DOI: https://doi.org/10.30970/fp.1(55).2025.667677

УДК 336.76:004.738.5:343.3

РИЗИКИ ВІДМИВАННЯ ГРОШЕЙ У СФЕРІ ФІНТЕХ: ВИКЛИКИ ДЛЯ ФІНАНСОВОГО МОНІТОРИНГУ

РИСІН Віталій Васильович
доктор економічних наук, професор,
професор кафедри фінансів
Національного університету «Львівська політехніка»
ORCID ID: https://orcid.org/0000-0002-2883-4563

МАЛЮСЬКА Марія Олександрівна
здобувачка вищої освіти Національного університету «Львівська політехніка»
ORCID ID: https://orcid.org/0009-0007-3361-2221

Анотація. *Розвиток технологій у сфері фінансів супроводжується, з одного боку, трансформацією фінансових послуг та покращенням клієнтського досвіду, а з іншого – створенням нових і непередбачуваних ризиків для регуляторів у сфері відмивання коштів. Метою статті є характеристика ризиків відмивання грошей, що виникають з огляду на стрімкий розвиток сфери фінтех та обґрунтування механізмів мінімізації таких ризиків. У роботі визначено та прокласифіковано сучасні виклики для фінансового моніторингу в умовах міжнародного співробітництва. Зокрема, визначено чотири категорії викликів, а саме етичні, регуляторні, технологічні та організаційні. Значну увагу було приділено аналізу використання віртуальних активів як інструменту легалізації кримінальних доходів. Авторами досліджено особливості застосування новітніх технологій, зокрема SupTech та RegTech, для боротьби з відмиванням грошей, та визначено перспективні напрямки розвитку цих технологій.*

Ключові слова: *фінтех, відмивання грошей, фінансовий моніторинг, віртуальні активи, протидія відмиванню грошей.*

Постановка проблеми. Стрімкий розвиток фінансових технологій змінює традиційну фінансову систему, створюючи нові можливості не тільки для сумлінних учасників ринку, а й для суб'єктів, залучених до протиправної діяльності. У зв'язку з цим, сфера відмивання грошей набуває нових форм та з кожним роком охоплює значно більшу кількість інструментів. Таке явище несе загрози для міжнародної безпеки, що створює нагальну необхідність дослідження ризиків та викликів, пов'язаних із використанням новітніх фінтех продуктів для цілей відмивання грошей і фінансування тероризму. Актуальним також є питання створення та запровадження уніфікованого законодавства для спільного розуміння міжнародною спільнотою середовища розвитку протиправних діянь. Відмивання грошей, безперечно, несе значні ризики для функціонування фінансових ринків. Уряди країн та підрозділи фінансової розвідки часто не встигають адекватно протидіяти новим інструментам та методам, які використовують професійні посередники відмивання коштів. Тому аналіз наявних механізмів регулювання та протидії, а також їх трансформація з

огляду на виклики сьогодення є актуальними напрямами для наукових досліджень.

Аналіз останніх досліджень та публікацій. Оцінка змісту актуальних наукових праць за темою дослідження дозволяє виділити ризики та виклики пов'язані з сектором фінтех та його стрімким розвитком. Значну увагу у літературі приділяють впливу віртуальних активів на трансформацію методів відмивання коштів. Наприклад, Крістіан Лойпрехт (Christian Leuprecht) стверджує, що біткоїн та інші альтернативні валюти широко поширені на перших двох етапах відмивання коштів, при цьому поєднуються з сторонніми біржами, які є дієвими для приховування походження коштів [1]. Водночас Деніел Дюпюї (Daniel Dupuis) та Кімберлі Глісон (Kimberly Gleason) описують шість доступних механізмів обміну активів для відмивання грошей, підкреслюючи еволюцію цих способів [2]. Рой Маджед Сінно (Roy Majed Sinno) та ін. демонструють стрімку зміну фінансових схем – від відмивання коштів через торгівлю (TBML) до відмивання коштів через послуги (SBML), наголошуючи на сфері фінтех як сприятливому середовищу для цих цілей [3].

Важливим аспектом у протидії відмиванню коштів є регулювання децентралізованих фінансів. Дослідження Владлени Бенсон (Vladlena Benson) та ін. підкреслюють необхідність надійної регуляторної стратегії для усунення «сліпих зон» у DeFi, якими користуються злочинці [4].

