

УДК 343.37:336.717.1:[323.173+323.28]:658.14

JEL Classification: G21, K42, L14

Doi: 10.31767/su.2(101)2023.02.01

Т. Г. Бондарук,

доктор економічних наук, професор,
завідувач кафедри фінансів, банківської справи та страхування,
E-mail: bondaruk55@ukr.net
Researcher ID: Q-5166-2016,
ORCID: <https://orcid.org/0000-0001-9410-6428>;

Л. М. Богріновцева,

кандидат економічних наук, доцент,
доцент кафедри фінансів, банківської справи та страхування,
E-mail: kostrach26@gmail.com
ORCID: <https://orcid.org/0000-0001-9597-1085>;
Національна академія статистики, обліку та аудиту;

О. С. Бондарук,

кандидат економічних наук,
старший викладач кафедри фінансово-економічної безпеки,
Національна академія Служби безпеки України,
E-mail: bondaruk00001@gmail.com
Researcher ID: H-7703-2017,
ORCID: <https://orcid.org/0000-0002-3472-9516>

Шахрайство із використанням банківських платіжних карток як спосіб фінансування тероризму та сепаратизму

Обґрунтовано, що активізація тероризму та сепаратизму в Україні в період війни актуалізує завдання боротьби з їх фінансуванням. Завдяки різноманітності фінансових послуг та інструментів банківська сфера є привабливим об'єктом для застосування шахрайських схем. Відмивання коштів із використанням банківських платіжних карток і подальше фінансування тероризму та сепаратизму є важливою складовою злочинної діяльності. Мета статті – дослідження основних напрямів шахрайства із використанням банківських платіжних карток як способу фінансування тероризму і сепаратизму та визначення шляхів уникнення такої діяльності. У процесі дослідження використовувалися методи індукції, дедукції, системного підходу, логічного узагальнення, графічної візуалізації. Виявлено, що шахрайство набуває нових удосконалених форм і способів, найпоширенішими з яких є скімінг, кеш-трепінг, фішинг, телефонний дзвінок з метою отримати секретні дані. Обґрунтовано, що основними методами мінімізації рівня шахрайства з банківськими платіжними картками є забезпечення обізнаності та фінансової грамотності клієнтів банку в питаннях різних видів шахрайських дій, а також проведення модернізації та організація системи захисту програмного забезпечення банківської установи.

Встановлено, що сучасний стан диджиталізації банківського сектору створює нові ризики для шахрайства із використанням банківських платіжних карток для фінансування тероризму та сепаратизму. Обґрунтовано, що система протидії фінансуванню тероризму та сепаратизму через шахрайство передбачає такі механізми протидії, як ідентифікація фінансовими посередниками осіб, котрі звертаються за фінансовими послугами, та вивчення фінансових операцій, які проводяться такими особами, з метою виявлення тих, що можуть стосуватися фінансування тероризму та сепаратизму. В Україні у зоні ризику перебувають фінансові операції, які не підпадають під вимоги ідентифікації і можуть використовуватися для фінансування терористичних операцій та розгортання сепаратизму. А саме, ідеться про фінансові операції, що проводяться з допомогою платіжних систем.

Ключові слова: шахрайство, банківська сфера, фінансування тероризму і сепаратизму, банківські платіжні картки, фінансові операції.

Постановка проблеми. У часи війни активізація тероризму та сепаратизму в Україні зумовлює необхідність по-новому формулювати завдання боротьби з їх фінансуванням. За інформацією Служби безпеки України, на території України не

було структурних ланок міжнародних терористичних організацій, країна не зазнавала терористичних атак з їх боку й були відсутні передумови до виникнення терористичних проявів [1]. Ситуація кардинально змінилася на початку 2014 року. Подальше її погіршення після 24 лютого 2022 року

пов'язане з безпрецедентним проявом відкритої агресії – повномасштабним вторгненням РФ на територію України. Характер розвитку подій під час воєнного стану, особливо на перших етапах ескалації терористичної загрози та загрози сепаратизму в Україні, беззаперечно свідчить про використання фінансової системи з метою інтеграції та переспрямування фінансових потоків на підтримку цієї злочинної діяльності [1]. Високий рівень загрози терористичної та сепаратистської діяльності в Україні посилює як вразливість системи протидії фінансуванню такої діяльності, так і ризики фінансовій безпеці країни загалом [12].

Банківська сфера завдяки різноманітності фінансових послуг та інструментів є привабливим об'єктом для застосування шахрайських схем і в період війни. Відмивання коштів із використанням банківських платіжних карток та подальше фінансування тероризму і сепаратизму є важливою складовою злочинної діяльності. Розвиток новітніх фінансових технологій, поглиблення інформаційних зв'язків на міжнародному рівні значно вплинули на швидкість обігу коштів у банківській системі. Також урізноманітнилися форми розрахунків, у тому числі пов'язаних зі скоєнням фінансових злочинів, зокрема таких, як відмивання злочинних доходів для фінансування тероризму і сепаратизму. В умовах сьогодення все більшої популярності набирають інноваційні способи оплати, стрімко зростає обсяг безготівкових розрахунків із використанням банківських карток, що, своєю чергою, сприяє ефективному і прозорому функціонуванню економіки країни, зменшенню частки тіньового сектору економіки, а також скороченню витрат на обслуговування готівкового обігу. Поряд з цим поширення цього виду платіжного засобу призвело до зростання обсягів і урізноманітнення видів шахрайства у фінансовій сфері. Відповідальними при здійсненні розрахунків з допомогою банківської картки є банківські установи, які водночас самі зазнають шкоди від таких дій. Шахрайські схеми охоплюють практично всі сфери діяльності, починаючи від зовнішньоекономічної та завершуючи страховою і фінансово-кредитною діяльністю; велика частка протиправних дій здійснюється також через інтернет. Ураховуючи те, що нові технології – це не тільки нові можливості, а й нові ризики, слід приділили значну увагу дослідженню та мінімізації шахрайства із використанням банківських платіжних карток.

