nia podatku na maino" [About Diagnosis of the Local Taxation System in Ukraine and Decentralization of Property tax Administration]. *U-LEAD z Yevropoiu*. https://hromady.org/wp-content/uploads/2023/07/2_3006_ULEAD.pdf

Pasichnyi, M. "Yak posylyty finansovu spromozhnist terytorialnykh hromad?" [How to Strengthen the Financial Capacity of Territorial Communities?]. *LB.ua*. September 28, 2023. https://lb.ua/blog/mykola_pasichnyi/576952_yak_posiliti_finansovu_spromozhnist.html

Shvabii, K. et al. "Diahnostyka systemy mistsevoho opodatkuvannia Ukrainy: analitychnyi zvit. U-LEAD z Yevropoiu" [Diagnostics of the Local Taxation System of Ukraine: Analytical Report]. *U-LEAD with Europe*. 2023. https://u-lead.org.ua/storage/admin/files/d7ee40daa7f8543c84903bb0b76b51dd.pdf

Tesliuk, N. P., Nazarenko, Ya. Ya., and Nakonechna, S. A. "Transportnyi podatok ta yoho rol u formuvanni mistsevykh biudzhetiv" [Transport Tax and Its Role in the Formation of Local Budgets]. *Efektyvna ekonomika*, no. 2 (2021). DOI: https://doi.org/10.32702/2307-2105-2021.2.75

"Valovyi vnutrishnii produkt (VVP) v Ukraini 2024" [Gross Domestic Product (GDP) in Ukraine 2024]. *Minfin*. https://index.minfin.com.ua/ua/economy/gdp/

"Vdoskonalennia mekhanizmu administruvannia mistsevykh podatkiv: tezy z obhovorennia" [Improvement of the Local Tax Administration Mechanism: Theses from the Discussion]. *Detsentralizatsiia*. July 17, 2023. https://decentralization.ua/en/news/16898

УДК 336.7+339.7
JEL: G15; G18; G20; K42
DOI: https://doi.org/10.32983/2222-4459-2024-2-228-236

ОСОБЛИВОСТІ ПРОТИДІЇ ВІДМИВАННЮ ГРОШЕЙ НА СУЧАСНИХ ФІНАНСОВИХ РИНКАХ

©2024 **РИСІН В. В., ФЕДОРОВИЧ Б. І.**

УДК 336.7+339.7
JEL: G15; G18; G20; K42

Рисін В. В., Федорович Б. І. Особливості протидії відмиванню грошей на сучасних фінансових ринках

Розвиток новітніх фінансових технологій спричинив значне прискорення руху грошових потоків, розширення спектра можливостей для здійснення розрахунків та використання цифрових фінансових інструментів. Одним із негативних наслідків цього процесу стала поява нових схем відмивання грошей. Метою статті є якісна оцінка змін у сфері відмивання грошей з використанням фінансових установ, викликаних розвитком новітніх фінансових технологій та віртуальних інструментів, а також визначення переліку ознак операцій з віртуальними активами, що можуть свідчити про реалізацію схем відмивання грошей. Віртуальні активи мають значний потенціал для стимулювання фінансових інновацій та ефективності на фінансових ринках, проте окремі їх характеристики створюють нові можливості для легалізації кримінальних доходів і фінансування тероризму. Зважаючи на це, важливого значення на сучасних фінансових ринках набуває вдосконалення методів протидії цьому явищу, зокрема формування переліку ознак операцій з віртуальними активами, які можуть свідчити про нелегальне походження коштів чи незаконні цілі їх руху. У роботі запропоновано орієнтовний перелік ознак відмивання грошей, який може бути застосований надавачами фінансових послуг у процесі моніторингу транзакцій. Наш підхід передбачає поділ таких ознак на шість категорій відповідно до обсягу та частоти здійснення, схеми проведення транзакцій, анонімності, характеристик бенефіціарів транзакцій, джерела походження коштів і географічного ризику. Визначено перелік ознак підозрілої активності при здійсненні транзакцій, застосування активів з високим рівнем анонімності, клієнтських ризиків, зв'язків зі злочинною діяльністю чи високоризикованими юрисдикціями. Для розуміння загальної картини та якісної оцінки ризиків відмивання грошей і фінансування тероризму визначені у статті ознаки повинні розглядатися в контексті всієї доступної інформації щодо окремих транзакцій. Урахування особливостей і вразливостей новітніх фінансових інструментів вважаємо важливою передумовою актуалізації чинних практик належної перевірки клієнтів і виявлення підозрілих фінансових операцій.

Ключові слова: *фінансові ринки, фінансові технології, віртуальні активи, відмивання грошей, ризик.*
Рис.: *1.* ***Бібл.:*** *18.*

Рисін Віталій Васильович *– доктор економічних наук, професор, професор кафедри фінансів, Національний університет «Львівська політехніка» (вул. Степана Бандери, 12, Львів, 79013, Україна)*
E-mail: *vitalii.v.rysin@lpnu.ua*
ORCID: *https://orcid.org/0000-0002-2883-4563*
Researcher ID: *https://www.webofscience.com/wos/author/record/X-7362-2018*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57222181730*
Федорович Богдан Іванович *– аспірант кафедри фінансів, Національний університет «Львівська політехніка» (вул. Степана Бандери, 12, Львів, 79013, Україна)*
E-mail: *Bohdan.i.fedorovych@lpnu.ua*
ORCID: *https://orcid.org/0009-0005-0494-2825*

