕРЕДУМОВИ ПОШУКУ НОВИХ ІНСТРУМЕНТІВ ДЛЯ ІНТЕРНЕТ-ПЛАТЕЖІВ

Черіан Ебрегем, експерт компанії "Дроп Лебс" (Drop Labs), опосередковано підтверджує зазначену тенденцію на прикладі ситуації з шахрайством у новітній платіжній системі "Еппл Пей" (Apple Pay). За його даними, рівень шахрайства на ринку США за операціями з фізичним використанням кредитних карток становить близько 0.1%. Водночас у платіжній системі "Еппл Пей" рівень шахрайства нині сягає 6%. Незважаючи на використання в цій системі прогресивних технологій, зокрема – сканера відбитків пальців Touch ID та бездротового високочастотного зв'язку малого радіуса дії NFC, слабким місцем "Еппл Пей", на думку експерта, залишається внесення користувачами даних про належні їм платіжні картки [1].

Таким чином, шахрайство за "card not present"-платежами, тобто без фізичного використання картки, посідає друге місце в "анти-рейтингу" шахрайських дій із платіжними картками (найпопулярнішим способом залишається підробка карток) [2].

Схема роботи мобільного платіжного інструменту з використанням QR-коду

Усе зазначене вище свідчить про актуальність пошуку нових, менш ризикових інструментів для здійснення платежів в Інтернеті. На нашу думку, доцільно по можливості уникати прямого використання реквізитів платіжної картки як ідентифікатора джерела коштів для інтернет-платежу. Бажано також відійти від передачі даних клієнта інтернет-торговцю (або компанії-посереднику платежу).

У контексті взаємодії учасників здійснення інтернет-платежу найважливішою ланкою вбачається взаємодія між покупцем і торговцем. З позиції платіжної системи, в якій здійснюється платіж, реалізація взаємодії саме між цими двома учасниками є найвитратнішою. Це пов'язано з тим, що покупець і торговець в Інтернеті не можуть бути "довіреними сторонами", у них навіть немає спільної третьої "довіреної сторони" (банку).

ТЕХНОЛОГІЯ QR-КОДУ ЯК НОВИЙ ПЛАТІЖНИЙ ЗАСІБ У НАЦІОНАЛЬНІЙ СИСТЕМІ МАСОВИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ (НСМЕП)

Отже, ставлячи за мету максимальне здешевлення проведення платежу між покупцем (клієнтом) і торговцем, на нашу думку, доцільно забезпечити не "матеріальну", а "віртуальну" природу як платіжного пристрою, так і платіжного засобу.

У ролі платіжного засобу пропонуємо розглянути можливість використання програмного додатка для смартфона. При цьому, на відміну від безконтактних платежів за технологією NFC, у нашому випадку смартфон не потребує обов'язкового обладнання модулем безпеки (secure element). Це дасть змогу банку взаємодіяти з клієнтом, оминаючи посередництво операторів мобільного зв'язку та компаній – виробників смартфонів.

Як уже зазначалося, в умовах підвищеного ризику шахрайських дій під час передавання даних від покупця (клієнта) до інтернет-торговця бажано такі дані торговцю не передавати взагалі. Отже, вважаємо за доцільне концептуально змінити підхід до здійснення платежу: від "Пулл" ("PULL")- системи до "Пуш" ("PUSH")-системи, коли сам торговець передає "інвойс" або іншу інформацію, необхідну для здійснення платежу, а клієнт, використовуючи отримані дані, здійснює платіж. Зрозуміло, що процес передавання такої інформації торговцем покупцю має бути автоматизовано. Як транспорт для передавання даних пропонуємо використовувати QR-код[1].

На схемі у загальному вигляді показано порядок взаємодії учасників системи. Торговець генерує графічний QR-код з інформацією про певний товар чи замовлення. Покупець (клієнт) зчитує QR-код за допомогою камери смартфона або планшета (1). Спеціальний мобільний додаток, встановлений на мобільному пристрої, розпізнає дані замовлення та, після підтвердження клієнтом, забезпечує передавання до банку-емітента інформації, зашифрованої в QR-коді (даних про торговця, товар, вартість товару тощо), а також запит про ініціювання платежу (2). Інформація з мобільного пристрою передається до банку засобами безпровідної мережі Інтернет. Банк-емітент перевіряє дані клієнта і, в разі успішної його ідентифікації та наявності коштів на рахунку, списує з нього необхідну суму. Після цього через процесинговий центр банк-емітент надсилає до банку-еквайра повідомлення про оплату товару (3, 4). Банк-еквайр інформує про успішну оплату товару торговця (5A), а також надсилає відповідь банку-емітенту (5, 6), який, у свою чергу, надсилає повідомлення про статус операції на мобільний пристрій клієнта (7).