Аналіз останніх досліджень і публікацій. Дослідженню проблем фінансового шахрайства з використанням банківських платіжних карток присвячено значну кількість праць. Так, І. Домінова досліджувала джерела ризику шахрайства та види шахрайства з платіжними картками під час електронного банківського обслуговування, а також тенденції розвитку шахрайства на вітчизняному

фінансовому ринку [3]. Ю. Коцан-Олинець не лише аналізує сучасний стан шахрайства, вчиненого з використанням банківських платіжних карток, а й пропонує можливі напрями роботи із запобігання вчиненню таких злочинів пов'язаних із шахрайськими діями в банківській системі [4]. Форми, методи та засоби протидії корупційній злочинності розглядає у своїх працях С. Науменко (зокрема [5]). В. Пивоваров [9] досліджує шахрайство із банківськими картками з позицій способів його вчинення та висвітлює окремі питання віктимологічної профілактики. Незважаючи на широкий спектр досліджень за цією проблематикою та з огляду на швидкість розвитку технологій питання виявлення фінансового шахрайства та запобігання йому, насамперед у частині фінансування тероризму і сепаратизму в період війни, є важливими й актуальними.

Метою статті є дослідження основних видів шахрайства з використанням банківських платіжних карток як способу фінансування тероризму і сепаратизму та визначення шляхів його уникнення. У процесі дослідження використовувалися методи: індукції, дедукції, узагальнення – для уточнення теоретичних засад формування платіжних систем; системного підходу – для систематизації та узагальнення проблематики фінансового шахрайства; логічного узагальнення, графічного зображення – для візуалізації основних положень і висновків.

Виклад основного матеріалу дослідження. Різноманітні організаційні та фінансові інновації спрямовані на оптимізацію витрат, пов'язаних з фінансовими операціями, а також на скорочення часу, потрібного для їх проведення. Це, своєю чергою, сприяє безпечнішому й ефективнішому функціонуванню бізнесу.

На сьогодні банківська (платіжна) карта не є єдиним електронним платіжним засобом, з допомогою якого власник має можливість ініціювати переказ коштів, отримати готівку в касах банку чи банкоматах чи здійснювати інші операції. Поряд із банківською картою набув широкої популярності платіжний застосунок. Відповідно до Закону України “Про платіжні послуги”, платіжний застосунок – це програмне забезпечення, що дає змогу користувачу ініціювати платіжну операцію з рахунку платника (у тому числі з допомогою платіжних інструментів) та/або здійснювати інші операції, передбачені договором з надавачем платіжних послуг [10]. Зазначеним Законом переказ коштів без відкриття рахунку визначається як платіжна послуга, що надається платнику з метою переказу коштів у готівковій чи безготівковій формі отримувачу або надавачу платіжних послуг, який діє від імені отримувача, під час якої надавач цієї послуги не використовує відкритий у нього рахунок платника та/або отримувача [10].

Національний банк України описує платіжну картку як електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу коштів з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором [7].

Шахрайство з платіжними картками можна визначити як діяння, вчинене будь-якою особою, яка з наміром обману використовує банківську (платіжну) карту або платіжний застосунок, щоб зняти готівкові кошти чи здійснити послуги з виконання інших платіжних операцій без відома власника рахунку. Використання реквізитів картки без фізичного володіння нею вважається формою злочину.

Ризик фінансування тероризму та сепаратизму слід розглядати як похідну від загрози терористичної діяльності або сепаратизму та вразливості фінансової системи бути використаною з метою фінансування такої діяльності [1].

Банківські картки з'явилися у середині минулого століття більш як у 170 країнах світу і стали

незамінним інструментом розрахунку в усіх сферах діяльності. Водночас цей технологічний прорив супроводжується зростанням кількості шахрайських операцій з банківськими картками та рахунками, що відбуваються досить часто і стають усе більш поширеними в Україні. Зловмисники стають все винахідливішими й активно використовують сучасні технології, у чому їм значною мірою допомагає легковажність власників карток.

Важливим етапом технологічного розвитку у сфері безготівкових розрахунків з допомогою платіжних карток є запровадження безконтактних платіжних технологій, що в разі пришвидшило оплату. Технологія PayPass була запропонована та розроблена у 2002 р. компанією MasterCard і дозволяє зекономити 14 – 18 секунд. Своєю чергою, компанія Visa представила проєкт Visa PayWare, який з 2010 р. набув широкої популярності у країнах Європи, адже не потребує введення PIN-коду. Основні платіжні компанії світу – Visa, MasterCard, American Express – активно запроваджують безконтактні способи безготівкової оплати, базовий алгоритм якої представлено на рис. 1 (побудовано авторами).

Більша частина населення України (майже дві третини) вважають безконтактні платежі безпечними.