UDC 336.7+339.7
JEL: G15; G18; G20; K42

Rysin V. V., Fedorovych B. I. Peculiarities of Counteracting the Money Laundering in Contemporary Financial Markets

The development of new financial technologies has led to a significant acceleration of cash flows, an expansion of the range of opportunities for settlements and the use of digital financial instruments. One of the negative consequences of this process was the emergence of new money laundering schemes. The aim of the article is to qualitatively assess the changes in the sphere of money laundering with the use of financial institutions caused by the development of new financial technologies and virtual instruments, as well as to determine the list of signs of transactions with virtual assets that may indicate the implementation of money laundering schemes. Virtual assets have significant potential to stimulate financial innovation and efficiency in financial markets, but their individual characteristics create new opportunities for money laundering and terrorism financing. In view of this, it is of great importance in modern financial markets to improve methods of counteracting this phenomenon, in particular, the formation of a list of signs of transactions with virtual assets, which may indicate the illegal origin of funds or illegal purposes of their movement. The publication proposes an approximate list of signs of money laundering, which can be used by financial service providers in the process of monitoring transactions. Our approach involves dividing such attributes into six categories according to the volume and frequency of transactions, transaction patterns, anonymity, characteristics of transaction beneficiaries, source of funds, and geographic risk. A list of signs of suspicious activity when carrying out transactions, the use of assets with a high level of anonymity, client risks, links with criminal activity or high-risk jurisdictions has been determined. In order to understand the big picture and qualitatively assess the risks of money laundering and terrorism financing, the features identified in the article should be considered in the context of all available information on individual transactions. Taking into account the features and vulnerabilities of the latest financial instruments, we consider it an important prerequisite for updating the current practices of customer due diligence and detection of suspicious financial transactions.

Keywords: *financial markets, financial technologies, virtual assets, money laundering, risk.*
Fig.: *1.* ***Bibl.:*** *18.*

Rysin Vitalii V. *– D. Sc. (Economics), Professor, Professor of the Department of Finance, National University «Lviv Polytechnic» (12 Stepana Bandery Str., Lviv, 79013, Ukraine)*
E-mail: *vitalii.v.rysin@lpnu.ua*
ORCID: *https://orcid.org/0000-0002-2883-4563*
Researcher ID: *https://www.webofscience.com/wos/author/record/X-7362-2018*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57222181730*
Fedorovych Bohdan I. *– Postgraduate Student of the Department of Finance, National University «Lviv Polytechnic» (12 Stepana Bandery Str., Lviv, 79013, Ukraine)*
E-mail: *Bohdan.i.fedorovych@lpnu.ua*
ORCID: *https://orcid.org/0009-0005-0494-2825*

Упродовж останніх десятиліть питання протидії відмиванню грошей з використанням фінансових посередників і фінансових інструментів перебувало у фокусі уваги як регуляторів, так і учасників фінансового ринку. На міжнародному ринку було розроблено низку стандартів протидії відмиванню грошей та фінансуванню тероризму, які значним чином були імплементовані в законодавство більшості цивілізованих країн світу. У практиці діяльності банків та інших фінансових установ з'явилися і використовуються дієві інструменти для належної перевірки клієнтів, виявлення підозрілих фінансових транзакцій та їх реальних бенефіціарів, упередження реалізації поширених схем легалізації кримінальних доходів тощо.

На сьогодні відмивання доходів незаконного походження розглядається не лише як кримінальний злочин, але і як перманентна загроза для фінансових ринків і корпоративного сектора. З огляду на це, побудова ефективної системи протидії відмиванню грошей та фінансуванню тероризму є одним із ключових напрямів національної безпеки країни. Складність побудови такої системи полягає в тому, що останніми роками фінансовий сектор бурхливо розвивається і диджиталізується, з'являються нові фінансові інструменти, які, відповідно, створюють нові можливості діяльності з відмивання коштів злочинного походження. Додатково слід акцентувати увагу на глобалізаційних і інтеграційних процесах, які теж мали вагомий вплив на фінансові ринки та спричинили розвиток світової фінансової інтеграції. Її наслідком стало значне прискорення руху грошових потоків, розширення спектра можливостей для здійснення розрахунків. Проте водночас зазначені процеси стимулювали появу певного «вікна можливостей» і для організованої злочинності, яка отримала додаткові інструменти для приховування джерел походження своїх доходів та інтеграції останніх в офіційну економіку.

Зважаючи на викладене, на сучасному етапі функціонування фінансових ринків гостро постало питання вдосконалення чинної практики протидії відмиванню злочинних доходів та адаптації такої практики до нових реалій світової фінансової системи – появи новітніх цифрових фінансових інструментів, децентралізованих платформ для здійснення розрахунків, зростання конкуренції між традиційними та новими учасниками фінансового ринку.

Питання легалізації кримінальних доходів активно дискутувалося у вітчизняній науці з моменту формування законодавчо-нормативної бази та створення в Україні уповноваженого органу – Держфінмоніторингу. Активну участь у дослідженні питань удосконалення боротьби з відмиванням грошей брали як представ-

ники регуляторів фінансового ринку, так і фінансисти-практики та науковці. Проте події останніх років – пандемія COVID-19, початок повномасштабної агресії та воєнний стан в Україні – суттєво змінили акценти у вивченні підвищення ефективності протидії руху кримінальних грошових потоків і використання коштів злочинного походження для фінансування терористичної діяльності.

