

ГАЛИНСЬКА КАРІНА ЮРІЇВНА

кандидатка юридичних наук, асистентка кафедри
фінансового права Національного юридичного
університету імені Ярослава Мудрого
ORCID 0009-0000-7856-8665

АРТЕМЕНКО КСЕНІЯ ВАЛЕРІЇВНА

студентка IV курсу факультету прокуратури На-
ціонального юридичного університету імені Яро-
слава Мудрого

БОРИЩАК ВАЛЕРІЯ ОЛЕКСІЇВНА

студентка IV курсу факультету прокуратури На-
ціонального юридичного університету імені Яро-
слава Мудрого

УДК 347.73:347.734: 336.717: 343.35
DOI 10.37772/2518-1718-2024-3(47)-25

Р2Р ПЕРЕКАЗИ: СУЧАСНА ХАРАКТЕРИСТИКА В КОНТЕКСТІ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЮ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Сьогодні Р2Р (peer-to-peer) перекази з картки на картку стали невід’ємною частиною нашого повсякденного життя. Це зручний спосіб швидко і зручно здійснити переказ коштів без посередників, банківських черг або складних процедур. Завдяки сучасним цифровим технологіям такі перекази здійснюються в лічені секунди через мобільні додатки, інтернет-банкінг або спеціалізовані сервіси, що забезпечує максимальну швидкість і простоту фінансових операцій.

Очевидно, що Р2Р перекази відкривають нові можливості для взаємодії між різними суб’єктами, роблячи фінансові послуги доступнішими, зручнішими та з низькою вартістю. Але до того ж такі платежі повинні характеризуватися безпечним користуванням та прозорістю, що є двома найбільш важливими характеристиками для тих, хто завдяки цим рішенням часто вперше стикається зі світом фінансових послуг. Тож, у цій статті розглянуто основні переваги, можливості, дискусійні аспекти Р2Р переказів, а також їх вплив на фінансову безпеку держави.

У статті акцентовано увагу на положеннях постанови Національного банку України щодо карткових обмежень на перекази між фізичними особами, що базується на рішенні РНБО щодо протидії нелегальному гральному бізнесу. Водночас констатовано, що запровадження таких обмежень має й інший контекст, у тому числі, протидія запобігання незадекларованим доходам суб’єктів господарювання, боротьба з тінзовим обігом коштів і фінансовими махінаціями відомими як дропи («мулінг грошей»). Проаналізовано правове підґрунтя для створення безпечного середовища фінансовим установам задля проведення транзакцій і зменшення небезпечних переказів як «мулінг грошей».

Здійснено детальний аналіз такого явища як фінансовий мулінг, що полягає в незаконній передачі або пере-
міщенні грошових коштів через посередників, які використовуються для злочинної діяльності. Розглянуто осно-
вні механізми залучення осіб до цього процесу, способи, якими злочинні угруповання використовують фінансові
мули для відмивання грошей, а також правові наслідки для тих, осіб, які приймають участь у таких схемах. По-
значено міжнародний досвід притягнення до кримінальної відповідальності таких осіб, засоби для створення
безпечного середовища фінансовим установам задля проведення транзакцій.

Ключові слова: цифровізація, банк, фінансова безпека, відмивання грошей, відповідальність, банківський
рахунок, гроші, переказ коштів, Р2Р-платіж, транзакція, дроп, фінансовий мул, KYC, FATF, AMLD5, AML.

Постановка проблеми. Перекази з картки на картку, також відомі як P2P (peer-to-peer, card2card або C2C) дозволяють одній людині миттєво переказувати гроші іншій через цифрову платформу, як правило, додаток, де гроші вносяться з банківського рахунку, кредитної чи дебетової картки або поповненням рахунку готівкою. Послуга доступна для цифрових гаманців, додатків, які відрізняються від більш традиційних способів оплати низькою вартістю, тоді як стандартні версії часто безкоштовні, а також тим, що їх легко вивчити та використовувати. Платіжні системи P2P інтегрують сучасні цифрові технології для спрощення фінансових операцій між користувачами. Позначимо, що наразі доволі розповсюдженими системами P2P, якими користується велика кількість осіб – є PayPal, Apple Pay та ін.

Використання платіжних інструментів P2P, які відносяться до групи альтернативних платежів, різко зростає в останні кілька років. Згідно з дослідженням, опублікованим Statista, у 2022 року транзакції з альтернативними платежами досягнули глобальної вартості близько 14 трильйонів доларів США завдяки зростанню каналів електронної комерції та дедалі частішому використанню безконтактних платежів у магазинах і загалом в альтернативних формах (наприклад, інтерактивні тотеми з сенсорним екраном, сканери для самообслуговування тощо) [1].

Поширення використання P2P-платежу у проведеному дослідженні вимагає їх детального аналізу в кількох площинах. По-перше, з позицій безпеки і захисту даних, адже очевидним є те, що зростання кількості P2P-транзакцій робить їх привабливими для шахраїв. Тож виникає нагальна потреба у дослідженні того, як забезпечується захист особистих даних користувачів і які технології використовуються для запобігання несанкціонованим переказам. По-друге, важливим є належне їх правове підґрунтя. Це пов'язано із тим, що P2P-платежі іноді можуть виходити за межі традиційного банківського регулювання. І це актуалізує їх розгляд з точки зору правового регулювання таких транзакцій, позначення вимог, які висуваються до них, а також яким чином захищаються права споживачів. По-третє, з точки зору технологічних інновацій. Справа у тому, що P2P-платежі розвиваються завдяки новим цифровим технологіям, таким як блокчейн, мобільні додатки, біометрична аутентифікація. Тож це обумовлює позначення їх взаємозв'язків. По-четверте, економічний вплив: збільшення частки P2P-платежів може мати значний вплив на фінансовий сектор та економіку в цілому. Важливо дослідити, як цей процес впливає на традиційні банківські послуги, ринок платіжних систем і споживчі звички.

