УДК 343
DOI https://doi.org/10.32782/TNU-2707-0581/2023.2/21

Бугера С.І.
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю
при Раді національної безпеки і оборони України

ДО ПИТАННЯ ПРОТИДІЇ ШАХРАЙСТВУ З ПЛАТІЖНИМИ КАРТКАМИ

У статті розглянуто питання протидії шахрайству з платіжними картками. Встановлено, що шахрайство з платіжними картками можна класифікувати як: банкоматне шахрайство; шахрайство в середовищі Card-Not-Present; шахрайство в термінальній мережі; соціальна інженерія. Для протидії шахрайству з платіжними картками важливим є використання зарубіжного досвіду з цього питання. Зокрема, використання електронних систем запобігання шахрайству, а також електронних засобів контролю в США на сьогодні є пріоритетом та складовою міжнародної політики із ведення електронної комерційної діяльності. Досвід США може бути адаптований в Україні щодо: створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції та торгівлі, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв; реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство; використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства; посилення міжнародного співробітництва та залучення громадськості до соціально-виховної роботи з профілактики шахрайства в сфері електронної торгівлі. Встановлено, що протидії шахрайству з платіжними картками потребує комплексного вирішення. Насамперед, доцільним є вдосконалення законодавства з цього питання, зокрема в частині кримінальної відповідальності. Важливим є також дослідження зарубіжного досвіду в частині розроблення запобіжних заходів на спеціально-кримінологічному та загальносоціальному рівнях. При цьому одним з найбільш дієвих способів протидії шахрайству з платіжними картками залишається виконання громадянами таких правил: отримувати інформацію, особливо з приводу фінансових виплат, лише з офіційних джерел; не переходити за сумнівними гіперпосиланнями; не повідомляти конфіденційну інформацію, зокрема дані банківських карток, стороннім; у разі підозри шахрайських дій – негайно повідомляти правоохоронним органам. Офіційні сторінки державних органів, благодійних організацій, банківських структур у месенджерах та соціальних мережах мають бути верифікованими.

Ключові слова: *платіжні картки, шахрайство, протидія, законодавство, зарубіжний досвід.*

Постановка проблеми. Протидія шахрайству з платіжними картками залишається актуальною проблемою і під час повномасштабної війни в Україні. При цьому найпоширенішим видом шахрайства стала фейкова соціальна допомога від державних чи міжнародних організацій: у 2022 році Національний банк України виявив близько 4500 фішингових ресурсів, для порівняння – у 2021 році ця цифра була на порядок меншою [1].

Необхідно зазначити, що Верховна Рада України утворила Тимчасову слідчу комісію (ТСК) із питань розслідування можливих фактів шахрайства у сфері фінансових послуг, які здійснюються з використанням інформаційних, електронних комунікаційних систем та електронних комунікаційних мереж. Серед основних завдань ТСК: розслідування можливих фактів шахрайства та іншої незаконної діяльності у сфері фінансових послуг та ринків фінансових послуг, які здійснюються з використанням інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж, а також розслідування можливих фактів залучення та навчання третіх осіб з метою їх участі в незаконній діяльності у сфері фінансових послуг та ринків фінансових послуг. За результатами роботи члени ТСК мають підготувати пропозиції про вдосконалення законодавства щодо протидії шахрайству та іншій незаконній діяльності у сфері фінансових послуг та ринків фінансових послуг [2].

Аналіз останніх досліджень і публікацій. Питання протидії шахрайству з платіжними

картками досліджували у свої працях такі вчені, як А. О. Єременко, А. М. Клочко, О. В. Курман, С. І. Ніколаюк, О. І. Олійничук, С. В. Поперешняк, Т. В. Романенко, С. В. Самойлов та інші. При цьому підвищення рівня використання інформаційно-комунікаційних технологій у фінансовій системі та необхідність забезпечення удосконалення протидії шахрайству з платіжними картками, потребують проведення подальших наукових досліджень.

Метою статті є дослідження проблем протидії шахрайству з платіжними картками та розроблення практичних рекомендацій з даного питання.