Цю тему досить ґрунтовно досліджують як закордонні, так і вітчизняні науковці та фахівці. Так, М. Карлін та О. Івашко акцентують увагу на обмеженні використання коштів кримінального та тіньового походження під час відбудови економіки України. Остання вимагатиме залучення значних іноземних інвестицій, а отже, потребує запровадження адекватних механізмів стимулювання для інвесторів [1]. Безперечно, такі механізми передбачають прозорість джерел надходження капіталу, а також унеможливлення участі в інфраструктурних проєктах різноманітних шахрайських фінансових структур, що можуть бути задіяні в легалізаційних схемах.

Колектив авторів під керівництвом С. Дмитрова зазначає, що розвиток інформаційних технологій та фінансових інновацій робить фінансові установи, зокрема банки, ще більш привабливими об'єктами для реалізації схем відмивання грошей. Найбільш ризикованими в цьому контексті є банки, що перебувають у власності компаній-нерезидентів чи іноземних осіб [2, с. 9]. Каналами для виведення грошей через банки є офшорні зони чи країни з недосконалими процедурами контролю за бенефіціарами фінансових операцій та джерелами походження грошей.

І. Грабчук та О. Григоревська розглядають воєнний стан як фактор, що зумовлює зміни сфер відмивання грошей з огляду на те, що частину наявних схем неможливо чи складно реалізовувати, зважаючи на посилення контролю з боку держави чи інші інфраструктурні чинники. Водночас з'являються нові можливості для отримання злочинних доходів і подальшого їх відмивання, що часто пов'язані із забезпеченням військових [3].

Дослідження Г. Яровенко та М. Рожкової зосереджене на питаннях ризику конвергенції в діяльності системи протидії відмиванню грошей. Авторки зазначають, що стабільність цієї системи значним чином залежить від рівня розвитку країни та застосовуваних заходів щодо попередження загроз легалізації кримінальних доходів [4].

C. Wronka розглядає, як відмиваються незаконно отримані кошти через онлайн-платформи та компанії в різних секторах економіки в цифрову епоху, та зазначає, що виявлення прогалин у наявних механізмах боротьби з відмиванням грошей надасть фахівцям з комплаєнсу, законодавцям і правоохоронним органам розуміння специфіки сучасного кібервідмивання грошей [5].

I. Ofoeda, E. Agbloyor, J. Y. Abor дослідили вплив регулювання у сфері протидії відмиванню грошей на фінансовий розвиток та економічне зростання на прикладі 165 країн світу та дійшли висновку, що країни повинні докладати свідомих зусиль для боротьби з відмиванням грошей шляхом упровадження політики, спрямованої на підвищення фінансової прозорості та стандартів, сприяння прозорості та підзвітності державного сектора, зниження правових і політичних ризиків, а також боротьби з хабарництвом і корупцією [6].

E. A. Akartuna, S. D. Johnson, A. E. Thornton зазначають, що нові технології, зокрема криптовалюти та новітні платіжні методи, здійснили певну революцію у фінансах, проте паралельно створили нові ризики відмивання грошей і фінансування тероризму. Такі ризики мають найбільшу ймовірність матеріалізації в низці технологічних секторів – технології розподіленого реєстру, нові платіжні методи та фінтех [7].

I. Khelil зі співавторпами виявив взаємозв'язок між диджиталізацією, відмиванням грошей та етичною поведінкою компаній. Ефективна диджиталізація є важливим інструментом у боротьбі з відмиванням грошей, окрім того, є взаємозв'язок між впровадженням диджиталізації в державних установах та інституційним середовищем, оскільки низького рівня відмивання грошей неможливо досягти, якщо кроки з диджиталізації, що вживаються урядами, не підкріплені низьким рівнем корупції та етичним бізнес-середовищем [8].

D. Kumar, M. E. Lokanan дослідили, як відмивання грошей впливає на сектор фінансових установ, та яким чином підрозділи фінансової розвідки можуть мінімізувати ризики відмивання грошей. Визначальним чинником мінімізації цих ризиків, на їх думку, є дотримання фінансовими установами корпоративної культури загалом і культури комплаєнсу зокрема [9].

Фокусом дослідження H. M. Wang, M. L. Hsieh є криптовалюта як інструмент для відмивання грошей. Автори, зокрема, зазначають, що на додаток до внутрішньої та міжнародної міжвідомчої співпраці між юрисдикціями майбутні зусилля регуляторів мають бути спрямовані на такі характеристики криптовалют, як анонімність, децентралізація та блокчейн, які можуть допомогти зробити використання криптовалют менш привабливим для мотивованих злочинців на всіх етапах відмивання грошей [10].

Дослідження W. Gaviyau, A. B. Sibindi присвячене питанням застосування політики належної обачності щодо клієнтів (*CDD – customer due diligence*) в епоху розвитку фінтеху, зокрема вони акцентують увагу на тому, що технології CDD теж потребуватимуть новітніх підходів з огляду на появу нових фінансових інструментів та більш жорстких вимог регуляторів [11].