Можливим напрямком фінансового моніторингу Маркус Сміт (Marcus Smith) та Мілінд Тіварі (Milind Tiwari) визначають впровадження блокчейн-інфраструктури для зменшення ризиків відмивання коштів [5]. І нарешті, Георгіос Павлідіс (Georgios Pavlidis) аналізує використання штучного інтелекту міжнародними організаціями у протидії фінансуванню тероризму, проте зазначає важливість балансу у прагненні посилити ефективність моніторингу і збереженню прав користувачів [6]. Виходячи з викладеного, зазначимо, що за умов бурхливого розвитку фінансового ринку, залишається актуальним дослідження наявних викликів для системи фінансового моніторингу, а також визначення ефективних механізмів регулювання операцій і діяльності учасників ринку.

Метою статті є характеристика ризиків відмивання грошей, що виникають з огляду на стрімкий розвиток сфери фінтех, та обґрунтування механізмів мінімізації таких ризиків. У процесі підготовки статті здійснено аналітичний огляд літературних джерел, звітів міжнародних організації, рекомендацій регуляторних органів та законодавства окремих країн з питань протидії відмиванню грошей та фінансування тероризму. Проведено порівняння динаміки появи фінтех-стартапів у різних регіонах, а також систематизовано виклики, що виникають перед органами, відповідальними за здійснення фінансового моніторингу.

Виклад основних результатів. Фінтех (Financial technology) не має єдиного визначення, узгодженого на міжнародному рівні. У широкому контексті цей термін використовується для опису програм та інновацій, що слугують для забезпечення доступу до банківських і фінансових послуг. Проте, у багатьох розглянутих дослідженнях і звітах зазвичай користуються більш конкретним визначенням. Наприклад, у звіті підготовленому Information Exchange Working Group (IEWG), фінтех стосується організацій, які здійснюють платежі або перекази коштів за допомогою нових технологій [7]. Члени групи Егмонт включають у це визначення компанії, що здійснюють таку діяльність: інтернет-банкінг, мобільний банкінг, цифрові або електронні гроші, платформи грошових переказів, краудфандингові платформи та постачальники послуг віртуальних активів.

Хоча фінтех організації перебувають у конкуренції з традиційними фінансовими установами, вони також взаємодіють з наявними суб'єктами традиційної фінансової інфраструктури. До прикладу, європейська модель кооперації полягає у наданні банком-партнером ліцензійної інфраструктури, а фінтех-стартап забезпечує технологію або клієнтський сервіс. У 2015 році ЄС запровадив директиву PSD2, яка відкрила банківські системи для відкритого банкінгу – сторонніх фінтех-сервісів [8]. Це дало поштовх для появи численних агрегаторів рахунків, платіжних застосунків та альтернативних фінансових платформ, що, у свою чергу, сприяло стрімкому зростанню сектору. Фінтех упродовж останніх років еволюціонував від «занадто малого, щоб звертати увагу» — до «занадто великого, щоб ігнорувати» — і зрештою «надто значущого, щоб дозволити йому зазнати краху [9]. Зазначене підтверджується даними про кількість стартапів у сфері фінансових технологій за регіонами світу (табл. 1 та рис. 1).

Таблиця 1.

Кількість стартапів у сфері фінансових технологій за регіонами світу у 2018-2024 рр.

Рік	Америка	Європа, Близький Схід та Африка	Азіатсько-Тихоокеанський регіон	Сума
2018	5 686	3 581	2 864	12 131
2019	5 779	3 583	2 849	12 211
2020	8 775	7 385	4 765	20 925
2021	10 755	9 323	6 268	26 346
2023	11 651	9 681	5 061	26 393
2024	13 100	10 969	5 886	29 955

Джерело: складено авторами за даними [10]