Аналіз останніх досліджень і публікацій. Позначимо, що до вивчення проблем грошових пере-

казів, протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, цифрових новацій у сфері грошового обігу і розрахунків були додичні низка науковців як економістів, так і правників: Децик О., Головей Є., Сталіров В., Прокопошина О., Пилипенко П.М., Маллорі М., Ключко А. М., Волченко Н. В., Дмитрик О. О., Маринів Н.А., Парашенко О.К., Овчаренко А.С. та ін. Поряд із тим позначена тематика не втрачає своєї актуальності і потребує подальшого розгляду.

Метою статті є визначення концепції P2P-платежу, аналіз переваг та дискусійних аспектів такого роду з точки зору забезпечення фінансової безпеки, протидії відмиванню грошей.

Виклад основного матеріалу. Платіжні сервіси P2P використовують електронний переказ коштів (EFT) – процес переміщення грошей з одного рахунку на інший в електронному вигляді. EFT може включати прямі депозити, банківські перекази, оплати рахунків в Інтернеті, а також операції з дебетовими та кредитними картками. Можна стверджувати, що платіжні сервіси P2P – це особливий вид EFT, який дозволяє прив'язати відповідний банківський рахунок, дебетову або кредитну картку до додатку або платформи, а потім використовувати його з метою переказу грошей [1]. Так, сьогодні одним із найпопулярніших сервісів P2P-платежів є PayPal, Venmo, Cash App та Zelle.

Водночас, незважаючи на таку популярність, за допомогою P2P-платежу набуває поширення один з видів легалізації (відмивання) грошей, що має назву мулінг грошей (money muling) (по-іншому ще називають «дроп»).

Легалізація (відмивання) доходів, отриманих незаконним шляхом, відповідно до ст. 5 Закону України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» включає будь-які дії, що пов'язані з проведенням фінансових операцій або угод з такими доходами, а також заходи, спрямовані на приховування чи маскуванню їх незаконного походження, права власності на них, джерел їх походження, місцезнаходження, переміщення або зміну форми. Також це стосується придбання, володіння чи використання доходів, отриманих у результаті злочинної діяльності [2].

Відповідно до роз'яснення, опублікованого на офіційному сайті Міністерства внутрішніх справ України, дропи (або ж «грошові мули») – це особи, які за певну винагороду надають зловмисникам доступ до своїх банківських рахунків і карток. Ці фінансові інструменти використовуються як проміжні для переказів грошей різних сум між рахунками. Зловмисники використовують дропи для маскуванню

своїх дій та ускладнення роботи правоохоронців під час розслідування злочинів. Тобто «грошові мули» безпосередньо не причетні до злочинів, які генерують гроші (кіберзлочинність, онлайн-шахрайство, наркотики, торгівля людьми тощо), вони є співучасниками, оскільки відмивають доходи, отримані від таких злочинів. Простіше кажучи, грошові мули допомагають злочинним синдикатам залишатися анонімними під час переміщення коштів по всьому світу [3].

Процес грошового мулінгу залежить від здатності знайти особу для переказу коштів з одного рахунку на інший. Мулів вербують злочинці, і ці вербувальники мулів також відомі як «пастухи». Мули відкривають новий банківський рахунок і отримують гроші від третьої сторони на свої банківські рахунки, а потім незаконно переказують їх комусь іншому, дозволяючи злочинцям залишатися анонімними, переміщуючи кошти по всьому світу. Мули отримують компенсацію за свою участь, зазвичай у формі грошей.

Прокопишина О. зазначає, що мули транспортують кошти в ланцюжку подібних транзитних рахунків, який може складатися з декількох мулів (5 і більше). У свою чергу, це дозволяє мулам замести сліди, влаштувати так званий «міксер», коли неможливо зібрати історію транзакцій, розходяться суми та контрагенти. І поки регулятор комунікує з тим чи іншим банком щодо підозрілих дій клієнтів та отримання доступу до інформації платіжних карток, «життя» одного грошового мула чи навіть цілого ланцюжка може закінчитися [4].

Характерно, що особи можуть погодитися стати грошовими мулами, не знаючи мети транзакцій. Більше того, деякі особи навіть не усвідомлюють, що беруть участь у злочинній діяльності. Водночас, деякі особи усвідомлюють наслідки, але погоджуються на такі дії за грошову винагороду.

Аналіз алгоритму, що використовується для такого відмивання грошей, дозволяє стверджувати, що нові банківські рахунки для переказу грошей, відкриті мулами, служать початковим етапом процесу відмивання. Етап розшарування передбачає приховування джерела грошей через низку транзакцій. Це дозволяє інтегрувати початкові незаконно зароблені гроші назад в економіку.

Що стосується видів грошових мулів, то їх можна згрупувати таким чином:

1) несвідомі, тобто ті, які не розуміють, що вони є частиною такої схеми відмивання грошей. Зазвичай їх запрошують через пропозицію на роботу або через схему романтичних стосунків в Інтернеті – є довіра до шахрая та віра у реальне існування посади на роботі, або романтичних стосунків.