Окремі науковці зосереджують свою увагу на нетипових аспектах боротьби з відмиванням грошей, наприклад впливу заходів з протидії легалізації кримінальних доходів на фінансову інклюзію. Так, I. Ofoeda стверджує, що регулювання у сфері протидії відмиванню коштів сприяє фінансовій доступності в країнах з нижчим рівнем розвитку, проте має негативний вплив на фінансову інклюзію в розвинутих країнах [12]. Колектив авторів на чолі з L. S. Goecks зосередили увагу на методах одночасного виявлення відмивання грошей та фінансового шахрайства, зокрема на кількісних, якісних і змішаних методах [13].

Критичний аналіз перелічених вище та інших публікацій щодо сучасної специфіки протидії відмиванню грошей дозволяє визначити основні актуальні напрями вдосконалення політик учасників фінансових ринків щодо запобігання легалізації кримінальних доходів. Водночас особливі умови функціонування фінансового ринку в Україні, через негативний вплив війни та пов'язаних із нею чинників, обумовлюють необхідність більш глибокого дослідження особливостей протидії відмиванню грошей на фінансовому ринку України.

Метою статті є якісна оцінка змін у сфері відмивання грошей з використанням фінансових установ, викликаних розвитком новітніх фінансових технологій та віртуальних інструментів, а також визначення переліку ознак операцій з віртуальними активами, що можуть свідчити про реалізацію схем відмивання грошей.

Новітні фінансові технології та інструменти створюють для злочинців нові можливості для маскування джерел походження коштів. Цей процес, а саме, відмивання грошей, має низку спільних характеристик із методами, що використовуються для фінансування тероризму. В обох випадках для проведення незаконних транзакцій використовується низка методів, що експлуатують вразливості фінансового сектора та послуг, які ним надаються. Традиційні методи уникнення процедур належної перевірки включають змішування нелегальної готівки із виручкою підприємств, що працюють з готівкою, з метою її декларування як законного доходу, конвертацію доходів в іноземну валюту або виручки в іноземну валюту з подальшим виведенням коштів в офшорні юрисдикції, а також використання казино, фіктивних компаній, операцій з цінними паперами на позабіржовому ринку тощо. Перелічені методи широко використовуються і в сучасних умовах, і слід зазначати, що у практиці діяльності фінансових установ і підрозділів фінансової розвідки напрацьовано дієвий інструментарій протидії реалізації подібних схем. Але, з іншого боку, одним із побічних ефектів широкого впровадження новітніх технологій стало вдосконалення перелічених методів, завдяки чому вони стали більш оперативними, багатоходовими та складнішими для виявлення.

Новітні технології часто розглядають як інновації, які суттєво змінюють наявні ринки та операції завдяки значно кращим характеристикам. Напрямами імплементації таких технологій на сучасних фінансових ринках є цифрові валюти (чи криптовалюти), що використовують технологію розподіленого реєстру (*DLT – distributed ledger technology*), а також нові платіжні методи та технології, які використовуються в діяльності фінансових установ.

Технології розподілених реєстрів (DLT) забезпечують цифрову, децентралізовану платформу реєстрів, відкриту для певної або необмеженої кількості користувачів [14]. На відміну від звичайних реєстрів, вони не мають центрального координатора. Натомість реєстр (та його копії) ведеться та підтримується користувачами, які діють напіванонімно за допомогою механізмів консенсусу для автентифікації та додавання нових транзакцій за допомогою криптографічних методів [15]. Найяскравішим прикладом розподіленого реєстру є блокчейн, де користувачі можуть обмінюватися криптовалютами (або цифровими токенами) один з одним. Застосування DLT на сучасних фінансових ринках розширюється, оскільки ця технологія дає можливість швидко та дешевше здійснювати міжнародні та локальні платежі, уникнути високих комісійних і конвертаційних витрат, гарантувати належний рівень безпеки при здійсненні розрахунків завдяки шифруванню [16].

Водночас слід акцентувати увагу на низці ризиків, характерних для застосування DLT і блокчейну в діяльності учасників фінансових ринків. До таких ризиків можна віднести високий рівень кіберзагроз, волатильність цифрових інструментів, які побудовані на блокчейні, а також ризики регулятивного характеру, серед яких вважаємо за доцільне виділити ризик легалізації кримінальних доходів.

Нові платіжні методи можна розглядати як новітні способи здійснення традиційних фінансових операцій. До цих методів здебільшого від-

носять мобільні грошові перекази, передплачені картки, які дозволяють користувачам зберігати, переказувати та знімати кошти без необхідності встановлювати ділові відносини з фінансовою установою. Зазначені фінансові інструменти вже тривалий період часу перебувають у фокусі уваги структур, що здійснюють боротьбу з відмиванням грошей як на національному, так і на міжнародному рівнях. Особливо висока ймовірність застосування таких методів в країнах, де рівень розвитку фінансового ринку невисокий та регулювання його діяльності недосконале. Варто зауважити, що завдяки розвитку технологій платіжні методи теж швидко еволюціонують, зокрема з'являються мобільні платіжні застосунки, які забезпечують обробку платежів, що безперечно розширює спектр можливостей для злочинців, які реалізовують схеми відмивання грошей.