У 2013 році під час міжнародної конференції "Платіжний форум" Національним банком було презентовано технологію мобільних платежів із використанням QR-коду в НСМЕП на базі відкритих міжнародних стандартів як один із продуктів цієї платіжної системи, призначений для здійснення інтернет-платежів.

Особливості функціонування цього продукту НСМЕП базуються на зазначених вище принципах та визначені нормативними документами НСМЕП "Специфікація мобільного платіжного інструменту на базі технології QR-код"[2] та Положення "Про застосування технології QR-коду в Національній системі масових електронних платежів на базі відкритих міжнародних стандартів"[3].

Перелік операцій, які можуть бути виконані з використанням технології QR-коду в НСМЕП, а також порядок взаємодії учасників детальніше подано в таблиці. Серед основних характеристик застосування QR-коду в НСМЕП виокремимо такі.

Інформаційне наповнення QR-

[1] QR-код (від англ. quick response – "швидка відповідь") – матричне (двомірне) графічне зображення, що формується за спеціальним алгоритмом і дає змогу розпізнавати й обробляти закладену в ньому інформацію програмним засобом скануючого пристрою (смартфона, планшета тощо).

[2] Затверджено рішенням ради Платіжної організації НСМЕП, протокол № 221/2013 від 16.09.2013 р.

[3] Затверджено рішенням ради Платіжної організації НСМЕП, протокол № 236/2014 від 19.05.2014 р.

коду в НСМЕП суттєво відрізняється від типового підходу до використання QR-коду в інших практиках. Зазвичай QR-код несе інформацію про "посилання" на сайт (URL) до тієї інформації, що потрібна користувачу. Слабким місцем такого підходу є можливість легкої модифікації інформації, оскільки в URL не існує формальних ознак, за якими можна перевірити, чи його не спотворено. Натомість у платіжному засобі НСМЕП QR-код фактично несе інформацію "інвойсу", що має фіксований формат та захищений електронно-цифровим RSA-підписом. Завдяки цьому навіть якщо хтось модифікує інформацію, це буде виявлено і не призведе до помилкового (шахрайського) платежу.

Окремо перелічимо деякі інші переваги цього продукту:

- для інтернет-платежів, які передбачають доставку товару клієнту, існує спеціальна система захисту покупки: поки товар не буде доставлено і клієнт не прийме його, він не передає доставнику код операції, який торговець, у свою чергу, має надати еквайру для отримання коштів. Якщо код не буде надано протягом визначеного часу, кошти повертаються клієнту;
- з'являється можливість приймати платежі за кількома новими каналами продажу, такими, як телевізійні продажі та продажі з афіш чи оголошень;
- під час використання технології QR-коду на касових апаратах суттєво зменшуються витрати на приймання платежів, оскільки достатньо лише змінити програмне забезпечення, та немає необхідності в обладнанні платіжного терміналу або ПІН-паду;
- це рішення дає можливість реалізувати послугу моментальних переказів між клієнтами;
- QR-код НСМЕП може бути використаний для отримання готівки в банкоматі (звісно, для цього слід відповідно доопрацювати програмне забезпечення банкомата);
- оскільки всі способи застосування, що покривають практично весь спектр платіжних послуг, не потребують використання матеріального платіжного пристрою або платіжного засобу, суттєво зменшуються витрати на організацію платежів порівняно з іншими технологіями.

СВІТОВИЙ ДОСВІД

Практика використання QR-коду у сфері платежів не нова. Наприклад, у 2012 році "Оні Банк Акор" (Oney Banque Accord), банківський підрозділ провідної французької мережі супермаркетів "Ашан" (Auchan), представив бренд багатоканальних мобільних платежів на основі QR-коду під назвою "Флеш'н Пей" (Flash'n Pay).