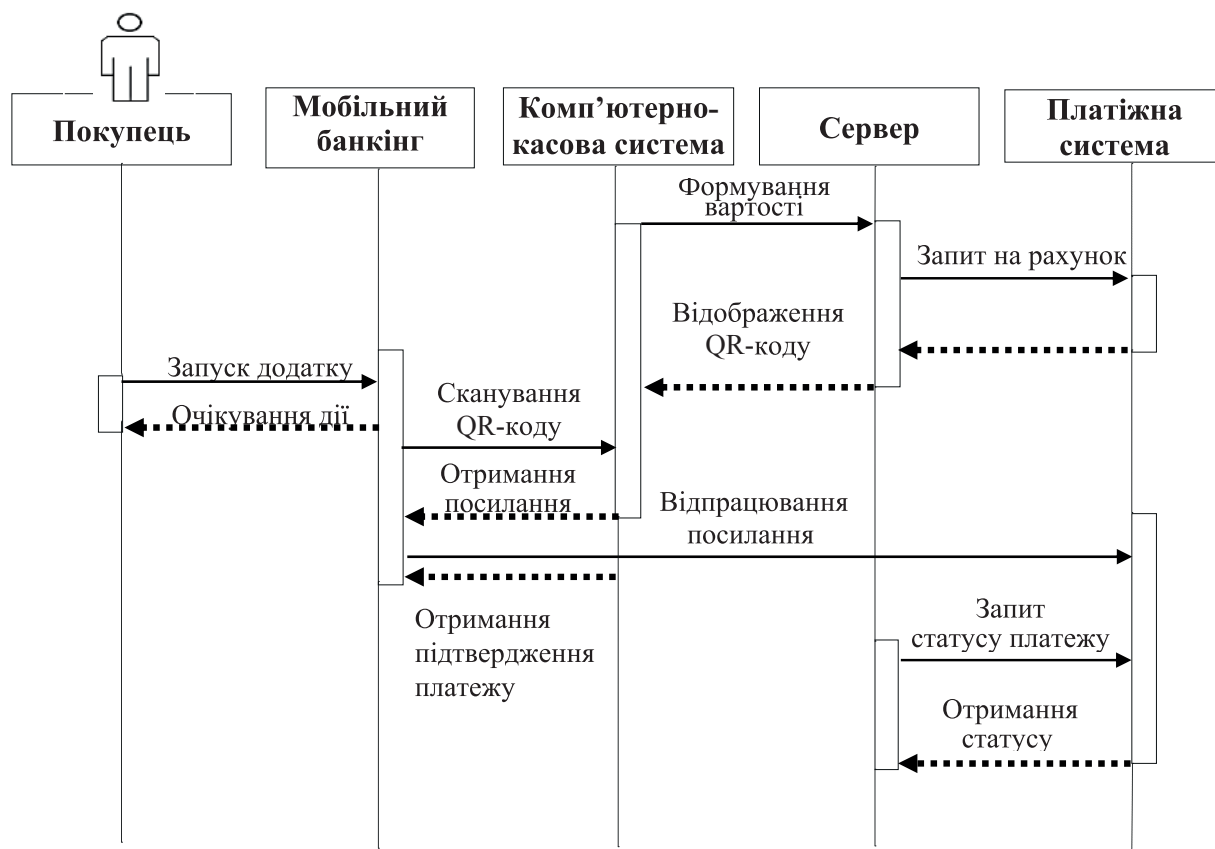


Рис. 1. Алгоритм безконтактної безготівкової оплати послуг

Існує декілька систем безконтактної оплати з мобільних пристроїв, до найбільш поширених належать Google Pay, Apple Pay та Samsung Pay. Усі вони працюють за схожими принципами, однак між ними існує ряд відмінностей. Спільним є те, що всі три системи підтримують технологію Near Field Communication (NFC, безконтактний зв'язок ближньої дії), яка полягає в обміні даними з платіжними терміналами, які також її підтримують. Водночас Samsung Pay реалізує власну технологію Magnetic secure transmission (MST, магнітна безпечна передача) – імітацію магнітного сигналу, який, імітуючи магнітну смугу пластикової карти, дозволяє проводити оплату майже на всіх терміналах, в тому числі й без підтримки NFC, що розширює можливості користувачів системи MST. В основі представлених систем лежить загальна ідея – токенизація платежів, яка дозволяє зробити транзакції безпечнішими.

Значна частина українців (60%) оплачують свої покупки безконтактним способом. Так, більше

половини (58%) використовували для безконтактної оплати банківські карти, а кожен четвертий (28%) платив за товари або послуги з допомогою смартфона, причому за рік число тих, хто використовував цей метод, зросло на 15%; оплату браслетом або смартгодинником здійснило 7% покупців. Ті, хто платив електронними пристроями, здійснювали оплату з допомогою сервісу Google Pay (44%), на другому місці – Apple Pay (33%), на третьому – Samsung Pay (11%).

Зберігається тенденція до поширення безконтактних платежів з допомогою смартфонів та інших NFC-пристроїв. Користувачі, знайомі з технологією безконтактної оплати, вважають її зручною та швидкою, зазначають зручність платежів з допомогою банківської карти (80%) і смартфона (70%), а також з допомогою смартгодинників (63%), браслетів (60%) та брелоків (46%). Схема оплати через NFC-модуль наведена на рис. 2 (побудовано авторами).

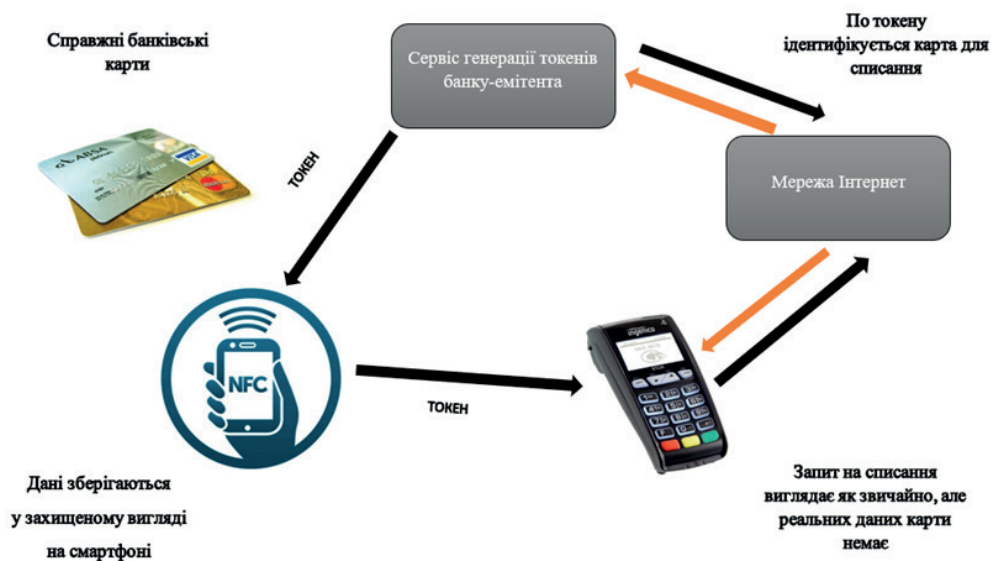


Рис. 2. Схема оплати через NFC-модуль

У 2017 році в Україні з'явився ще один спосіб безконтактної оплати, а саме NFC-кільце з чипом для оплати. В умовах сьогодення цей гаджет став доступним для широкого кола людей.