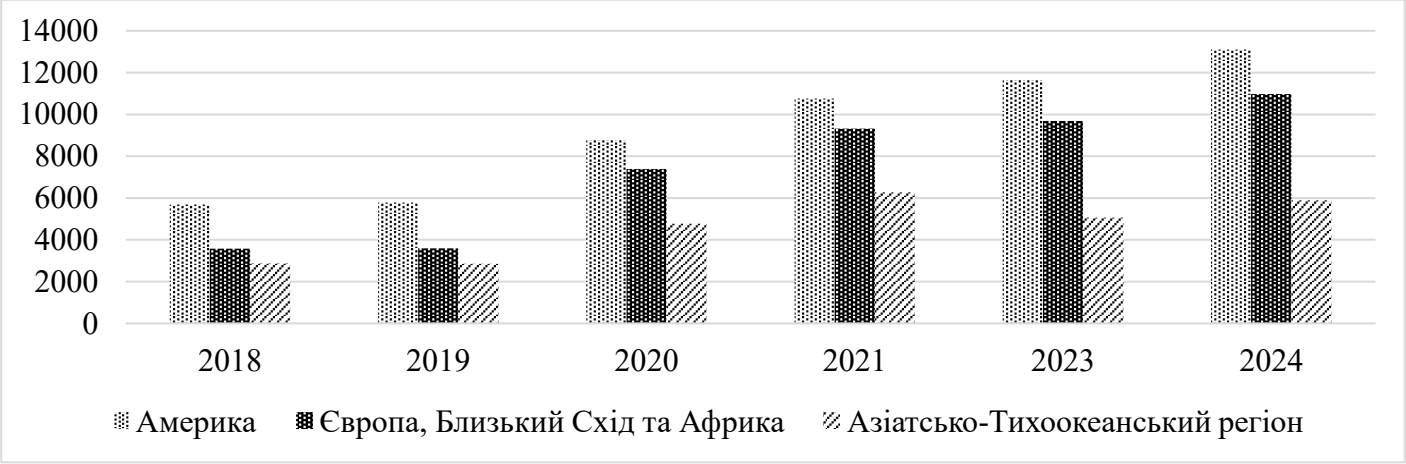

Рис. 1. Динаміка кількості стартапів фінтех за 2018-2024 рр.
Джерело: складено авторами за даними [10]

З кожним роком простежується зростання кількості проєктів, особливо на американських континентах та в регіоні, що охоплює Європу, Близький Схід і Африку. Загальна кількість компаній зросла на 17 852 одиниць, що свідчить про зростання майже у 2,5 рази за період 2018-2024 років. Зважаючи на стрімке збільшення кількості фінансово-технологічних компаній і розвитку економіки

загалом, удосконалюються також методи відмивання коштів. Створення передумов для цифровізації у секторі фінансів сприяють утворенню більшої кількості шахрайських схем з більш продуманими алгоритмами приховування діяльності. Така тенденція підкреслює критичну необхідність у реакції регуляторів на цю галузь.

Відмивання грошей у більшості літературних джерел визначається як процес переміщення, перетворення або використання активів, отриманих унаслідок злочинної діяльності, з метою приховування їхнього незаконного походження. Відмивання грошей існує на багатьох рівнях і може здійснюватись в різних обсягах. Це явище може бути спровокованим необхідністю легалізувати кошти, які хоч і були отримані чесною працею, але з яких не було сплачено податки. Така ситуація існує на побутовому рівні у країнах з низьким доходом населення і високим податковим навантаженням. Роботодавці намагаються не втратити конкурентоспроможність в оплаті праці за рахунок недоплачених прямих податків з доходів робітників. Хоча відповідальність за це несе той же роботодавець – у фізичної особи, яка не проконтролювала сплату податків за себе, виникає необхідність заводити готівку з конвертів у фінансову систему для подальшого легального використання. Для невеликих сум, як наприклад заробітна плата, часто використовуються схеми дроблення і заведення коштів на рахунки у різних банках. Якщо суми перевищуватимуть порогові значення, можуть використовуватись VASP (постачальники послуг віртуальних активів). MONEYVAL визначає VASP як будь-яку фізичну або юридичну особу, яка в якості ділової діяльності здійснює одну або декілька з наведених нижче видів діяльності або операцій для іншої фізичної або юридичної особи, або від її імені:

- обмін між віртуальними активами та фіатними валютами;
- обмін між однією або кількома формами віртуальних активів;
- переказ віртуальних активів;
- зберігання та/або управління віртуальними активами або інструментами, що дозволяють контролювати віртуальні активи; та
- участь та надання фінансових послуг, пов’язаних із пропозицією емітента та/або продажем віртуального активу [11].