Платіжні операції, які можуть бути здійснені з використанням технології QR-коду в НСМЕП

1	2
Розрахунок в Інтернеті за віртуальні товари	**Розрахунок в Інтернеті за реальні товари**
• Клієнт на сайті торговця обирає товар, вказує спосіб оплати – QR НСМЕП, торговець формує підсумковий рахунок. • QR-код зчитується програмним додатком клієнта, дані демонструються клієнту. У разі згоди клієнт шляхом введення ПІН-коду ініціює відправку запиту оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль (OTP) і надсилає його на номер телефону клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такі функції не підтримує) зчитує одноразовий пароль (OTP) із повідомлення і повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту (через процесинг та емітента) код трансакції і повідомляє торговцю про зарахування коштів на рахунок. Торговець видає віртуальний товар. Клієнт отримує необхідний товар.	• Під час розрахунку за реальні товари використовується схема оплати з підтвердженням доставки. • Клієнт на сайті торговця обирає товар, вказує спосіб оплати – QR НСМЕП, торговець формує підсумковий рахунок. • QR-код зчитується програмним додатком клієнта, дані демонструються клієнту. В разі згоди клієнт шляхом введення ПІН-коду ініціює відправку запиту оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль і надсилає його на номер телефона клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такої функції не підтримує) зчитує одноразовий пароль (OTP) із повідомлення і повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту (через процесинг та емітента) код трансакції і повідомляє торговцю про отримання коштів на його користь. Торговець організовує доставку товару. Клієнт отримує необхідний товар і передає торговцю код трансакції. Торговець через свій програмний додаток передає код трансакції еквайру й отримує гроші на рахунок.
Розрахунок у магазині	**Оплата товару в телемагазині**
• Клієнт обирає товар, вказує спосіб оплати – QR НСМЕП, йому формується підсумковий рахунок і QR-код на чеку. • QR-код зчитується програмним додатком клієнта, дані демонструються клієнту. У разі згоди клієнт шляхом введення ПІН-коду ініціює відправку запиту оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль і надсилає його на номер телефона клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такої функції не підтримує) зчитує одноразовий пароль із повідомлення і повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту (через процесинг та емітента) код трансакції. Торговець запитує у еквайра стан замовлення (шляхом передачі даних, зашифрованих в QR-коді) й отримує підтвердження оплати. Клієнт отримує необхідний товар.	• Під час розрахунку за реальні товари в телемагазині використовується схема оплати з підтвердженням доставки. • Клієнт за допомогою програмного додатка клієнта зчитує з телевізора QR-код. • Дані, зазначені вище, демонструються клієнту. Клієнт за допомогою ПІН-коду дає згоду, вводить реквізити доставки (адресу, дату і час, контактний телефон) і відправляє запит оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль і надсилає його на номер телефона клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такої функції не підтримує) зчитує одноразовий пароль із повідомлення і повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту (через процесинг та емітента) код трансакції і повідомляє торговцю про отримання коштів на його користь. • Торговець організовує доставку товару. Клієнт отримує необхідний товар і передає торговцю код трансакції. Торговець через свій програмний додаток передає код трансакції еквайру й отримує кошти на рахунок.

1	2
Оплата товару / квитків з афіші	**Зняття готівки в банкоматі**
• Під час розрахунку за товари та послуги з афіші використовується схема оплати з підтвердженням доставки. • Клієнт за допомогою програмного додатка клієнта зчитує з афіші QR-код. • Дані демонструються клієнту. Клієнт за допомогою ПІН-коду дає згоду, вводить реквізити доставки (адресу, дату і час, контактний телефон) і відправляє запит оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль і надсилає його на номер телефона клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такої функції не підтримує) зчитує одноразовий пароль (OTP) із повідомлення і повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку, і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту (через процесинг та емітента) код трансакції і повідомляє торговцю про отримання коштів на його користь. • Торговець організовує доставку товару. Клієнт отримує необхідний товар і передає торговцю код трансакції. Торговець через свій програмний додаток передає код трансакції еквайру й отримує кошти на рахунок.	• Клієнт на клавіатурі банкомата набирає необхідну суму, вказує спосіб оплати – QR НСМЕП, йому формується підсумковий рахунок, у тому числі в вигляді QR-коду. • QR-код зчитується програмним додатком клієнта, дані демонструються клієнту. В разі згоди клієнт шляхом введення ПІН-коду ініціює відправку запиту оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль і надсилає його на номер телефона клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такої функції не підтримує) зчитує одноразовий пароль (OTP) із повідомлення і повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту (через процесинг та емітента) код трансакції і передає на банкомат інформацію про видачу готівкових коштів. Клієнт отримує запитану суму.
Переказ коштів із рахунка клієнта на рахунок іншого клієнта	
• Клієнт-отримувач у своєму програмному додатку обирає опцію "показати реквізити". На мобільному пристрої (телефоні) відображається QR-код. • QR-код містить нульову суму, за якою розраховується підпис, а сума переказу вказується відправником. • QR-код зчитується програмним додатком клієнта-відправника, дані демонструються клієнту. Він вводить суму платежу і в разі згоди шляхом введення ПІН-коду ініціює відправку запиту оплати до емітента. • Емітент перевіряє підпис клієнта, у разі відповідності оцінює ризик-параметри (зокрема, якщо за цими реквізитами клієнт уже здійснював платежі або якщо сума менша за встановлений ліміт, необов'язково використовувати другий канал аутентифікації). • Якщо другий канал усе ж використовується, емітент генерує одноразовий пароль і надсилає його на номер телефона клієнта SMS-повідомленням. Програмний додаток клієнта (або сам клієнт, якщо програмний додаток такої функції не підтримує) зчитує одноразовий пароль (OTP) із повідомлення й повторно відправляє запит на оплату. • Після перевірки клієнта емітент списує кошти з його рахунку і в разі успішного завершення відправляє повідомлення про оплату до процесингу, підписуючи його своїм ключем. Процесинг перевіряє підпис емітента і відправляє повідомлення про оплату еквайру. • Еквайр після перевірки QR-коду підтверджує оплату, повертає клієнту-відправнику (через процесинг та емітента) код трансакції і зараховує клієнту-отримувачу необхідну суму коштів. Клієнт-отримувач може переглянути залишок коштів на рахунку або історію операцій і виявити зарахування.	