Фінансові послуги, що надаються традиційними фінансовими посередниками, тим часом перебувають у центрі уваги боротьби з відмиванням грошей та протидії фінансуванню тероризму. Чинні законодавчо-нормативні акти, міжнародні стандарти (зокрема, рекомендації FATF) вимагають від фінансових установ дотримуватися вимог політики «знай свого клієнта» (KYC) та належної перевірки клієнтів (CDD). Ці підходи зорієнтовані на отримання максимально достовірної інформації про клієнта та характер його діяльності, що дає змогу аналізувати його транзакції та в разі виявлення нетипових чи підозрілих фінансових операцій повідомляти про таку активність підрозділи фінансової розвідки. Однак інновації у сфері фінтеху сприяють швидкій цифровізації традиційних фінансових послуг, забезпечуючи все більш віддалений та анонімний доступ до онлайн-банкінгу, фандрайзингу та торгівлі цінними паперами. Така віддаленість клієнта від місця отримання послуг чи здійснення операцій може генерувати ризики відмивання грошей і потребує вдосконалення процедур перевірки та верифікації користувачів.

Виходячи з викладеного охарактеризуємо специфіку протидії відмиванню грошей на сучасних фінансових ринках, зважаючи на нові виклики та загрози, які виникають з огляду на стрімке впровадження нових технологій.

Віртуальні активи та пов'язані з ними послуги володіють значним потенціалом для стимулювання фінансових інновацій та ефективності на фінансових ринках, але, як зазначалося вище, окремі їх характеристики створюють нові можливості відмивання доходів, отриманих злочинним шляхом, чи фінансування незаконної діяльності. Можливість швидко здійснювати транскордонні транзакції не тільки дозволяє злочинцям купувати, переміщувати та зберігати активи в цифровому вигляді, часто поза межами регульованої фінансової системи, але й приховувати походження чи реальне призначення коштів. Це ускладнює своєчасне виявлення підозрілої діяльності фінансовими посередниками, а отже, створює додаткові перешкоди для розслідування злочинної діяльності національними уповноваженими органами.

Ще у 2018 році Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF), провідний міжнародний орган, оновила свої стандарти з метою роз'яснення їх застосування до діяльності з надання послуг з віртуальних активів і постачальників послуг з віртуальних активів. Зазначене оновлення було скероване насамперед на зменшення ризиків відмивання грошей та фінансування тероризму, пов'язаних з діяльністю у сфері віртуальної валюти та провайдерів послуг з віртуальними активами, а також на захист цілісності світової фінансової системи [17].

За оцінками FATF, найпоширенішими злочинами, пов'язаними з відмиванням грошей, є нелегальний продаж зброї, шахрайство, ухилення від сплати податків, комп'ютерні злочини (наприклад, кібератаки, що призводять до крадіжок), експлуатація дітей, торгівля людьми, уникнення санкцій, фінансування тероризму [18]. З-поміж цього переліку найпоширенішим видом зловживань є незаконний обіг підконтрольних речей (зокрема, зброї) або з продажем безпосередньо у віртуальних валютах, або з використанням віртуальних валют у процесі розшарування у схемах відмивання грошей. Друга найпоширеніша категорія пов'язана з шахрайством, аферами, програмами-вимагачами та здирництвом. Упродовж останніх років професійні мережі відмивачів грошей почали використовувати віртуальні валюти як один із способів переказу, збору або розшарування злочинних доходів.

З огляду на те, що використання віртуальних активів має всі перспективи до розширення, важливого значення набуває вдосконалення методів виявлення спроб використання таких активів для цілей відмивання грошей. Вагому роль при цьому відіграє моніторинг фінансових транзакцій та виявлення таких їх ознак, які можуть свідчити про нелегальне походження коштів чи незаконні цілі їх руху. Перелік таких ознак наведено на *рис. 1*.

Віртуальні (цифрові) активи на сьогодні ще не належать до числа основних інструментів фінансових ринків, проте їх застосування набуло популярності серед злочинців. Використання криптовалют для цілей відмивання грошей розпочалося ще у 2010-х роках, нині вони стають усе більш поши-

Рис. 1. Ознаки підозрілих операцій з віртуальними активами

Джерело: авторська розробка.

ним інструментом злочинної діяльності. Зважаючи на це, для фінансових установ, що здійснюють операції з такими активами, важливо сформувати чіткий перелік індикаторів для виявлення потенційної незаконної діяльності.

У процесі аналізу транзакцій з віртуальними активами слід звертати увагу на спроби структурування операцій, тобто подрібнення однієї великої операції на низку дрібніших для уникнення процедур обов'язкової перевірки. Як підозрілу активність слід розглядати здійснення кількох транзакцій на великі суми упродовж короткого періоду часу, особливо за новими чи раніше неактивними рахунками (такі операції характерні у випадку із програмами-вимагачами). Водночас ознаками відмивання грошей можуть бути:

- переказ віртуальних активів одразу декільком закордонним провайдерам послуг, що працюють у слабо регульованих юрисдикціях;
- розміщення криптовалют на біржі з подальшим зняттям без проведення будь-яких операцій, або конвертація в інші активи без очевидного економічного змісту, чи виведення одразу на приватний гаманець;
- внесення віртуальних активів з адрес, що раніше були ідентифіковані як шахрайські чи пов'язані із викраденими активами.

Важливе значення має оцінка схеми проведення транзакцій із віртуальними активами. У цьому контексті підвищену увагу слід приділяти транзакціям нових клієнтів – внесенню значних за обсягом депозитів, що не відповідають профілю клієнта; використання всієї суми депозиту для торгівлі одразу після його розміщення; переведення всієї внесеної суми на інші платформи, особливо позабіржові. Щодо інших категорій клієнтів, посиленого моніторингу вимагають транзакції з кількома віртуальними активами чи рахунками (без логічного обґрунтування), регулярні перекази на один і той самий рахунок кількома особами; вхідні невеликі за обсягом транзакції з непов'язаних гаманців з подальшим переказом на інший гаманець чи обміном на фіатну валюту; обмін віртуальних активів на фіатну валюту із потенційними збитками; конвертація значної суми фіатної валюти у віртуальні активи, чи навпаки, без очевидного економічного змісту.