2) свідомі (кмітливі), ті які ігнорують свою діяльність з шахрайством. Наприклад, банк, у якому

відкрила людина картку, зробив попередження про існування шахрайської діяльності, натомість така особа, може спочатку і ненавмисно, але продовжує брати участь у мулінгу грошей. У такої людини виникає мотивація продовжувати злочинні дії – фінансова вигода.

3) співучасники, тобто виконує будь-яку роль, чи то серійно відкриває банківські рахунки для отримання грошей, чи керує рахунками, чи рекламує послуги як грошовий мул, чи наймає інших грошових мулів [5].

Позначимо, що гроші, які обертаються через рахунки дропів, часто є здобутими незаконним шляхом, наприклад, через торгівлю наркотиками, людьми, зброєю тощо. Також рахунки дропів можуть використовуватися для ухилення від податків або для переведення коштів, викрадених з інших рахунків.

«Грошових мулів» можуть залучати на постійній основі, коли вони самі переказують отримані кошти за вказівками та отримують свій відсоток, або одноразово, коли дроп надає банківські картки з пінкодами та доступом до інтернет-банкінгу за разову плату [3].

Наведемо декілька статистичних даних. Так, за проведеним дослідженням від UK Finance ми бачимо, що у 2020 році було понад 17 000 підозрюваних у грошових мулах, у яких фігурували 21-30-річні особи, що на п'ять відсотків більше, ніж у попередньому році [6]. За даними Європолу, найбільше об'єктом нападу є ті особи, що тільки що прибули в країну, безробітні та студенти, які страждають від фінансових труднощів. Як правило, це особи у віці до 35 років, однак Європол виявив тенденцію, відповідно до якої сьогодні організовані злочинні групи почали націлюватися на молодше покоління (від 12 до 21 року) [7].

Показово, що сьогодні фахівцями наводяться типові характеристики дропів. Наприклад, це може бути студент (19 років), який має розмір доходу до 20 тисяч гривень, у якого у перший тиждень після відкриття картки по рахунку здійснено 55 переказів на 274 тисяч гривень. У підсумку за 7 місяців обсяг операцій зарахувань склав 2,8 млн. грн. по усім рахункам клієнта відкритих у двох банків. А ось інший приклад: безробітна особа з села (20 років), розмір доходу якої складає 8 тис. грн., відкриває рахунок в одному з банків України і через 3 місяці після відкриття рахунку і «неактивного» періоду, починає різко відправки переказів Р2Р. Загалом сума зарахувань становила 1 млн. гривень за один місяць! [8].

Міжнародний досвід свідчить про активну боротьбу з таким видом відмивання грошей як мулінг. Це відбувається перед усім шляхом встановлення кримінальної відповідальності за даний злочин, а також чіткого позначення правил грошового обігу

[5-12]. Приміром, ФБР вказує, що будь-який грошовий мул може бути притягнутий до відповідальності та ув'язнений за різними звинуваченнями, як-от шахрайство з електронним зв'язком, банківське шахрайство, відмивання грошей і викрадення особистих даних. З точки зору США, федеральне агентство додає, що робота в якості грошових мулів може завдати шкоди особистому кредитному рейтингу, а також фінансовому становищу [5].

Що стосується України, то за даними Національного банку України, у 2023 році обсяги переказів за допомогою карток Р2Р стабільно зростали – від 210 млрд грн у січні до 247 млрд у грудні, перевищивши обсяги покупок і зняття готівки через платіжні картки. У НБУ вважають, що це свідчить про певну «аномальну активність у цьому сегменті платіжних операцій». Інакше кажучи, це може бути ознакою збільшення тіншових фінансових операцій, які використовуються для ухилення від сплати податків або відмивання незаконно отриманих коштів [13].

З метою запобігання розповсюдження розгляданого явища Правлінням Національного банку України було прийнято постанову «Про внесення змін до постанови Правління Національного банку України від 24 лютого 2022 року № 18» №102 від 27 серпня 2024 року [14]. В цій постанові закріплено ліміт у 150 тис. грн. на місяць для переказів фізичних осіб з картки на картку, дія якого розпочинається з 1 жовтня 2024 року до 31 березня 2025 року включно [14]. Аналіз цього нормативно-правового акту дозволяє зробити наступні висновки:

1) ліміт не застосовується у разі переказу коштів між власними рахунками клієнта відкритими в одному банку та до переказів юридичних осіб;

2) ліміт не застосовується, якщо оплата здійснюється на банківський рахунок фізичної особи за реквізитами IBAN;

3) банкам надано право не застосовувати ліміт щодо переказів окремих категорій фізичних осіб, які не є суб'єктами господарської діяльності та займаються волонтерською діяльністю, тобто волонтери.

Як вбачається, запровадження такого заходу за метою НБУ пов'язано із тим, що ліміт стане засобом для мінімізації використання платіжної інфраструктури у відмиванні доходів, зокрема, з використанням рахунків дропів.

Поряд із тим, потребує вирішення проблема, що пов'язана із перевіркою переказів надавачами платіжних послуг, а також створенням внутрішніх документів щодо незастосування заборони проведення платежів, які перебільшують ліміт понад 150 тис.грн. Це, приміром, стосується руху коштів на рахунках волонтерів (як що широко подивитися на цей аспект, що він буде стосуватися як визначення правового статусу особи, яка займається волонтерською діяль-

ністю, так і критеріїв для підтвердження її переказів, адже у вище вказаній постанові застосовуються такі оціночні категорії, як «типову діяльність як волонтера», «інформація з відкритих джерел, що є підтвердженням даної діяльності» та ін. [14])

Показово, що однією з найбільш поширених процедур, яка вже використовується в українських банках та бізнесі для перевірки особи – це KYC (Know Your Customer). Так, KYC – це комплекс заходів і процедур, які фінансові установи та інші компанії використовують для ідентифікації та верифікації особистості своїх клієнтів. Головною метою KYC є захист як банку, так і фінансових ринків загалом від незаконної діяльності. Це включає участь у шахрайстві, відмиванні грошей, корупції чи хабарництва [15]. До речі, у багатьох країнах діють нормативно-правові акти для забезпечення виконання та регулювання процесів KYC. Вперше вони були запроваджені Групою розробки фінансових заходів протидії відмиванню грошей (FATF) у 1990-х роках, а найновіші впровадження почалося в США з Патріотичним актом у 2001 році. Загалом понад 190 країн дотримуються вказівок FATF щодо KYC [15].