Водночас третина населення вважає, що безконтактні способи оплати є небезпечними і доступнішими для шахрайських операцій. З часом шахрайство набуває нових, удосконалених форм і способів, що зумовлено, насамперед, стрімким розвитком ІКТ. На сьогодні налічується близько 70 шахрайських схем із банківськими платіжними картками. До найпоширеніших схем належать скімінг, кеш-трепінг, фішинг, телефонний дзвінок з метою отримати секретні дані та ін. (рис. 3, побудовано авторами).

Розглянемо деякі з таких способів. Скімінг (Skimming) – це такий вид шахрайства, за якого зверху картрідера встановлюється (зазвичай на клей) пристрій під колір банкомату, який зчитує платіжні картки під час їх прийому. PIN-код фіксується накладкою на клавіатуру або встановленою неподалік камерою. Отримані дані використовуються шахраями для виготовлення дублікатів платіжних карток [8].

Кеш-трепінг (Cash trapping) – вид банкоматного шахрайства, коли в отвір для видачі готівки в банкоматі встановлюється планка з двостороннім скотчем для перехоплення готівки при видачі. У підсумку на екрані банкомата з'являється пові-

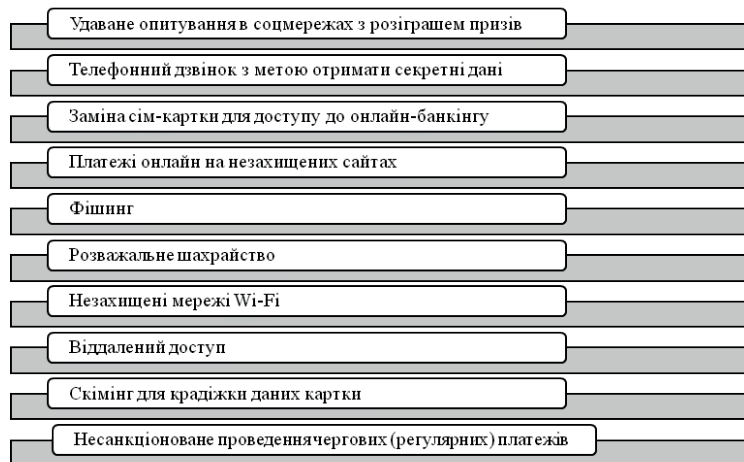


Рис. 3. Основні види шахрайства з банківськими картками

домлення про видачу коштів, клієнт отримує смс-повідомлення про списання грошей з рахунку, але гроші із банкомата так і не з'являються [2].

Зняття коштів із використанням банкомату без відображення цієї операції на рахунку (Transaction reversal fraud) – метод, який злочинці використовують для викрадення готівки в банкоматах. Цей вид шахрайства відбувається у два етапи:

1. Зловмисник самостійно здійснює операцію зі зняття готівки з банківської платіжної картки, під час якої у відкритий шаттер (диспенсер) розміщується спеціальний пристрій.

2. Зловмисник проводить операцію видачі готівки на максимально можливу суму, під час якої банкноти залишаються у спеціальному пристрої, а банкомат автоматично генерує операцію типу Reversal на картковий рахунок.

Результатом проведення цих операцій є те, що зловмисник отримує готівку, при цьому баланс карткового рахунку залишився практично незмінним.

Фішинг (Phishing) – вид інтернет-шахрайства, який використовує соціальну інженерію та масові розсилки спеціально сформованих електронних листів для отримання користувацьких даних або завантаження на пристрої небезпечних шкідливих програм [6]. Це відбувається через надсилання власнику картки листа із посиланням, адреса якого схожа на адресу реальної компанії. Після переходу за цим посиланням та зазначення даних, які використовуються власником для доступу до особистого кабінету або до інтернет-банкінгу, шахраям стають доступні персональні дані власника карти. Схема фішинг-шахрайства представлена на рис. 4 (побудовано авторами).

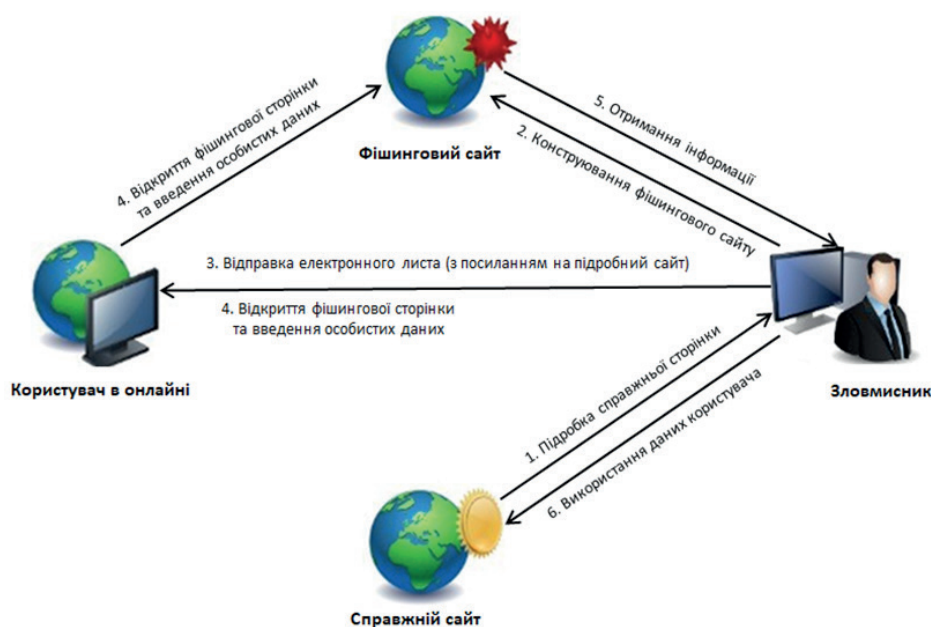


Рис. 4. Схема фішинг-шахрайства

Шахрайство з використанням телефонних дзвінків полягає в тому, що зловмисники телефонують тримачам картки, виступаючи агентом дохідних служб або банківським працівником, та намагаються викрасти інформацію про картку протягом дзвінка.