Анонімність віртуальних активів традиційно розглядається як вразливість у контексті протидії відмиванню грошей. Їх окремі технологічні характеристики створюють перешкоди для виявлення злочинної діяльності, а отже, роблять віртуальні валюти привабливими для злочинців, які прагнуть приховати або зберегти свої кошти. Водночас слід наголоси-

ти, що сама лише ознака анонімності автоматично не свідчить про незаконну транзакцію, а може бути одним із інструментів захисту віртуальних валют від викрадення. Тому аналізувати цю ознаку потрібно лише в контексті інших характеристик клієнта та історії відносин із ним. До переліку характеристик анонімності, що потребують поглибленого аналізу, вважаємо за доцільне віднести такі:

- використання віртуальних активів з підвищеним рівнем анонімності (наприклад, *AEC – anonymity-enhanced cryptocurrency*);
- обмін активів, що працюють на прозорому блокчейні, на AEC, чи приватні монети;
- здійснення операцій через P2P платформи;
- транзакції з використанням сервісів змішування;
- перекази з гаманців, що пов'язані з даркнет-ринками, сервісами змішування / перемішування, сайтами з азартними іграми, іншою незаконною діяльністю;
- транзакції користувачів, що використовують IP-адреси, які дозволяють анонімне спілкування;
- використання віртуальних активів, що можуть бути частиною шахрайських схем;
- операції через криптомати чи криптокіоски.

Нетипова поведінка бенефіціарів транзакцій з віртуальними активами також може бути підставою для виникнення підозри щодо законності таких транзакцій. Тут маються на увазі різноманітні порушення в процесі створення облікових записів користувачів (окремі рахунки під різними іменами, ненадійні IP-адреси, реєстрація інтернет-доменів у юрисдикціях з неналежним рівнем контролю тощо). Окрім того, процедура перевірки клієнта теж може виявити низку ризикованих характеристик, зокрема ненадання клієнтом інформації про джерела походження коштів, недостовірна інформація про взаємовідносини з контрагентом, підробка документів, що посвідчують особу, розбіжності між використовуваними IP-адресами. Важливими напрямом реалізації процедур перевірки клієнта є виявлення підставних осіб, які свідомо чи несвідомо діють в інтересах професійних відмивачів грошей. Ознаками підставних осіб можуть бути вік клієнта (якщо він суттєво перевищує середній вік користувачів певної платформи), належність до вразливих чи малозабезпечених верств суспільства, невідповідність обсягу здійснюваних операцій фінансовому профілю клієнта.

Щодо інших ознак нетипової поведінки клієнта, яка може свідчити про його долученість до реалізації схем відмивання грошей, то варто виділити часту зміну ідентифікаційних даних, укладення угод з віртуальними активами з різних IP-адрес упродовж короткого періоду часу, проведення періодичних транзакцій з певною групою контрагентів, що приносять значний прибуток або збиток.

Світова практика протидії відмиванню грошей свідчить, що доволі часто віртуальні активи можуть використовуватися для легалізації доходів злочинних угрупувань, що займаються наркобізнесом, шахрайством, крадіжками та вимаганням з використанням кібертехнологій. Зважаючи на це, важливе значення має оцінка джерел походження коштів чи багатства. Ознаками нелегітимного їх походження можуть бути:

- операції з банківськими платіжними картками, що пов'язані із випадками шахрайства, вимагання, даркнет-ринками тощо;
- операції з коштами від азартних ігор в мережі «Інтернет»;
- зняття великих сум готівки чи внесення готівки для купівлі віртуальних активів;
- використання підставних компаній, ICO, де персональні дані інвесторів можуть бути можуть бути недоступними;
- джерело багатства клієнта пов'язане з інвестиціями у віртуальні активи, ICO (особливо шахрайські проєкти), а також доходи, отримані від провайдерів послуг, шо не підлягають належному контролю у сфері протидії відмиванню грошей та фінансуванню тероризму.

Специфіка прояву географічного ризику на сучасних фінансових ринках полягає в наявності прогалин у регулюванні новітніх фінансових інструментів, зокрема віртуальних активів. Використовуючи такі обставини, структури, що займаються відмиванням грошей, частину своїх операцій намагаються здійснювати через установи чи біржі, які зареєстровані або працюють у юрисдикціях з відсутнім або мінімальним регулюванням у сфері протидії відмиванню коштів та фінансуванню тероризму. З огляду на це, особливої уваги потребують ризики, пов'язані з юрисдикціями походження, призначення та транзиту транзакції. Про наявність таких ризиків може свідчити використання для проведення операцій бірж чи посередників, що розташовані у високоризикованих юрисдикціях, або здійснення клієнтом діяльності в таких юрисдикціях.