У міжнародний літературі термін VASP не стосується конкретної технології, він може охоплювати криптовалютні підприємства, маркетплейси NFT, суб’єктів, що надають послуги ATM, кастодіальних гаманців та децентралізовані біржі. Таке різноманіття технологічних рішень дозволяє обрати найдешевший і найзручніший спосіб для приховування незаконного походження доходів або справжнього власника активів. Наприклад, нелегальні кошти можуть швидко та анонімно конвертуватися у віртуальні активи (BTC, XMR, USDT) через низку популярних VASP-платформ. Після цього здійснюється міксинг або chain-hopping — багаторазове обмінювання криптовалют для розмивання сліду транзакцій. Такі дії ускладнюють відстеження і віддаляють цифровий слід від початкового етапу, де фіатні кошти вперше були перетворені у віртальні активи. Завдяки таким технологіям, фінальна інтеграція активів у традиційну фінансову систему стає менш ризикованою.

Фактор незаконності отримання доходів у результаті протиправної діяльності, а також бажання використати кошти на фінансування тероризму або іншу протиправну діяльність створює необхідність для більш продуманих схем, аніж описано вище. Зокрема, до процесу легалізації коштів можуть залучатись професійні учасники, що володіють широким інструментарієм технологічних рішень для досягнення цілей легалізації коштів. Ними можуть бути окремі особи (individual PML), організації

(Professional money laundering organisation (PMLO)) та цілі мережі (Professional money laundering network (PMLN)) співучасників такого процесу [12]. Такі мережі задля задоволення потреб клієнтів відкривають рахунки в іноземних банках, засновують або купують іноземні компанії та використовують існуючу інфраструктуру, яка контролюється іншими структурами. Крім того, співпраця між різними професійними учасниками також урізноманітнює канали, через які можуть проходити незаконні доходи, тим самим зменшуючи ризик виявлення та конфіскації. PML пропонують різноманітні послуги, включаючи використання віртуальних валют в спробі анонімізувати тих, хто вчиняє злочини і їхні незаконні операції. Слід також зазначити, що PMLO працюють транскордонно. Вони висококваліфіковані та діють у різноманітних умовах, уміло уникаючи уваги правоохоронних органів. Співучасники постачальників віртуальної валюти також використовують підставні компанії та афілійовані організації, які обслуговують онлайнову базу клієнтів у всьому світі для електронного переказу фіатної валюти.

З огляду на наявні ризики, способи відмивання коштів і різноманітність технологічних рішень, ефективне функціонування системи фінансового моніторингу у сфері Фінтех є критично важливим для створення безпечних умов взаємодії у фінансових секторах. Для досягнення цієї мети в межах окремої держави, урядам необхідно постійно вдосконалювати наявні механізми фінансового моніторингу. В українському законодавстві фінансовий моніторинг визначається як сукупність заходів, що вживаються суб'єктами фінансового моніторингу у сфері запобігання та протидії, що включають проведення державного фінансового моніторингу та первинного фінансового моніторингу [13]. Національний Банк України оперує дещо іншим визначенням фінансового моніторингу: «…це діяльність із виявлення незаконно отриманих доходів та запобігання фінансуванню тероризму» [14].

Проте, слід зауважити, що у міжнародному праві немає визначення фінансовому моніторингу. Так само як і відсутнє чітке розуміння фінтеху, суб'єктів та об'єктів цього сектору. Як зазначає MONEYVAL, не всі країни члени внесли VASP до національних законів про ПВК/ФТ як підзвітні суб'єкти. Це створює можливості для існування структур, що використовують регуляторний арбітраж. Фінтех компанії можуть спеціально реєструватися там, де етичні і соціальні стандарти контролю слабші, що підриває глобальну систему протидії відмиванню грошей. Детальніше це можна пояснити таким чином: європейський регулятор вимагає застосування процедур «знай свого клієнта (KYC), а компанія просто відкриває «хаб» у країні без KYC. Це призводить до такого явища як «race to the bottom» — коли юрисдикції змагаються, хто слабше здійснює регулювання, щоб привабити клієнтів. З практичної точки зору це проявляється у неможливості наглядовими органами здійснювати моніторинг операцій організацій. Отож, можна стверджувати, що базовим викликом є відсутність відповідного правового поля або міжнародного законодавства для здійснення фінансового моніторингу. Причиною попереднього можна вважати різний рівень розвитку країн. Як зазначає Комітет експертів з оцінки заходів протидії відмиванню коштів, юрисдикції які мають невеликий фінтех сектор, як правило, схильні до більш академічної оцінки ризиків, які значною мірою покладаються на публікації міжнародних організацій [11]. Не всі наглядові органи мають вичерпні ресурси з точки зору персоналу та знань, і наявний ризик орієнтований підхід часто не пристосований до оцінки специфічних ризиків ринку. Існуючі методи моніторингу фінтех скоріше нагадують адаптацію старої структури регулювання традиційної системи до нового явища.