Виклад основного матеріалу. Кримінальні правопорушення, що вчиняють у сфері банківської діяльності, стали досить поширеними і становлять суттєву небезпеку для суспільства й держави і одним із виявів таких суспільно небезпечних діянь є шахрайство з використанням банківських платіжних карток, оскільки суспільна небезпечність таких злочинів полягає в тому, що, поряд із посяганням на власність громадян, їхні грошові кошти, які перебувають на банківських рахунках, цей злочин спричиняє шкоду злагодженому функціонуванню банківської системи. Предметом шахрайства з банківськими платіжними картками є грошові кошти, що знаходяться на банківських рахунках. З об'єктивної сторони цей злочин полягає в заволодінні грошовими коштами громадян, які знаходяться на банківських рахунках, шляхом обману чи зловживання довірою. Шахрайство, вчинене з використанням платіжних карток або їх реквізитів, має розцінюватись як шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки [3, с. 81].

Шахрайство з платіжними картками можна класифікувати як: 1) банкоматне шахрайство: фізичний скімінг (Skimming) – полягає у встановленні зловмисниками на банкоматі обладнання для копіювання даних магнітної смуги та запису ПІН-коду платіжної картки; Cash Trapping – полягає у встановленні зловмисником на банкоматах спеціальних пристроїв, які дозволяють здійснити захват готівки за операціями, які здійснюють законні держателі карток; Transaction Reversal Fraud (TRF) – в результаті зловмисник отримує готівку при фактично незмінному балансі карткового рахунку, за якими проводилась операція; програмний скімінг (Cyber Skimming) – полягає у встановленні зловмисником на банкоматі шкідливого програмного забезпечення, яке здійснює копіювання даних магнітної смуги та ПІН-кодів платіжних карток; прямий диспенс (Jackpotting) – полягає у встановленні та активації зловмисником на банкоматі шкідливого програмного забезпечення, яке дає диспенсеру банкомату команду на видачу всіх банкнот завантажених в касети; 2) шахрайство в середовищі Card-Not-Present: фішинг; віруси на комп'ютерах і мобільних пристроях; 3) шахрайство в термінальній мережі: фізичний скімінг (Skimming); програмний скімінг (Cyber Skimming); 4) соціальна інженерія: вішинг – сутність шахрайства полягає у мотивації шахраєм клієнта банку до здійснення дій, які він за інших обставин в звичайній обстановці, маючи час на обміркування та можливість порадитись з іншими людьми, не здійснив би. Зловмисники стимулюють клієнтів: здійснювати перекази своїх коштів на карткові рахунки шахраїв (банкомати або системи Інтернет-банкінгу); розголошувати реквізити своїх платіжних карток та/або свої персональні данні, необхідні для проведення операцій в мережі Інтернет; надавати копії документів, що ідентифікують особу, та можуть бути використанні при оформленні споживчих та грошових кредитів [4].

Загалом методи несанкціонованого доступу до інформації можна умовно поділити на дві категорії: з використанням методів соціальної інженерії та без них. На відміну від другого випадку, коли зловмисник повинен володіти знаннями у галузі ІТ, у першому для отримання конфіденційних даних він спирається на знання з соціології та психології. Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки, як когнітивні упередження. Основна тактика соціальної інженерії – за допомогою психологічних методів (наприклад, спілкуючись начебто від імені сервісної компанії чи банку) переконати користувача розкрити інформацію особистого характеру (паролі, номери кредитних карток тощо) [5].

Загалом протидія шахрайству з платіжними картками є актуальною проблемою для багатьох країн. Зокрема, Федеральна торгова комісія США (FTC) у січні 2022 року повідомила, що за 2021 рік шахраї вкрали в користувачів соціальних мереж близько 770 мільйонів доларів, що вдвічі більше, ніж у 2020 році. Від афер в соцмережах постраждало понад 95 тисяч користувачів [6].

В Україні зловмисники в Інтернеті привласнюють гроші під виглядом надання виплат українцям, які постраждали від війни. Аферисти поширюють фейкову інформацію про соціальні виплати, створюючи сторінки-клони державних

організацій, керівництва держави, представників ООН, Червоного Хреста, благодійних фондів, банків тощо. Для реалізації злочину здебільшого використовують фішинг. Громадянам пропонують ввести персональні дані та номер банківської картки нібито для зарахування грошей. Однак відомості, введені на таких ресурсах, автоматично стають відомі зловмисникам. Маючи дані банківських карток громадян, вони привласнюють гроші з рахунків [7].