"Щоб використовувати "Флеш'н Пей", покупцям необхідно завантажити додаток для смартфона, а потім "прив'язати" свої платіжні картки та картки лояльності до свого облікового запису. Під час оплати покупцеві на касовому терміналі пред'являється QR-код. Покупець захоплює його зображення за допомогою камери свого телефону і вводить ПІН-код для завершення платежу. "Флеш'н Пей" також застосовується для проведення операцій електронної та мобільної комерції. Наприклад, для здійснення купівлі в інтернет-магазині покупці використовують свій телефон для захоплення зображення 2D штрих-коду, який генерується при оплаті, а потім вводять ПІН-код на своїх телефонах" [3].

У США подібний крок зробили "Вол-Март" (Wal-Mart), "Тарґет" (Target), "7-ілевен" (7-Eleven), "Бест Бай" (Best Buy) та інші великі компанії-ритейлери. У серпні 2012 року вони спільно створили "Мерчент Кестемер Іксчендж" (Merchant Customer Exchange, MCX) – нову компанію мобільних платежів та акцій, що запропонувала покупцям універсальну мобільну комерцію, яка поєднує в собі зручність оплати на касі з персоналізованими пропозиціями.

Окремі українські банки також впровадили технологію QR-коду для здійснення платіжних операцій, наприклад, для отримання готівки в банкоматі без використання платіжної картки.

Водночас схема інформаційних потоків, яка пропонується до використання в продукті НСМЕП, суттєво відрізняється від інших варіантів та забезпечує мінімальні ризики під час міжбанківської взаємодії. Варто зазначити, що використання QR-коду в НСМЕП розглядається не як заміна використання "класичних" інструментів інтернет-платежів (зокрема, CNP-платежів із залученням "хмарних" технологій, токенів тощо), а як спосіб розширення продуктової лінійки та підвищення привабливості цієї платіжної системи для банків і клієнтів.

ПОТОЧНИЙ СТАН ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ QR-КОДУ В НСМЕП

На сьогодні компанії – розробники програмно-технічних засобів НСМЕП отримали від Національного банку специфікації технології QR-коду та проводять розроблення відповідних рішень для мобільних телефонів, спеціалізованих терміналів (у тому числі на базі касових апаратів), а також рішень для процесингових центрів та систем банків (емітентів та еквайрів). Дві компанії успішно завершили випробування та починають пілотні проекти з упровадження зазначених рішень до промислової експлуатації за участі банків – учасників НСМЕП.

❐

Список використаних джерел

1. Smart Mouse Traps and Lazy Mice // Drop Labs. – [Електронний ресурс]. – Режим доступу: http://www.droplabs.co/?p=1204.

2. Операции CNP (card not present) // Banki.ru. – [Електронний ресурс]. – Режим доступу: http://www.banki.ru/wikibank/cnp-operatsii/.

3. Oney Banque Accord launches QR code-based mobile payments service in France // The Paypers. – [Електронний ресурс]. – Режим доступу: http://www.thepaypers.com/mobile-payments/oney-banque-accord-launches-qr-code-based-mobile-payments-service-in-france/749533-16.