Відповідно до KYC процедура складається з трьох компонентів:

1) програма ідентифікації клієнтів (CIP) – підтвердження особи і витребування таких даних як ПІБ, дата народження, адреса проживання або ж ідентифікаційний номер;

2) належна перевірка клієнта (CDD) – оцінка ризиків для надавача платіжних послуг, зокрема щодо географічного розташування, перегляд кредитної історії, перевірка щодо застосування санкцій до особи, вчинення певних фінансових злочинів і тд. З цього етапу впливає інший, якщо потрібно провести детальнішу перевірку і має назву EDD – включає збір додаткових документів, дослідження походження коштів, моніторинг транзакцій;

3) регулярний моніторинг – тобто здійснення KYC повинно бути безперервним, адже «чисті» транзакції можуть стати сумнівними операціями [16].

Ще однією з критично важливих основ, яка підтримує фінансову безпеку, дотримання регуляторних норм та етичність ведення бізнесу є система заходів і законодавчих вимог – AML (Anti-Money Laundering), яка спрямована на запобігання відмиванню грошей та фінансуванню тероризму. Вона включає в себе процедури, які зобов'язані виконувати фінансові установи, банки та інші компанії для виявлення та попередження використання своїх послуг з метою легалізації незаконно отриманих. Так, практика боротьби з відмиванням коштів - це не просто регуляторні зобов'язання, а важливі заходи, які підтримують доброчесність банківського сектору та довіру суспільства до нього коштів [17].

Впровадження ефективних заходів протидії відмиванню коштів та фінансуванню тероризму у банках передбачає поєднання стратегічного нагляду, детальних процедурних завдань та безперервного навчання персоналу з метою дотримання суворих регуляторних стандартів та ефективної боротьби з фінансовими злочинами.

Ще одним способом задля покращення моніторингу переказу коштів виступають біометричні технології. Пов'язуючи біометричні дані з конкретними транзакціями, банки можуть більш точно відстежувати та аналізувати поведінку клієнтів у часі. Як зазначається науковцями, виявлення аномалій за допомогою використання біометричних даних дозволяє виявляти відхилення в транзакційній діяльності, що можуть свідчити про несанкціоновані або шахрайські дії. Це може призвести до генерації сповіщень для подальшого розслідування. Наприклад, біометрична автентифікація в банкоматах або під час онлайн-операцій допомагає пов'язувати транзакції з конкретними особами, що підвищує ефективність систем виявлення шахрайства. Так, використовуючи біометричні дані посилюється безпека для високо ризикованих транзакцій, для операцій з великими сумами або тих, що мають підвищений ризик, біометрична автентифікація забезпечує додатковий рівень захисту, підтверджуючи, що особа, яка виконує транзакцію, є законним власником рахунку [16].

Очевидно, що це може дозволити банкам позначити типову поведінку своїх клієнтів за допомогою профілювання користувачів і відхилень від нормальної поведінки, які можуть вказувати на активність рахунків-мулів, використовуючи аналіз подій і поведінкову біометрію. Ці рішення вже довели свою ефективність у протидії шахрайським атакам на захоплення облікового запису (АТО). Ретельно перевіряючи такі параметри, як взаємодія із сенсорним екраном, активність натискання клавіш, рухи миші, орієнтація пристрою та керування ним, поведінкова біометрія використовується в тандемі з розвідкою про події з інших методів виявлення, таких як відбитки пальців пристрою, аналіз геолокації та аналіз IP, щоб побудувати профіль кожного з них. поведінка користувача. Ці профілі історичної поведінки користувачів потім порівнюються з кожним новим запитом користувача, щоб перевірити, чи дійсно особа за екраном є законним клієнтом, ефективно відрізнявши їх від потенційних злочинців [19].

Науковці зауважують, що масштабне впровадження біометричних технологій у банківській сфері в Україні стане можливим тоді, коли споживачі банківських послуг усвідомлять переваги цих технологій, а також буде запроваджене належне правове регулювання роботи біометричних систем [20].

У 2024 році ЄС опублікував шостий пакет директив під назвою AMLD6 (Anti-Money Laundering Directives) Боротьба з відмиванням грошей [21]. AMLD6 закликає держави-члени переслідувати «посередників», які допомагають здійснювати незаконну діяльність. Також переглядається те, як країни-члени мають здійснювати кримінальне переслідування, і AMLD6 прагне покращити стримуючий ефект існуючого законодавства шляхом застосування суворіших покарань. Країни-члени ЄС тепер зобов'язані запроваджувати принаймні чотири роки позбавлення волі за серйозні злочини, пов'язані з відмиванням грошей, із суворішими покараннями для рецидивістів. Також застосовуються значні фінансові штрафи (до 5 мільйонів євро для фізичних осіб), щоб позбавити винних будь-якого прибутку, отриманого від незаконної діяльності [21].