При цьому відповідно до ст. 67 Закону України «Про платіжні послуги» [8] надавачі платіжних послуг зобов'язані запровадити систему захисту інформації, що має забезпечувати безперервний захист інформації про виконання платіжних операцій та індивідуальної облікової інформації на всіх етапах її формування, обробки, передавання та зберігання. Система захисту інформації має забезпечувати цілісність, конфіденційність, доступність та простежуваність інформації, що формується, обробляється, передається та зберігається під час виконання платіжних операцій, відповідно до вимог, встановлених нормативно-правовими актами Національного банку України.

Загалом сума збитків банків, торговців, клієнтів від незаконних дій з платіжними картками у 2022 році становила понад 481 млн гривень. Це на 46% більше ніж у довоєнному 2021 році. Кількість незаконних дій з платіжними картками, за якими були понесені збитки, зросла на 8%. У 2022 році середня сума однієї незаконної операції становила близько 2 200 гривень, що на третину більше, ніж у 2021 році (1 600 гривень). На один мільйон гривень видаткових операцій із використанням платіжних карток на незаконні дії/шахрайські операції припадало 69 гривень. Це не набагато більше, ніж у 2021 році (65 гривень), та свідчить про те, що сума збитків від шахрайства зростала співставно із зростанням суми операцій з платіжними картками українських банків. За даними НБУ, 86% від загальної кількості випадків платіжного шахрайства за 2022 рік відбулися в мережі Інтернет, водночас лише 14% – через фізичні пристрої (торговельна мережа, банкомати, пристрої самообслуговування) [9].

Необхідно зазначити, що Українська міжбанківська Асоціація членів платіжних систем «ЄМА» є добровільним недержавним некомерційним неприбутковим об'єднанням. Метою діяльності Асоціації є – всебічне сприяння розвитку зручних та безпечних безготівкових платіжних інструментів і сервісів в Україні. Асоціація працює для того, щоб зробити використання безготівкових платіжних інструментів і технологій при розрахунках і кредитуванні в Україні невід'ємним елементом фінансової культури [10].

Протягом 2022 року Асоціація «ЄМА» у співробітництві з чеським підрозділом компанії ThreatMark (США) заблокували на рівні реєстраторів 568 активних фішингових та шахрайських сайтів в українському сегменті Інтернет, націлених проти споживачів фінансових послуг. Водночас коефіцієнт успішного блокування шкідливих ресурсів на рівні реєстратора (closure rate) склав 95,5%. Зростання кількості фішингових сайтів пов'язане з дедалі більшим поширенням схеми виманювання у банківських клієнтів облікових записів до онлайн-банкінгу, після чого з їх карткових рахунків знімаються гроші та на їх ім'я оформлюються онлайн-кредити. Популярність злочинних партнерських моделей Scam-as-a-Service та Phishing-as-a-Service призвела до масштабування шахрайських схем на міжнародному рівні та зниження порога входу для новачків, що не мають спеціальних навичок для проведення скам-атак. В 2022 році зросла кількість виявлених фейкових застосунків у Google Play та App Store, більшість з яких рекламуються як застосунки для реалізації залишків палива за низькими цінами та застосунки для отримання грошової допомоги від держави та міжнародних організацій. Також збільшилася кількість фейкових банківських чатботів у Telegram, що виманюють карткові реквізити та облікові записи до онлайн-банкінгу [11].

Для протидії шахрайству з платіжними картками Національний банк України в травні 2023 року розпочав Всеукраїнську інформаційну кампанію з платіжної безпеки #ШахрайГудбай разом із Департаментом кіберполіції Національної поліції України, а також за підтримки Проєкту USAID «Реформування фінансового сектору». Вона стане продовженням першої подібної кампанії, що успішно пройшла у 2020 році. Її мета – поліпшити обізнаність громадян та нагадати їм про основні правила безпеки під час безготівкових розрахунків, особливо в мережі Інтернет. Характерно, що більшість випадків, коли громадяни втрачають свої кошти, виникають через розголошення ними даних своєї картки, одноразових паролів для підтвердження операцій, даних для входу до інтернет-банкінгу. Половина від загальної суми збитків від шахрайства з платіжними картками відбулася через соціальну інженерію [12].