Дані статистики свідчать про загальну тенденцію до збільшення питомої ваги операцій з допомогою платіжних карток в об'ємі всіх операцій, здійснених без використання готівки. Найбільша частка операцій з допомогою платіжних карток має місце в таких країнах, як Саудівська Аравія (92,4%), Китай (82,4%), Канада (78,8%), Індія (63,5%), Швеція (66,5%).

За останні роки в Україні теж простежується стрімке зростання обсягу операцій з використанням платіжних карток (рис. 5, побудовано автора-

ми за даними [7]). На ринку банківських платіжних карток спостерігаються стабільно позитивні тенденції протягом усього аналізованого періоду. Поштовхом до збільшення кількості безготівкових операцій стали карантинні обмеження. За 2020 рік кількість таких операцій зросла на 18,3%, відповідно сума – на 8,7% порівняно з 2019 роком. Частка безготівкових операцій у 2020 році становила 55,2%, а отже, переважала у загальній сумі операцій із платіжними картками. У 2021 році кількість безготівкових операцій з використанням платіжних карток зросла на 35,1% порівняно з 2020 роком, відповідно їх сума зросла на 40,3%. Разом з тим кількість операцій з отримання готівки з допомогою платіжних карток у 2021 році зменшилася на 1,1% порівняно з попереднім роком, водночас їх сума зросла на 14,0%.

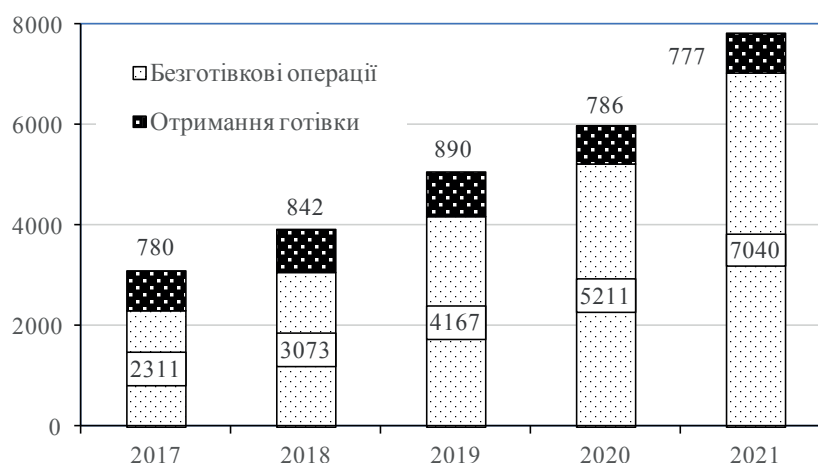


Рис. 5. Кількість операцій, здійснених з допомогою банківських платіжних карток, Україна, 2017–2021 рр., млн од.

Незважаючи на воєнні дії, у травні – грудні 2022 року кількість безготівкових операцій, здійснених з допомогою банківських платіжних карток, продовжувала зростати, за цей період вона становила 93% у загальній кількості операцій з платіжними картками [7]. Нагадаємо, що подання статистичної інформації у лютому – квітні 2022 року було призупинено Національним банком України (далі – НБУ).

За даними НБУ, у 2018 році порівняно з попереднім роком сума шахрайських операцій була значно меншою, а саме, викрадено 250 млн грн з рахунків клієнтів банку проти 600 млн грн у 2017 році. У 2018 році залученими до незаконних операцій були картки, емітовані 53-ма фінансовими установами, тоді як у 2017 році жертвами шахраїв були клієнти 41-го банку. Найбільш поширеним у той період був банкоматний скімінг, який встановлювали на банкомати у таких регіонах, як Київська область та м. Київ, м. Дніпро, Одеська область та м. Одеса [7].

У 2020 році кількість випадків шахрайства з банківськими рахунками та платіжними картками становила 101 000 та зросла на 29 000 порівняно з 2019 роком. У 2021 році на один мільйон гривень видаткових операцій з використанням платіжних карток обсяг збитків від шахрайських дій становив 65 грн (у 2020 році цей показник становив 48 грн). Упродовж 2022 року, під час повномасштабної війни в Україні, платіжне шахрайство не зникло, навіть спостерігалось суттєве збільшення його проявів. Національний банк України у 2022 році виявив близько 4500 фішингових ресурсів (у 2021 році цей показник був на порядок меншим). Найпоширенішим видом шахрайства у 2022 році стала фейкова соціальна допомога від міжнародних та державних організацій постраждалим під час війни українцям [7].

Методи виявлення шахрайства на кредитній картці класифікуються на дві загальні категорії: аналіз шахрайства (виявлення зловживання) та аналіз поведінки користувача (виявлення анома-

лії). Перша група методів стосується контролю за класифікацією на рівні транзакцій. У цих методах операції позначаються як шахрайські або звичайні на основі попередніх історичних даних. Потім набір даних використовується для створення моделей класифікації, які можуть передбачити стан (нормальний або шахрайський) за новими транзакціями. Існує безліч методів створення моделей для типової класифікації двох класів завдання, такі як індукція правил [13], дерева рішень [15], нейронні мережі [14] тощо. Використання цього підходу дозволяє виявити більшість прийомів шахрайства, які спостерігалися раніше. Другий підхід стосується методологій без нагляду, які базуються на поведінці під час проведення розрахунків. У цьому методі транзакція визначається як шахрайська, якщо вона суперечить нормальній поведінці користувача. Ми вважаємо, що шахраї поведуться не так само, як власник облікового запису, а також не знають модель поведінки власника. У рамках цього методу вибудовується законна поведінкова модель користувача для кожного облікового запису, яка потім зіставляється з фактичною поведінковою моделлю під час здійснення транзакції, що дає змогу виявити можливі шахрайські дії. Профілі можуть містити інформацію про діяльність власника облікового запису, яка стосується типу торговців, кількості, місця розташування та часу транзакцій.