Важливою проблемою також є діяльність регулюючих органів у середовищі обмеженої інформації. На національному рівні аналіз секторальних ризиків значною мірою покладається на відповіді, які органи влади отримують від самого приватного сектору, при цьому дії для перевірки фактів з боку наглядового органу практично не вживаються. Також існує часовий лаг при настанні випадку з підозрілою трансакцією, повідомленням фінтех компанією до регуляторних органів і розглядом останніх цього звернення.

Наступним викликом для фінмоніторингу є постійна поява нових технологічних рішень і швидкість їхнього впровадження приватним сектором. Уряди зазвичай не мають достатньо розвинених технологій для моніторингу діяльності фінтех-компаній у реальному часі, автоматизованого аналізу і швидких алгоритмів відповіді на них. Масштаб і транскордонність операцій також постають викликом для наявних процедур моніторингу. Через обмеження, пов’язані зі збором і аналізом даних, що наведені вище, складається враження, що більшість держав мають обмежене уявлення про фінтех-компанії і їхні продукти, які діють на території цих країн. Це стосується як іноземних компаній, які надають послуги національним клієнтам, так і національних незареєстрованих чи неліцензованих підприємств.

Також варто врахувати наявність вигод для деяких учасників міжнародної фінансової системи від недосконалості регуляторних правил. Етика і соціальні чинники не є в пріоритеті перед економічними перевагами, коли йдеться про мільярдні фінансові потоки. За оцінками Nasdaq Verafin, через фінансову систему в усьому світі пройшло 3,1 трильйона доларів незаконних коштів у 2023 році [15]. Компанії впроваджують «мінімально достатні» заходи, формально виконуючи вимоги, але фактично залишають простір для зловживань. Не можна оминути увагою наявність професійних учасників відмивання коштів, які, хоч і свідомі незаконності своєї діяльності, проте за комісійну винагороду допомагають легалізувати доходи отримані незаконним шляхом. З огляду на зазначене вище, для системи фінансового моніторингу можна визначити чотири категорії викликів (рис. 2).

Рис. 2. Категорії викликів для системи фінансового моніторингу
Джерело: власна розробка авторів.

Для мінімізації зазначених ризиків і подоланню викликів, уряди країн, міжнародні організації намагаються впроваджувати нові технології і розвивати свої системи фінмоніторингу. Традиційно рекомендації FATF (Групи розробки фінансових заходів боротьби з відмиванням грошей), які хоч і не затверджені законом, проте є правилами, обов’язковими до виконання юрисдикціями у всьому світі. Після 2021 року FATF посилила увагу до цифрових фінансових інновацій: було актуалізовано керівництво щодо регулювання VASP і впровадження «правила подорожі» (travel rule) для криптовалютних трансакцій. «Правило подорожі» вимагає від фінансових установ отримувати, зберігати та передавати певну інформацію про відправника та бенефіціара негайно під час передачі віртуальних активів [16]. Під час опитування 2024 року 70% респондентів (65 із 94 юрисдикцій, за винятком тих, які забороняють або планують заборонити VASP) прийняли законодавство, яке

імплементує правила трансакцій. Крім того, 15 юрисдикцій повідомили, що вони знаходяться в процесі ухвалення законодавства для цього. Наприклад, подали законопроекти, видали законопроект, провели громадські консультації щодо законопроектів тощо. Тим не менш, майже третина респондентів ще не прийняла законодавство про впровадження правил про прозорість криптотрансакцій.