Також Національний банк України з метою зниження ризиків шахрайства встановив до

надавачів платіжних послуг вимогу застосувати посилену автентифікацію користувачів. Так, надавачі платіжних послуг зобов'язані застосовувати посилену автентифікацію користувачів під час: отримання ними дистанційного доступу до рахунків; ініціювання дистанційної платіжної операції; будь-яких інших дій у разі підозри вчинення шахрайства чи інших неправомірних дій (або існування такого ризику). За результатами процедури посиленої автентифікації користувача надавач платіжної послуги має створити унікальний код автентифікації, який дає змогу пов'язувати операцію на певну суму і конкретного отримувача. Цей код повинен прийматися надавачем платіжних послуг щоразу під час отримання користувачем доступу до рахунку, ініціювання дистанційної платіжної операції тощо. Зокрема, якщо раніше під час онлайн-розрахунків було достатньо інформації про платіжну картку і одноразового пароля, тепер необхідно буде використовувати як мінімум два елементи захисту, які підтверджують, що платіж здійснює користувач, який має законні підстави для використання конкретного платіжного інструмента, а не шахрай [13].

Для протидії шахрайству з платіжними картками необхідно дотримуватись таких правил безпеки: не тримати PIN-код картки разом із самою карткою; не розголошувати PIN-код і CVV2-код платіжної картки; регулярно змінювати PIN-код картки; встановити добовий ліміт на зняття готівки з платіжної картки; під'єднати послугу SMS-інформування про всі операції за картковим рахунком; не використовувати чужі телефони для входу в Особистий кабінет мобільного банку; уникати зберігання даних картки на сайтах інтернет-магазинів; у разі втрати (крадіжки) картки негайно телефонувати до банківської установи для її блокування [14].

Важливим є також використання зарубіжного досвіду з цього питання. Зокрема, використання електронних систем запобігання шахрайству, а також електронних засобів контролю в США на сьогодні є пріоритетом та складовою міжнародної політики із ведення електронної комерційної діяльності. Досвід США може бути адаптований в Україні щодо: створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції та торгівлі, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв; реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство; використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства; посилення міжнародного співробітництва та залучення громадськості до соціально-виховної роботи з профілактики шахрайства в сфері електронної торгівлі [15].

Висновки. Підсумовуючи, необхідно зазначити, що питання протидії шахрайству з платіжними картками потребує комплексного вирішення, і зокрема, щодо: розроблення запобіжних заходів на спеціально-кримінологічному та загальносоціальному рівнях з урахуванням зарубіжного досвіду та вдосконалення відповідного законодавства в частині посилення кримінальної відповідальності.

При цьому одним з найбільш дієвих способів протидії шахрайству з платіжними картками залишається виконання громадянами таких правил: отримувати інформацію, особливо з приводу фінансових виплат, лише з офіційних джерел; не переходити за сумнівними гіперпосиланнями; не повідомляти конфіденційну інформацію, зокрема дані банківських карток, стороннім; у разі підозри шахрайських дій – негайно повідомляти правоохоронним органам. Офіційні сторінки державних органів, благодійних організацій, банківських структур у месенджерах та соціальних мережах мають бути верифікованими [16]. Важливим є також виконання п. 18 Плану реалізації Стратегії кібербезпеки України [17] щодо запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів.

Список літератури:

1. НБУ назвав найбільш поширений вид шахрайства з використанням платіжних карток. URL: https://www.rbc.ua/rus/news/nbu-nazvav-naybilsh-poshi reniy-vid-shahraystva-1676453413.html.

2. Рада утворила ТСК з питань розслідування шахрайства у сфері фінансових послуг. URL: https://www.ukrinform.ua/rubric-economy/3716087-rada-utvorila-tsk-z-pitan-rozsliduvanna-sahrajstva-u-sferi-finansovih-poslug.html.

3. Кришевич О. В. Шахрайство у сфері обігу банківських платіжних карток: кримінально-правовий аспект. С. 81-84. URL: http://elar.naiau.kiev.ua /bitstream/123456789/15212/1/%D0%97%D0%91I%D0%A0%D0%9D%D0%98%D0%9A_2019_p082-085.pdf.

4. Шахрайство з платіжними картками. URL: https://bankalliance.ua / pages/ about_us/Anti-fraud_26012021.pdf.

5. Соціальна інженерія (безпека). URL: https://uk.wikipedia.org/wiki/ Соціальна_інженерія_(безпека).