Наразі в Україні також існує гостра потреба у розробленні ефективних заходів щодо запобігання фінансовому шахрайству в інвестиційно-будівельній сфері. У липні 2020 року НБУ запустив Всеукраїнську інформаційну кампанію з назвою “ШахрайГудбай”, метою якої стала протидія шахрайству, а її партнерами – близько 42-х банків України. Програма “ШахрайГудбай” містить інформацію про безпеку при здійсненні онлайн-покупок, про можливі випадки телефонного шахрайства, наголошуючи на важливості збереження конфіденційних даних картки [7]. 14 лютого 2022 року НБУ було проведено чергову Всеукраїнську інформаційну кампанію із назвою “ШахрайГудбай”, яка стала продовженням першої такої компанії, що успішно пройшла у 2020 році [7]. А з 03 травня 2023 року Національний банк України розпочав третю Всеукраїнську інформаційну кампанію з платіжної безпеки “ШахрайГудбай” [16]. Вона стала продовженням першої та другої подібних кампаній, що успішно пройшли у 2020–2022 роках.

15 лютого 2023 року НБУ повідомив про старт проекту з протидії кібершахрайству у фінансовому секторі, який був запущений Національним банком України та Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України. Головною метою цього проекту стало посилення захисту громадян від кіберзлочинців, які активізували свою діяльність у період воєнного стану в Україні [7].

Ключем до швидкого виявлення незаконних шахрайських операцій і запобігання їм, зокрема до скорочення збитків від подібної діяльності, є самі клієнти – власники рахунків, тому важливим є навчання клієнтів запобіганню шахрайству. Своєю чергою, банкам для запобігання ризику шахрайських дій при онлайн-обслуговуванні необхідно вибудувати чітку систему виявлення та мінімізації цих ризиків. Отже, основними методами мінімізації рівня шахрайства з банківськими платіжними картками є:

1) забезпечення обізнаності та фінансової грамотності клієнтів банку в питаннях щодо різних видів шахрайських дій з метою скорочення фінансових втрат;

2) проведення модернізації та організація захисту власного програмного забезпечення банківської установи відповідно до сучасних вимог безпеки, а також формування системи безперервного моніторингу для виявлення й аналізу нових форм шахрайства [11].

Висновки та перспективи подальших досліджень. Узагальнення вищевикладеного матеріалу дає змогу сформулювати висновок про активний розвиток ринку банківських платіжних карток в Україні, що підтверджується збільшенням частки активних операцій за картками, зростанням обсягів та кількості безготівкових транзакцій. Серед основних проблем, що перешкоджають розвитку безготівкових операцій, усе ще залишаються недовіра частини клієнтів до інтернет-банкінгу, недосконалість ідентифікації клієнтів та страх шахрайства.

Сучасний стан диджиталізації банківського сектору створює нові ризики для шахрайства із використанням банківських платіжних карток і подальшого фінансування тероризму та сепаратизму. Водночас при цьому виникають нові можливості та рішення для тих, хто відповідає за активи банку та захист клієнтів. Зважаючи на взаємозв'язок між ризиками шахрайства та новими технологіями, банкам слід значну увагу приділяти розробці й удосконаленню засобів запобігання шахрайству, перешкоджати злочинам у фінансовій сфері, інвестувати у нові технології, створені для виявлення та попередження про можливі випадки шахрайства, включаючи повідомлення про шахрайські дії в реальному часі, розпізнавання відбитків, голосу й обличчя.

Система протидії фінансуванню тероризму та сепаратизму шляхом шахрайства передбачає насамперед такі механізми протидії, як ідентифікація фінансовими посередниками осіб, котрі звертаються за фінансовими послугами, та вивчення фінансових операцій, що проводяться такими особами, з метою виявлення тих, які не підпадають під вимоги ідентифікації, а отже, можуть здійснювати фінансування злочинної діяльності.

Подальші дослідження спрямовуватимуться на пошук та поглиблене висвітлення оптимальних методів мінімізації ризику шахрайства з застосуванням платіжних застосунків в умовах функціонування інтернет-банкінгу.