Маллорі М. зауважає, що впровадження пакету директив має значні наслідки для підприємств і фінансових установ. Відтепер компанії повинні будуть захищати себе від комплаєнс-ризиків і запроваджувати відповідні механізми та системи контролю, проводити регулярні аудити та підвищувати обізнаність своїх співробітників. Це включає інвестиції в передові технології моніторингу й аналізу транзакцій для завчасного виявлення підозрілої фінансової діяльності. Ці дії необхідні для захисту цілісності компанії, уникнення суворих покарань і підтримки довіри зацікавлених сторін [22].

Досліджуючи тему обробки персональних даних, не треба оминати й Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (GDPR) [23]. Так, у документі зазначено про основоположні засади, які повинні бути дотримані при використанні та обробці персональних даних, зокрема законності, справедливості, прозорості, мінімальна, але точна інформація про клієнта, конфіденційність та підзвітність.

Сталіров В. зазначає про декілька прикладів порушення GDPR. Так, з такою вимогою як повнота не впорався шведський Klarna Bank, внаслідок чого Управління захисту даних Швеції наклало на банк штраф у розмірі 720 000 EUR. Банк не надав клієнтам інформацію про цілі та правові підстави обробки їх даних; одержувачів та країни за межами ЄС, яким передаються дані; права суб'єктів даних.

Порушення принципу точності призводить до штрафів. Так, румунська філія Raiffeisen Bank порушила принцип точності, коли обробляла недостовірні дані клієнтів. Розслідування розпочалося за скаргою заявника, який отримував текстові SMS-повідомлення про грошові перекази, які він не робив. Виявилося, що номер заявника помилково ввели в

додаток банку, але GDPR вимагає, щоб дані регулярно актуалізувалися та перевірялися. Тому Raiffeisen Bank сплатив штраф у 2000 EUR [24].

Зважаючи на євроінтеграційний вектор розвитку національного законодавства, не можна оминати нещодавньої новини щодо ухвалення законопроекту про ратифікацію угоди між Україною та Європейським Союзом про участь у програмі ЄС щодо боротьби із шахрайством (EUAF). Заступник міністра фінансів України з питань європейської інтеграції, Юрій Драганчук зазначив, що участь України у програмі ЄС щодо боротьби із шахрайством дасть нам змогу отримати необхідні знання та професійну підготовку у сфері захисту фінансових інтересів України та ЄС, а також зміцнить інституційну спроможність України в розбудові системи боротьби з шахрайством за європейськими стандартами [25]. Це буде гарним початком для встановлення співпраці та використання новітніх ІТ-технологій у боротьбі з фінансовими злочинами, зокрема таким як мулінг грошей.

Висновки. P2P платежі представляють собою важливу цифрову технологічну інновацію в сфері обігу грошей, що забезпечує користувачам можливість здійснювати перекази безпосередньо, без за-

лучення посередників, таких як банки або платіжні системи. Однак, поряд із перевагами, такими як швидкість і зручність, існують суттєві ризики, пов'язані з безпекою таких операцій. При цьому, однією з ключових вразливостей P2P-платежів є ризик їх використання для відмивання грошей через механізм «мулінг грошей».

Подібні способи не лише сприяють поширенню фінансових злочинів, але й створюють загрозу для фінансової системи держави в цілому. Незважаючи на впровадження механізмів захисту, до кола яких можна віднести ідентифікацію користувачів, за допомогою біометричних даних, моніторинг транзакцій, впровадження КУС та дотримання нормативно-правової системи AML, питання відмивання грошей залишається і надалі актуальним. Це підкреслює необхідність подальших наукових досліджень у сфері безпеки P2P-платежів, зокрема: щодо розробки більш досконалих інноваційних технологій для виявлення та попередження схем відмивання грошей, впровадження та удосконалення правового регулювання даних тем, а також встановлення відповідальності за таке правопорушення як «мулінг грошей».

ЛІТЕРАТУРА

1. P2P Payments (Peer-to-Peer payments): how they work. *Fabrick S.p.A.* 29 August 2023. URL: <https://www.fabrick.com/en-gb/insights/blog/p2p-payments/#:~:text=P2P,%20meaning%20peer-to-,with%20a%20cash%20top-up>.
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 р. № 361-IX. URL: <https://zakon.rada.gov.ua/go/361-20>
3. Схема з дроп-картами: що це і як не стати пособником шахраїв. *Міністерство внутрішніх справ України*. 20 лютого 2024. URL: <https://mvs.gov.ua/news/sxema-z-drop-kartami-shho-ce-i-iak-ne-stati-posobnikom-saxrayiv>
4. Prokopyshina O. In the fight against drops, the National Bank restricts transfers of citizens, the National Police proposes to imprison them. *Buhgalter 911*. 20 September, 2024. URL: <https://buhgalter911.com/en/news/news-1081293.html>
5. Scams and Safety. Money Mules. *FBI*. URL: <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules>
6. Money mule recruiters use fake online job adverts to target «Generation Covid? *UK Finance*. URL: <https://www.ukfinance.org.uk/press/press-release/money-mule-recruiters-use-fake-online-job-adverts-to-target-generation-covid>
7. Money Muling : guide. *Europol*. 20 June 2023. URL: <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
8. Боротьба з дропами: НБУ готується обмежити перекази, Нацполіція пропонує запровадити відповідальність. *Юридична газета*. 23 серпня 2024. URL: <https://yur-gazeta.com/golovna/borotba-z-dropami-nbu-gotuetsya-obmezhati-perekazi-nacpoliciya-proponue-zaprovaditi-vidpovidalnist.html#:~:text=Так,%20дропа%20або%20»грошові%20мули,грошових%20операцій%20на%20інші%20рахунки>
9. Money Mules (also known as Squaring). *West Yorkshire Police*. 2024. URL: <https://www.westyorkshire.police.uk/advice/fraud-and-financial-crime/fraud-and-financial-crime/money-mules-also-known-squaring>
10. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016ME/TXT>

11. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018L1673>
12. Директива Європейського Парламенту і Ради (ЄС) 2018/843 від 30 травня 2018 року про внесення змін до Директиви (ЄС) 2015/849 про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму та про внесення змін до директив 2009/138/ЄС і 2013/36/ЄС : Директива; Європейський Союз від 30.05.2018 № 2018/843. URL: https://zakon.rada.gov.ua/go/984_010-18
13. Дацик О. Дропи, міскодинг, розірваний платіж. Причини введення лімітів на карткові перекази. *LIGA*. 31 травня 2024. URL: <https://finance.liga.net/ua/bank/article/dropy-miskodynkh-rozirvaniy-platizh-prychyny-vvedennia-limitiv-na-kartkovi-pereказы>
14. Про внесення змін до постанови Правління Національного банку України від 24 лютого 2022 року № 18 : Постанова Правління Національного банку України від 09.07.2024 № 83. URL: https://bank.gov.ua/ua/legislation/Resolution_09072024_83
15. Houton J. 3 KYC components every financial institution must follow. *IDnow*. URL: <https://www.idnow.io/blog/financial-institution-kyc-components/>
16. Сталіров В. Що таке KYC у криптоіндустрії і чому ця процедура є обов'язковою? *Stalirov.Lawyer*. 23 квітня 2024. URL: [https://stalirov.lawyer/uk/posts/kyc-sho-ce-za-perevirka-v-kriptoindustriyi#:~:text=Know%20Your%20Customer%20\(KYC\)%20%E2%80%94,%D0%B4%D0%BE%D0%BF%D0%BE%D0%BC%D0%B0%D0%B3%D0%B0%D1%94%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%8F%D0%BC%20%D0%B2%D0%B8%D0%BA%D0%BE%D0%BD%D1%83%D0%B2%D0%B0%D1%82%D0%B8%20%D0%B2%D0%B8%D0%BC%D0%BE%D0%B3%D0%B8%20AML](https://stalirov.lawyer/uk/posts/kyc-sho-ce-za-perevirka-v-kriptoindustriyi#:~:text=Know%20Your%20Customer%20(KYC)%20%E2%80%94,%D0%B4%D0%BE%D0%BF%D0%BE%D0%BC%D0%B0%D0%B3%D0%B0%D1%94%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%8F%D0%BC%20%D0%B2%D0%B8%D0%BA%D0%BE%D0%BD%D1%83%D0%B2%D0%B0%D1%82%D0%B8%20%D0%B2%D0%B8%D0%BC%D0%BE%D0%B3%D0%B8%20AML)
17. Anti-Money Laundering (AML) in Banking: Why It Matters?. *ARATEK*. 22 April, 2024. URL: <https://www.aratek.co/news/anti-money-laundering-aml-in-banking-why-it-matters>
18. Пилипенко П. М., Артеменко К. В. Деякі проблеми інтеграції технології блокчейн в контексті трансформації фінансового сектору. *Правові новели*. 2024. № 22. С. 110–117. URL: <https://doi.org/10.32782/ln.2024.22.15>
19. Preventing Money Mules: The Impact of Behavioral Analytics in Financial Security. *Transmit Security*. November 1, 2023. URL: <https://transmitsecurity.com/blog/preventing-money-mules-the-impact-of-behavioral-analytics-in-financial-security>
20. Ключко А. М., Волченко Н. В. Біометричні технології для безпеки проведення банківських операцій в Україні та зарубіжних державах. *Часопис Київського університету права*. 2021. № 1. С. 299–304. URL: <https://doi.org/10.36695/2219-5521.1.2021.59>
21. Anti-money laundering: Council adopts package of rules. *Council of the EU*. 30 May 2024. URL: <https://www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/>
22. Mallaury M. AML compliance in 2024: Assessing the effectiveness of AMLD6 and EU's new AML package. *IDnow*. 2024. URL: <https://www.idnow.io/blog/aml-compliance-2024-aml6/>
23. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент; Європейський Союз від 27.04.2016 р. № 2016/679. URL: https://zakon.rada.gov.ua/go/984_008-16
24. Сталіров В. GDPR compliance: що це та кому потрібно виконати умови регламенту про захист персональних даних? *Stalirov.Lawyer*. 12 жовтня 2022. URL: <https://stalirov.lawyer/uk/posts/gdpr-dlya-ukrayins-kih-it-kompanij>
25. Мінфін: Верховна Рада ратифікувала Угоду про участь України у програмі ЄС по боротьбі із шахрайством (EUF). *Міністерство Фінансів України*. 20 серпня 2024. URL: https://mof.gov.ua/uk/news/minfin_verkhovna_rada_ratifikuvala_ugodu_pro_uchast_ukraini_u_programi_ies_po_borotbi_iz_shakhraistvom_euaf-4750

REFERENCES

1. Fabrick S.p.A. (2023, August 29). *P2P Payments (Peer-to-Peer payments): How they work*. Retrieved from: <https://www.fabrick.com/en-gb/insights/blog/p2p-payments/#:~:text=P2P,%20meaning%20peer-to-,with%20a%20cash%20top-up>
2. Law of Ukraine On Prevention and Counteraction to Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of the Proliferation of Weapons of Mass Destruction: No. 361-IX (2019, December 6). Retrieved from: <https://zakon.rada.gov.ua/go/361-20> [in Ukrainian].