6. Федеральна торгова комісія США: За 2021 рік шахраї вкрали в користувачів соцмереж $700 мільйонів. URL: https://ms.detector.media/ sots merezhi/post/28876/2022-01-28- federalna-torgova- komisiya-ssha-za-2021-rik-shakhrai-vkraly-v-korystuvachiv-sotsmerezh-700-milyoniv/.

7. Кіберполіція попереджає про шахрайство під виглядом соціальних виплат. URL: https://cyberpolice.gov.ua/article/kiberpolicziya-poperedzhaye-pro-shaxrajstvo-pid-vyglyadom-soczialnyx-vyplat-7002/.

8. Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text.

9. НБУ назвав суму збитків від шахрайства з платіжними картками за останній рік. URL: https://news.finance.ua/ua/nbu-nazvav-sumu-zbytkiv-vid-shahraystva-z-platizhnymy-kartkamy-za-ostanniy-rik.

10. Статут Української міжбанківської Асоціації членів платіжних систем «ЄМА» (нова редакція). URL: https://drive.google.com/file/d/1 4XrIuFLzv DcdAlhlQXN wOVvkCUuOL-ip/view.

11. Матриця платіжного шахрайства. Перезавантаження: Аналіз, тренди та прогнози, 2022/2023. URL: https://www.ema.com.ua/news/matricja-platizhnogo-shahrajstva-perezavantazhennja-analiz-trendi-ta-prognozi-2022-2023/.

12. Стартувала інформаційна кампанія #ШахрайГудбай: нагадуємо про важливі правила платіжної безпеки. URL: https://bank.gov.ua/ua/news/ all/startuvala- informatsiyna- kampaniya- shahraygudbay- nagaduyemo-pro-vajlivi-pravila-platijnoyi-bezpeki.

13. З метою зниження ризиків шахрайства надавачі платіжних послуг застосуватимуть посилену автентифікацію. URL: https://bank.gov.ua/ua/ news/all/ z-metoyu-znijennya- rizikiv- shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500.

14. Як захистити свою платіжну картку від шахраїв. URL: https://minre. gov.ua/2023/03/19/yak- zahystyty-svoyu -platizhnu-kartku-vid shahrayiv/.

15. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. URL: *Науковий* вісник Ужгородського Національного Університету, 2021. С. 220–224.

16. Кіберполіція попереджає про шахрайство під виглядом соціальних виплат URL: .

17. План реалізації Стратегії кібербезпеки України: додаток до рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», уведеного в дію Указом Президента України від 1 лютого 2022 року № 37/2022. URL: https://zakon.rada.gov.ua /laws/show/n0087525-21#Text.

Bugera S.I. ON THE ISSUE OF COMBATING FRAUD WITH PAYMENT CARDS

The article discusses the issue of countering fraud with payment cards. It is emphasized that payment card fraud can be classified as: ATM fraud; fraud in the Card-Not-Present environment; fraud in the terminal network; social engineering. In order to counter fraud with payment cards, it is also important to use foreign experience in this matter. In particular, the use of electronic fraud prevention systems, as well as electronic means of control in the USA today is a priority and a component of the international policy on conducting electronic commercial activities. The experience of the USA can be adapted in Ukraine regarding: the creation of a Unified information system for the prevention of fraud in the field of electronic commerce and trade, which will combine various information resources, platforms and databases about fraudsters; reforming the institution of criminal responsibility for electronic trade and commercial fraud; use of the latest electronic systems and advances in artificial intelligence to prevent electronic commercial fraud; strengthening international cooperation and involving the public in social and educational work on the prevention of fraud in the field of electronic commerce. It has been established that countering fraud with payment cards requires a comprehensive solution. First of all, it is expedient to improve the legislation on this issue, in particular in terms of criminal responsibility. It is also important to study foreign experience in terms of the development of preventive measures at the special criminological and general social levels. At the same time, one of the most effective ways to counter fraud with payment cards remains the implementation of simple but effective rules by citizens, in particular: receive information, especially regarding financial payments, only from official sources; do not follow dubious hyperlinks; not to disclose confidential information, including bank card details, to third parties; in case of suspicion of fraudulent actions – immediately report to law enforcement agencies. Official pages of state bodies, charitable organizations, banking structures in messengers and social networks must be verified.

Key words: *payment cards, fraud, opposition, legislation, foreign experience.*