Список використаних джерел

1. Актуальні методи, способи та фінансові інструменти фінансування тероризму та сепаратизму. Державна служба фінансового моніторингу України. 2014. URL: https://fiu.gov.ua/assets/userfiles/411/Типолог%20ДСФМУ/2014%2012%2029_tipolog2014.pdf (дата звернення: 10.05.2023).
2. Дубровик-Рохова А. Що потрібно знати про “фішинг”, “вішинг” і “кеш-треппінг”? *День*. 2017. № 18–19. URL: <https://day.kyiv.ua/uk/article/ekonomika/shcho-potribno-znaty-pro-fishyng-vishyng-i-kesh-trepping> (дата звернення: 10.05.2023).
3. Домінова І. В. Ризик шахрайства в умовах функціонування електронного банкінгу. *Бізнес-навігатор*. 2017. № 4. С. 92–98. URL: http://business-navigator.ks.ua/journals/2017/43_2_2017/20.pdf (дата звернення: 10.05.2023).
4. Заріцька О. С., Коцан-Олинець Ю. Я. Види шахрайства з банківськими картками та способи протидії їх проявам. Вісник Львівського торговельно-економічного університету. *Юридичні науки*. 2019. № 8. С. 95–100. DOI: <https://doi.org/10.36477/2616-7611-2019-08-10> (дата звернення: 10.05.2023).
5. Науменко С. Г. Шахрайство у сфері обігу банківських платіжних карток. *Корупційна злочинність у міжнародному вимірі: форми, методи та засоби протидії: мат. Міжнар. круглого столу* (Київ, 9–10 листоп. 2017 р.). Київ: Нац. акад. внутр. справ, 2017. С. 183–187. URL: https://www.naiu.kiev.ua/files/naukova-diyalnist/naukovi-zahodi/zbirniki/2017/mater_verstka_091117.pdf (дата звернення: 10.05.2023).
6. Яременко Р. Фішинг з юридичним присмаком: як не втрапити на гачок? *Liga Zakon*. 2019. URL: https://biz.ligazakon.net/analytics/186819_fshing-z-yuridichnim-prismakom-yak-ne-vtrapiti-na-gachok (дата звернення: 10.05.2023).
7. Офіційне Інтернет-представництво Національного банку України. URL: <https://bank.gov.ua/> (дата звернення: 10.05.2023).
8. Офіційний сайт Промінвестбанку. Практичні рекомендації. URL: https://www.pib.ua/private/pocket_offers/useful_information/recommendations/ (дата звернення: 10.05.2023).
9. Пивоваров В. В., Терещенко К. В. Шахрайство із банківськими картками: окремі питання віктимологічної профілактики. *Карпатський правничий часопис*. 2015. № 10. С. 132–137. URL: https://dspace.nlu.edu.ua/bitstream/123456789/9954/1/Pivovarov_132-137.pdf (дата звернення: 10.05.2023).
10. Про платіжні послуги: Закон України від 30.06.2021 р. № 1591-IX, станом на 01.04.2023 р. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text>
11. Рекомендації для зниження ризику шахрайських операцій: Лист Національного банку України від 04.07.2018 р. № 57-0009/36366. URL: <https://zakon.rada.gov.ua/laws/show/v3636500-18> (дата звернення: 10.05.2023).
12. Bondaruk T., Momotiuk L., Zaichko I. Budgetary policy of Ukraine in time of challenges and its impact on financial security. *Statistics in transition new series and Statistics of Ukraine*. 2022. Vol. 23. № 5. P. 185–208. URL: https://sit.stat.gov.pl/SiT/OnlineFirst/05_Taisiia%20Bondaruk%20%20sit%2023%205p.pdf (дата звернення: 10.05.2023).
13. Chaudhary K., Yadav J., Mallick B. A review of Fraud Detection Techniques: Credit Card. *International Journal of Computer Applications*. 2012. Vol. 45. № 1. P. 39–44. URL: <https://research.ijcaonline.org/volume45/number1/pxc3878991.pdf> (дата звернення: 10.05.2023).
14. Delamaire L., Abdou H., Pointon J. Credit card fraud and detection techniques: a review. *Banks and Bank Systems*. 2009. Vol. 4. URL: https://www.researchgate.net/publication/40227011_Credit_card_fraud_and_detection_techniques_A_review (дата звернення: 10.05.2023).
15. Edge M., Sampaio P. A survey of signature based methods for financial fraud detection. *Journal of computers and security*. 2009. Vol. 28, Issue 6. P. 381–394. <https://doi.org/10.1016/j.cose.2009.02.001> (дата звернення: 10.05.2023).
16. Стартувала інформаційна кампанія #ШахрайГудбай: нагадуємо про важливі правила платіжної безпеки. Офіційне Інтернет-представництво Національного банку України. 03.05.2023. URL: <https://bank.gov.ua/ua/news/all/startuvala-informatsiy-na-kampaniya-shahraygudbay-nagaduyemo-pro-vajlivi-pravila-platijnovi-bezpeki> (дата звернення: 10.05.2023).

References

1. Aktualni metody, sposoby ta finansovi instrumenty finansuvannya teroryzmu ta separatyizmu [Actual techniques, methods and financial instruments of financing terrorism and separatism]. (2014). State

Financial Monitoring Service of Ukraine. *fiu.gov.ua*. Retrieved May 10, 2023 from https://fiu.gov.ua/assets/userfiles/411/Типолог%20ДСФМУ/2014%2012%2029_tipolog2014.pdf [in Ukrainian].

2. Dubrovnyk-Rokhova, A. (2017). Shcho potribno znaty pro “fishynh”, “vishynh” i “kesh-treppinh”? [What do you need to know about “Phishing”, “Vishing” and “Cash Trapping”?]. *Den – Day*, 18–19. Retrieved from <https://day.kyiv.ua/uk/article/ekonomika/shcho-potribno-znaty-pro-fishyng-vishyng-i-kesh-trepping> [in Ukrainian].

3. Dominova, I. V. (2017). Ryzyk shakhraistva v umovakh funktsionuvannia elektronnoho bankinhu [The fraud risk under conditions of electronic banking]. *Biznes-navihator – Business navigator*, 4, 92–98. Retrieved from http://business-navigator.ks.ua/journals/2017/43_2_2017/20.pdf [in Ukrainian].

4. Zaritska, O. S., & Kotsan-Olinets, U. Ya. (2019). Vydy shakhraistva z bankivskymy kartkamy ta sposoby protydyi yikh proiavam [Types of Fraud with Banking Cards and Ways to Counteract Its Manifestations]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu. Yurydychni nauky – Herald of Lviv University of Trade and Economics. Legal sciences*, 8, 95–100. Retrieved from <https://doi.org/10.36477/2616-7611-2019-08-10> [in Ukrainian].

5. Naumenko, S. H. (2017). Shakhraistvo u sferi obihu bankivskykh platizhnykh kartok [Fraud in the field of circulation of bank payment cards]. Proceedings from Koruptsiina zlochynnist u mizhnarodnomu vymiri: formy, metody ta zasoby protydyi: *Mizhnarodnyi kruhlyi stol (9–10 lystopada 2017 r.) – International round table*. (pp. 183–187). Kyiv: Natsionalna akademiia vnutrishnikh sprav. Retrieved from https://www.naiu.kiev.ua/files/naukova-diyalnist/naukovi-zaxodi/zbirniki/2017/mater_verstka_091117.pdf [in Ukrainian].

6. Yaremenko, R. (2019). Fishynh z yurydychnym prysmakom: yak ne vtrapyty na hachok? [Phishing with a legal flavor: how not to get caught?]. *Liga Zakon*. Retrieved from https://biz.ligazakon.net/analitics/186819_fshing-z-yuridichnim-prismakom-yak-ne-vtrapiti-na-gachok [in Ukrainian].

7. Ofitsiine Internet-predstavnytstvo Natsionalnoho banku Ukrainy [Official website of the National Bank of Ukraine]. *bank.gov.ua*. Retrieved from <https://bank.gov.ua/> [in Ukrainian].

8. Praktychni rekomendatsii. Ofitsiyni sait Prominvestbanku [Useful recommendations. Official website of the Prominvestbank]. *www.pib.ua*. Retrieved from https://www.pib.ua/private/pocket_offers/useful_information/recommendations/ [in Ukrainian].