3. Ministerstvo vnutrishnikh sprav Ukrainy. (2024, February 20). *Scheme with Drop Cards: What It Is and How Not to Become an Accomplice to Fraudsters*. Retrieved from: <https://mvs.gov.ua/news/sxema-z-drop-kartami-shho-ce-i-iak-ne-stati-posobnikom-saxrayiv> [in Ukrainian].
4. Prokopyshina, O. (2024, September 20). In the fight against drops, the National Bank restricts transfers of citizens, the National Police proposes to imprison them. *Buhgalter 911*. Retrieved from: <https://buhgalter911.com/en/news/news-1081293.html> [in Ukrainian].
5. FBI. Scams and Safety: Money Mules. Retrieved from: <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules>
6. UK Finance. *Money mule recruiters use fake online job adverts to target «Generation Covid.»* Retrieved from. URL: <https://www.ukfinance.org.uk/press/press-release/money-mule-recruiters-use-fake-online-job-adverts-to-target-generation-covid>
7. Europol. (2023, June 20). *Money Muling: Guide*. Retrieved from: <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
8. Fighting Drops: The National Bank Prepares to Limit Transfers, the National Police Proposes to Introduce Responsibility. *Yurydychna hazeta*. (2024, August 23). Retrieved from: <https://yur-gazeta.com/golovna/borotba-z-dropami-nbu-gotuetsya-obmezhati-perekazi-nacpoliciya-proponue-zaprovaditi-vidpovidalnist.html#:~:text=Так,%20дропи%20або%20«грошові%20мули,грошових%20операцій%20на%20інші%20рахунки> [in Ukrainian].
9. West Yorkshire Police. (2024). *Money Mules (also known as Squaring)*. Retrieved from: <https://www.westyorkshire.police.uk/advice/fraud-and-financial-crime/fraud-and-financial-crime/money-mules-also-known-squaring>
10. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016ME/TXT>
11. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018L1673>
12. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Retrieved from: https://zakon.rada.gov.ua/go/984_010-18 [in Ukrainian].
13. Datsyk, O. (2024, May 31). Drops, miscoding, broken payment: Reasons for introducing limits on card transfers. *LIGA..* Retrieved from: <https://finance.liga.net/ua/bank/article/dropy-miskodynh-rozirvanyi-platizh-prychyny-vvedennia-limitiv-na-kartkovi-perekazy> [in Ukrainian].
14. Resolution of the Board of the National Bank of Ukraine On Amendments to the Resolution of the Board of the National Bank of Ukraine No. 18 of February 24, 2022: No. 83 (2024, July 9). Retrieved from: https://bank.gov.ua/ua/legislation/Resolution_09072024_83 [in Ukrainian].
15. Houton J. 3 KYC components every financial institution must follow. *IDnow*. Retrieved from: <https://www.idnow.io/blog/financial-institution-kyc-components/>
16. Stalirov, V. (2024, April 23). What is KYC in the crypto industry and why is this procedure mandatory?. *Stalirov. Lawyer*. Retrieved from: [https://stalirov.lawyer/uk/posts/kyc-sho-ce-za-perevirka-v-kriptointistriyi#:~:text=Know%20Your%20Customer%20\(KYC\)%20%E2%80%94,%D0%B4%D0%BE%D0%BF%D0%BE%D0%BC%D0%B0%D0%B3%D0%B0%D1%94%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%8F%D0%BC%20%D0%B2%D0%B8%D0%BA%D0%BE%D0%BD%D1%83%D0%B2%D0%B0%D1%82%D0%B8%20%D0%B2%D0%B8%D0%BC%D0%BE%D0%B3%D0%B8%20AML](https://stalirov.lawyer/uk/posts/kyc-sho-ce-za-perevirka-v-kriptointistriyi#:~:text=Know%20Your%20Customer%20(KYC)%20%E2%80%94,%D0%B4%D0%BE%D0%BF%D0%BE%D0%BC%D0%B0%D0%B3%D0%B0%D1%94%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%8F%D0%BC%20%D0%B2%D0%B8%D0%BA%D0%BE%D0%BD%D1%83%D0%B2%D0%B0%D1%82%D0%B8%20%D0%B2%D0%B8%D0%BC%D0%BE%D0%B3%D0%B8%20AML) [in Ukrainian].
17. ARATEK. (2024, April 22). *Anti-Money Laundering (AML) in Banking: Why It Matters?*. Retrieved from: <https://www.aratek.co/news/anti-money-laundering-aml-in-banking-why-it-matters>
18. Pylypenko, P. M., & Artemenko, K. V. (2024). Some problems of blockchain technology integration in the context of the financial sector transformation. *Pravovi novely*, 22, 110–117. Retrieved from: <https://doi.org/10.32782/In.2024.22.15> [in Ukrainian].
19. Transmit Security. (2023, November 1). *Preventing Money Mules: The Impact of Behavioral Analytics in Financial Security*. Retrieved from: <https://transmitsecurity.com/blog/preventing-money-mules-the-impact-of-behavioral-analytics-in-financial-security>