ВИСНОВКИ

Охарактеризований вище перелік ознак, безумовно, не є вичерпним, зважаючи на бурхливий розвиток сучасних фінансових ринків та інструментів, які ними використовуються. Ми зосередили наше дослідження більшою мірою на ознаках

операцій з віртуальними активами, цифровими валютами та новітніми платіжними інструментами. Запропоновані у статті ознаки підозрілих фінансових операцій не повинні розглядатися ізольовано – для розуміння загальної картини та якісної оцінки ризиків відмивання грошей і фінансування тероризму слід оцінювати такі ознаки в контексті всієї інформації щодо тих чи інших транзакцій. Ця інформація може бути отримана від підрозділів фінансової розвідки, правоохоронних органів чи з відкритих джерел.

Підсумовуючи, зазначимо, що питання протидії відмиванню грошей та фінансуванню тероризму на сучасних фінансових ринках стає дедалі більш багатогранним і складним. Зважаючи на розвиток фінансових технологій, появу нових платіжних інструментів, розширення сфери використання віртуальних активів, чинні процедури перевірки клієнтів і моніторингу транзакцій, що використовуються традиційними фінансовими посередниками, вимагають постійної актуалізації та вдосконалення. Водночас розширення кола учасників фінансових ринків за рахунок нових провайдерів послуг у сфері віртуальних активів чи платіжних послуг ставить завдання поширення усталеної практики протидії відмиванню грошей у їхній діяльності. Для цієї категорії посередників важливо встановити дієві бар'єри на шляху руху коштів нелегітимного походження в офіційну економіку. ■

БІБЛІОГРАФІЯ

1. Карлін М., Івашко О. Вплив «брудних» грошей на діяльність суб'єктів поведінкових фінансів на ринку фінансових послуг України. *Економіка та суспільство*. 2022. Вип. 41. DOI: https://doi.org/10.32782/2524-0072/2022-41-42
2. Економіко-математичний інструментарій національної оцінки ризиків легалізації коштів (фінансування тероризму) / за ред.. С. О. Дмитрова. Суми : Ярославна, 2017. 216 с.
3. Грабчук І. Л., Григоревська О. О. Економічні наслідки відмивання грошей в умовах воєнного стану. *Бізнес Інформ*. 2022. № 9. С. 102–107. DOI: https://doi.org/10.32983/2222-4459-2022-9-102-107
4. Яровенко Г. М., Рожкова М. С. Оцінювання ризику конвергенції систем протидії відмивання грошей та кібербезпеки. *Економіка та суспільство*. 2022. Вип. 45. DOI: https://doi.org/10.32782/2524-0072/2022-45-84
5. Wronka C. «Cyber-laundering»: the change of monєy laundering in the digital age». *Journal of Money Laundering Control*. 2022. Vol. 25. No. 2. P. 330–344. DOI: https://doi.org/10.1108/JMLC-04-2021-0035
6. Ofoeda I., Agbloyor E., Abor J. Y. Financial sector development, anti-money laundering regulations and economic growth. *International Journal of Emerging Markets*. 2024. Vol. 19. No. 1. P. 191–210. DOI: https://doi.org/10.1108/IJOEM-12-2021-1823
7. Akartuna E. A., Johnson S. D., Thornton A. E. The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*. 2023. Vol. 36. P. 615–650. DOI: https://doi.org/10.1057/s41284-022-00356-z
8. Khelil I., El Ammari A., Bouraoui M. A., Khlif H. Digitalization and money laundering: the moderating effects of ethical behaviour of firms and corruption. *Journal of Money Laundering Control*. 2023. Vol. 26. No. 6. P. 1203–1220. DOI: https://doi.org/10.1108/JMLC-01-2023-0015
9. Kumar D., Lokanan M. E. Money laundering influence on financial institutions and ways to retaliate. *Journal of Money Laundering Control*. 2023. Vol. 26. No. 1. P. 133–147. DOI: https://doi.org/10.1108/JMLC-11-2021-0123
10. Wang H. M., Hsieh M. L. Cryptocurrency is new vogue: a reflection on money laundering prevention. *Security Journal*. 2024. Vol. 37. P. 25–46. DOI: https://doi.org/10.1057/s41284-023-00366-5
11. Gaviyau W., Sibindi A. B. Customer Due Diligence in the FinTech Era: A Bibliometric Analysis. *Risks*. 2023. Vol. 11. Iss. 1. Art. 11. DOI: https://doi.org/10.3390/risks11010011
12. Ofoeda I.Anti-money laundering regulations and financial inclusion: empirical evidence across the globe. *Journal of Financial Regulation and Compliance*. 2022. Vol. 30. No. 5. P. 646–664. DOI: https://doi.org/10.1108/JFRC-12-2021-0106
13. Goecks L. S., Korzenowski A. L., Gonçalves Terra Neto P., de Souza D. L., Mareth T. Anti-money laundering and financial fraud detection: A systematic literature review. Intelligent Systems in Accounting, *Finance and Management*. 2022. Vol. 29. Iss. 2. P. 71–85. DOI: https://doi.org/10.1002/isaf.1509
14. Christie L. Distributed Ledger Technology. POSTbrief 28. London : Parliamentary Office of Science and Technology (POST), *Houses of Parliament*, 2018. URL: https://researchbriefings.files.parliament.uk/documents/POST-PB-0028/POST-PB-0028.pdf
15. Choo K.-K. R. Chapter 15 – Cryptocurrency and Virtual Currency: Corruption and Money Laundering/ Terrorism Financing Risks? In: *Handbook of Digital Currency*, edited by David Lee Kuo Chuen. San Diego : Academic Press, 2015. P. 283–307. DOI: https://doi.org/10.1016/B978-0-12-802117-0.00015-1
16. Рисін В. В., Мамчук А. Р., Печенко Р. О. Впровадження технології блокчейну у контексті підвищення ефективності та безпеки діяльності банків. *Трансформаційна економіка*. 2023. № 5. С. 109–114. DOI: https://doi.org/10.32782/2786-8141/2023-5-19

17. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. *FATF Report*. September 2020. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf
18. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. *FATF*, Paris, France. 2023. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

REFERENCES

Akartuna, E. A., Johnson, S. D., and Thornton, A. E. "The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review". *Security Journal*, vol. 36 (2023): 615-650.
DOI: https://doi.org/10.1057/s41284-022-00356-z

Choo, K.-K. R. "Chapter 15 – Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?" In *Handbook of Digital Currency*, 283-307. San Diego: Academic Press, 2015.
DOI: https://doi.org/10.1016/B978-0-12-802117-0.00015-1

Christie, L. "Distributed Ledger Technology. POSTbrief 28". London : Parliamentary Office of Science and Technology (POST), *Houses of Parliament*, 2018. https://researchbriefings.files.parliament.uk/documents/POST-PB-0028/POST-PB-0028.pdf

Ekonomiko-matematychnyi instrumentarii natsionalnoi otsinky ryzykiv lehalizatsii koshtiv (finansuvannia teroryzmu) [Economic-mathematical Toolkit for National Risk Assessment of Money Laundering (Terrorist Financing)]. Sumy: Yaroslavna, 2017.

Gaviyau, W., and Sibindi, A. B. "Customer Due Diligence in the FinTech Era: A Bibliometric Analysis". *Risks*, art. 11, vol. 11, no. 1 (2023).
DOI: https://doi.org/10.3390/risks11010011

Goecks, L. S. et al. "Anti-money laundering and financial fraud detection: A systematic literature review". *Intelligent Systems in Accounting, Finance and Management*, vol. 29, no. 2 (2022): 71-85.
DOI: https://doi.org/10.1002/isaf.1509

Hrabchuk, I. L., and Hryhorevska, O. O. "Ekonomichni naslidky vidmyvannia hroshei v umovakh voiennoho stanu" [The Economic Consequences of Money Laundering under Martial Law]. *Biznes Inform*, no. 9 (2022): 102-107.
DOI: https://doi.org/10.32983/2222-4459-2022-9-102-107

"International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation". *FATF*, Paris, France. 2023. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Karlin, M., and Ivashko, O. "Vplyv «brudnykh» hroshei na diialnist subiektiv povedinkovykh finansiv na rynku finansovykh posluh Ukrainy" [The Influence of "Dirty" Money on the Activities of Behavioral Finance Subjects on the Financial Services Market in Ukraine]. *Ekonomika ta suspilstvo,* no. 41 (2022).
DOI: https://doi.org/10.32782/2524-0072/2022-41-42

Khelil, I. et al. "Digitalization and money laundering: the moderating effects of ethical behaviour of firms and corruption". *Journal of Money Laundering Control*, vol. 26, no. 6 (2023): 1203-1220.
DOI: https://doi.org/10.1108/JMLC-01-2023-0015

Kumar, D., and Lokanan, M. E. "Money laundering influence on financial institutions and ways to retaliate". *Journal of Money Laundering Control*, vol. 26, no. 1 (2023): 133-147.
DOI: https://doi.org/10.1108/JMLC-11-2021-0123

Ofoeda, I. "Anti-money laundering regulations and financial inclusion: empirical evidence across the globe". *Journal of Financial Regulation and Compliance*, vol. 30, no. 5 (2022): 646-664.
DOI: https://doi.org/10.1108/JFRC-12-2021-0106

Ofoeda, I., Agbloyor, E., and Abor, J. Y. "Financial sector development, anti-money laundering regulations and economic growth". *International Journal of Emerging Markets*, vol. 19, no. 1 (2024): 191-210.
DOI: https://doi.org/10.1108/IJOEM-12-2021-1823

Rysin, V. V., Mamchuk, A. R., and Pechenko, R. O. "Vprovadzhennia tekhnolohii blokcheinu u kontekсti pidvyshchennia efektyvnosti ta bezpeky diialnosti bankiv" [Implementation of Blockchain Technology in the Context of Improving the Efficiency and Security of Banks]. *Transformatsiina ekonomika*, no. 5 (2023): 109-114.
DOI: https://doi.org/10.32782/2786-8141/2023-5-19

"Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. *FATF Report*. September 2020". https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

Wang, H. M., and Hsieh, M. L. "Cryptocurrency is new vogue: a reflection on money laundering prevention". *Security Journal*, vol. 37 (2024): 25-46.
DOI: https://doi.org/10.1057/s41284-023-00366-5

Wronka, C. "«Cyber-laundering»: the change of money laundering in the digital age». *Journal of Money Laundering Control*, vol. 25, no. 2 (2022): 330-344.
DOI: https://doi.org/10.1108/JMLC-04-2021-0035

Yarovenko, H. M., and Rozhkova, M. S. "Otsiniuvannia ryzyku konverhentsii system protydii vidmyvannia hroshei ta kiberbezpeky" [Risk Assessment of the Anti-Money Laundering and Cyber Security Systems' Convergence]. *Ekonomika ta suspilstvo*, no. 45 (2022).
DOI: https://doi.org/10.32782/2524-0072/2022-45-84