9. Pyvovarov, V. V., & Tereshchenko, K. V. (2015). Shakhraistvo iz bankivskymy kartkamy: okremi pytannia viktymologichnoi profilaktyky [Bank card fraud: specific issues of victimological prevention]. *Karpatskyi pravnychy chasopys – Carpathian law journal*, 10, 132–137. Retrieved from https://dspace.nlu.edu.ua/bitstream/123456789/9954/1/Pivovarov_132-137.pdf [in Ukrainian].

10. Pro platizhni posluhy: Zakon Ukrainy vid 30.06.2021 r. № 1591-IX, stanom na 01.04.2023 r. [On payment services. Law of Ukraine of June 30, 2021 No. 1591-IX, as of April 1, 2023]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/1591-20#Text> [in Ukrainian].

11. Rekomendatsii dlia znyzhennia ryzyku shakhraiskykh operatsii: Lyst Natsionalnoho banku Ukrainy vid 04.07.2018 r. № 57-0009/36366 [Recommendations for reducing the risk of fraudulent transactions. Letter of the National Bank of Ukraine of July 4, 2018 No. 57-0009/36366]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/v3636500-18> [in Ukrainian].

12. Bondaruk, T., Momotiuk, L., & Zaichko, I. (2022). Budgetary policy of Ukraine in time of challenges and its impact on financial security. *Statistics in transition new series and Statistics of Ukraine*, 23 (5), 185–208. Retrieved from https://sit.stat.gov.pl/SiT/OnlineFirst/05_Taisiia%20Bondaruk%20%20sit%2023%205p.pdf

13. Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of Fraud Detection Techniques: Credit Card. *International Journal of Computer Applications*, 45 (1), 39–44. Retrieved from <https://research.ijcaonline.org/volume45/number1/pxc3878991.pdf>

14. Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, 4. Retrieved from https://www.researchgate.net/publication/40227011_Credit_card_fraud_and_detection_techniques_A_review

15. Edge M., & Sampaio P. (2009). A survey of signature based methods for financial fraud detection. *Journal of computers and security*, 28 (6), 381–394. Retrieved from <https://doi.org/10.1016/j.cose.2009.02.001>

16. Startuvala informatsiina kampaniia #ShakhrayGoodBye: nahadiemo pro vazhlyvi pravyla platizhnoi bezpeky [The information campaign #FraudsterGoodBye ShakhrayGoodbye was launched: we remind you about the important rules of payment security]. (2023). Official website of the National Bank of Ukraine. *bank.gov.ua*. Retrieved from <https://bank.gov.ua/ua/news/all/startuvala-informatsiyna-kapaniya-shakhraygudbay-nagadyemo-pro-vajlyvi-pravila-platijnoyi-bezpeki> [in Ukrainian].

T. G. Bondaruk,*DSc in Economics, Professor,**Acting Head of the Finance, Banking and Insurance Department,**E-mail: bondaruk55@ukr.net**Researcher ID: Q-5166-2016,**ORCID: <https://orcid.org/0000-0001-9410-6428>;***L. M. Bohrinovtseva,***PhD in Economics, Associate Professor,**Associate Professor of the Finance, Banking and Insurance Department,**E-mail: kostrach26@gmail.com**ORCID: <https://orcid.org/0000-0001-9597-1085>;**National Academy of Statistics, Accounting and Audit;***O. S. Bondaruk,***PhD in Economics,**Assistant Professor of the Department of Financial and Economic Security,**National Academy of the Security Service of Ukraine,**E-mail: bondaruk00001@gmail.com**Researcher ID: H-7703-2017,**ORCID: <https://orcid.org/0000-0002-3472-9516>*

Fraud Using Bank Payment Cards: A Way for Financing of Terrorism and Separatism

It is substantiated that intensification of terrorism and separatism in Ukraine in time of war rises the priority of problems related with fight against their financing. The banking system, offering a diversity of financial services and tools, is an attractive object for using fraudulent schemes. Money laundering using bank payment cards and with further financing of terrorism and separatism is a significant component of criminal activities. The article's objective is to explore the main categories of fraud using bank payment cards as a way for financing of terrorism and separatism, and to determine methods for elimination of these activities. The research process involved methods of induction, deduction, system approach, logical generalization, graphic visualization. It was revealed that the fraud was taking new and more sophisticated forms and ways, of which the most common ones were skimming, cash trapping, fishing, or phone call to obtain secret data. It is argued that the principal methods for minimizing the fraud with bank payment cards is raising awareness and financial literacy of bank clients in issues related with various categories of fraudulent actions, as well as modernization and upgrading the software protection system in a bank.

It is determined that the current phase of digitalization in the bank sector creates new risks of fraud using bank payment cards for financing of terrorism and separatism. It is substantiated that the system designed to counteract financing of terrorism and separatism by way of fraud involves two mechanisms: identification, by bank employees, of persons applying to banks for financial services, and surveillance of financial transactions made by these persons, to detect the ones that may involve financing terrorism and separatism. The risk zone in Ukraine spreads on the financial transactions that, not being subject to identification, may be used to finance terrorist actions or support separatism. It refers to the financial transactions made by use of payment systems.

Key words: *fraud, bank sector, financing of terrorism and separatism, bank payment cards, financial transactions*

Бібліографічний опис для цитування:

Бондарук Т. Г., Богріновцева Л. М., Бондарук О. С. Шахрайство із використанням банківських платіжних карток як спосіб фінансування тероризму та сепаратизму. *Статистика України*. 2023. № 2. С. 4–13. Doi: 10.31767/su.2(101)2023.02.01

Bibliographic description for quoting:

Bondaruk, T. G., Bohrinovtseva, L. M., & Bondaruk, O. S. (2023). Shakhraistvo iz vykorystanniam bankivskykh platizhnykh kartok yak sposib finansuvannia teroryzmu ta separatyzmu [Fraud Using Bank Payment Cards: A Way for Financing of Terrorism and Separatism]. *Statystyka Ukrainy – Statistics of Ukraine*, 2, 4–13. Doi: 10.31767/su.2(101)2023.02.01 [in Ukrainian].