20. Klochko, A. M., & Volchenko, N. V. (2021). Biometric technologies for security of banking operations in Ukraine and foreign countries. *Chasopys Kyivskoho universytetu prava, 1*, 299–304. Retrieved from: <https://doi.org/10.36695/2219-5521.1.2021.59> [in Ukrainian].
21. Council of the EU. (2024, May 30). *Anti-money laundering: Council adopts package of rules*. Retrieved from: <https://www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/>
22. Mallaury M. (2024). AML compliance in 2024: Assessing the effectiveness of AMLD6 and EU's new AML package. *IDnow*. Retrieved from: <https://www.idnow.io/blog/aml-compliance-2024-amld6/> [in Ukrainian].
23. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from: https://zakon.rada.gov.ua/go/984_008-16 [in Ukrainian].
24. Stalirov, V. (2022, October 12). GDPR compliance: What it is and who needs to comply with the data protection regulation. *Stalirov.Lawyer*. Retrieved from: <https://stalirov.lawyer/uk/posts/gdpr-dlya-ukrayins-kih-it-kompanij> [in Ukrainian].
25. Ministerstvo Finansiv Ukrainy. (2024, August 20). *Ministry of Finance: Verkhovna Rada ratified the Agreement on Ukraine's participation in the EU anti-fraud program (EUAF)*. Retrieved from: https://mof.gov.ua/uk/news/minfin_verkhovna_rada_ratifikuvala_ugodu_pro_uchast_ukraini_u_programi_ies_po_borotbi_iz_shakhraistvom_euaf-4750 [in Ukrainian].

HALYNSKA KARINA

PhD in Law, Assistant at the Department of Financial Law
of the Yaroslav Mudryi National Law University

ARTEMENKO KSENIA

student of the Faculty of Prosecutor's Office
of the Yaroslav Mudryi National Law University

BORYSHCHAK VALERIA

student of the Faculty of Prosecutor's Office
of the Yaroslav Mudryi National Law University

P2P TRANSFERS: MODERN CHARACTERISTICS IN THE CONTEXT OF PREVENTION AND ANTI-LAUNDERING (LAUNDERING) OF INCOME OBTAINED BY CRIMINAL WAYS

Problem setting. Nowadays, P2P (peer-to-peer) card-to-card transfers have become an integral part of our daily lives. It is a convenient way to transfer money quickly and securely without intermediaries, bank queues or complicated procedures. Thanks to modern technology such transfers are made in seconds via mobile applications, internet banking or specialised services ensuring maximum speed and simplicity of financial transactions.

P2P transfers open up new opportunities for people to interact with each other making financial services more accessible, convenient and low-cost. But at the same time, such payments should be characterized by secure use and transparency which are two of the most important features for those who often first encounter the world of financial services through these solutions.

Purpose of research is to define the concept of P2P payment, analyze the advantages and debatable aspects of this kind from the point of view of ensuring financial security, combating money laundering.

Analysis of recent researches and publications. Scientists, economists and lawyers, contributed to the study of the problems of money transfers, combating the legalization (laundering) of proceeds obtained through crime, digital innovations in the field of money circulation and calculations: O. Decyk, E. Golovei, V. Stalirov, O. Prokoposhina, Pylypen-

ko P.M., Mallory M., Klochko A.M., Volchenko N.V., Dmytryk O.O., Maryniv N.A., Parashchenko O.K., Ovcharenko A.S. etc. At the same time, the indicated topic does not lose its relevance and needs further consideration.

Article's main body. In this article we will look at the main advantages and disadvantages, the possibilities of P2P transfers, their impact on the development of financial technologies as well as the security nuances that should be taken into account when conducting such transactions.

The article is focused on the decision of the National Bank of Ukraine on card restrictions on transfers between individuals this restriction is based on the decision of the National Security and Defence Council of Ukraine to combat illegal gambling but in fact the goal is much broader, including countering hidden business profits and unofficial wages as well as combating financial fraud known as money laundering. It is analysed that the legal regulations to create a safe environment for financial institutions to conduct transactions and reduce unsafe money mulesing transfers.

The article is provided a detailed analysis of the phenomenon of financial mulling which is the illegal transfer or movement of funds through intermediaries used for criminal activities. The authores analyses that the main mechanisms of involvement of individuals in this process the ways in which criminal groups use financial mules for money laundering as well as the risks and legal consequences for those who become involved in such schemes, including international experience of bringing to criminal responsibility. It also examined the legal regulators and tools to create a secure environment for financial institutions to conduct transactions.

Conclusions and prospects for the development. P2P payments represent an important digital technological innovation in the field of money circulation, which provides users with the ability to make transfers directly, without the involvement of intermediaries such as banks or payment systems. However, along with advantages such as speed and convenience, there are significant risks associated with the security of such operations. At the same time, one of the key vulnerabilities of P2P payments is the risk of their use for money laundering through the “money muling” mechanism.

Such methods not only contribute to the spread of financial crimes, but also create a threat to the financial system of the state as a whole. Despite the implementation of protection mechanisms, which include identification of users using biometric data, monitoring of transactions, implementation of KYC and compliance with the AML regulatory framework, the issue of money laundering remains relevant. This emphasizes the need for further scientific research in the field of security of P2P payments, in particular: regarding the development of more advanced innovative technologies for the detection and prevention of money laundering schemes, the implementation and improvement of legal regulation of these topics, as well as the establishment of liability for such an offense as “money laundering”.

Keywords: peer-to-peer (P2P), digitization, bank, financial security, money laundering, liability, bank account, money, fund transfer, P2P payment, transaction, drop, financial sludge, KYC, FATE, AMLD5, AML.

За ДСТУ 8302:2015 цю статтю слід цитувати:

Галинська К. Ю., Артеменко К. В., Борищак В. О. P2P перекази: сучасна характеристика в контексті запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом. *Право та інновації*. 2024. № 3 (47). С. 187–196.