Іншим заходом щодо зниження ризику діяльності Фінтех, зокрема VASP, є застосування у цьому секторі заходів контролю за виходом на ринок і відповідного ризик-орієнтованого нагляду з метою ПВК/ФТ. Приклади спеціальних засобів контролю включають:

- використання лише дозволених моделей віртуальних активів, які зберігають платіжний канал для внесення та зняття коштів;
- встановлення порогових значень транзакцій для зняття або внесення та
- вимоги використання інструментів аналізу блокчейну для виявлення червоних прапорців високого ризику, з акцентом на схильність до незаконних джерел, кількості переходів із незаконних джерел, використання міксерів, chain hopping, блокчейнів з підвищеною анонімністю тощо [11].

Ще одним можливим механізмом у досягненні цілей безпечного фінансвого середовища є створення підрозділів фінансової розвідки (ПФР). Такі підрозділи є національними центрами для отримання і аналізу звітів про підозрілі операції та відповідної інформації про відмивання грошей, пов’язані з ними предикатні злочини та фінансування тероризму. Їхня міжнародна співпраця координується Егмонтською групою. Як глобальна організація, Егмонтська група спрощує та сприяє обміну інформацією, знаннями та співпраці між ПФР [17]. Важливо, щоб усі учасники глобального фінансового ринку мали такі структури і брали участь у міжнародному співробітництві.

У контексті теми дослідження варто також звернути увагу на потенціал розвитку технологій для автоматизованої регуляції як з боку урядів, так і у внутрішніх системах фінансових компаній. Для загальної назви технологій, що можуть використовуватись регулятором, Інститут фінансової стабільності (FSI) використовує означення SupTech, тоді як RegTech зазвичай визначається аналогічно, але використовується у значенні технологій регулювання приватними компаніями [18]. Хоча варто зауважити, що з функціональної точки зору це дуже схожі механізми. Застосування SupTech буде ефективним у зборі даних фінансової звітності у реальному часі, а також в управлінні і перевірці даних, їх консолідації та візуалізації. Зокрема, використання штучного інтелекту дає можливість оперувати величезними масивами даних та оптимізації витрат і людської праці у цих процесах. Спільними зусиллями з піднаглядними суб'єктами, Центральний банк Республіки Австрія (OeNB) розробив платформу звітності, яка усуває розрив між IT-системами суб'єктів нагляду та наглядовим органом. Система дозволяє банківському сектору надсилати критично важливу інформацію до OeNB без збільшення адміністративного навантаження на суб’єктів господарювання [19]. SupTech-додатки, особливо в сфері аналізу даних, можуть перетворити моніторинг ризиків з ретроспективного на прогнозний та проактивний процес. Впровадження таких технологій актуально також буде і для Фінтех.

Національний Банк України також має візію щодо запровадження RegTech в Україні. До потенційних напрямів їх застосування можна віднести управління ризиками, надання звітності, ПВК/ФТ та санкції, а також запобігання та протидія шахрайству. Переваги RegTech полягають у підвищеній ефективності, зниженні

витрат та розширенні можливостей [20].

Висновки. Фінтех став каталізатором якісних змін у міжнародному фінансовому секторі. Проте його швидке зростання також супроводжується низкою специфічних ризиків. Відмивання коштів за допомогою віртуальних активів, цифрових платформ, глобальної мережі професійних посередників створює виклики для безпеки користувачів у всьому світі. Для мінімізації таких ризиків необхідне запровадження ефективних стратегій з регулювання ринку фінтеху. Важливо, щоб міжнародна спільнота мала узгоджене бачення щодо концептуального розуміння ринку фінансових технологій, а також мала спільно координовані системи регулювання та протидії відмиванню грошей. Для національних органів фінансового моніторингу важливо запроваджувати й удосконалювати системи моніторингу з впровадженням інноваційних рішень. Це сприятиме автоматизації процесів, надаватиме можливість спостереження за суб'єктами у режимі реального часу. Використання SupTech створюватиме можливість збору, обробці, консолідації та аналізу даних, що розвине наявні механізми і актуалізує регуляторні рішення відповідно до викликів теперішнього часу. З огляду на викладене, важливого значення набуває запровадження комплексних підходів з протидії відмиванню коштів із застосуванням фінансових технологій, а також гармонізація механізмів фінансового моніторингу різних юрисдикцій для подолання викликів, пов'язаних з транскордонністю.

Перспективи подальших досліджень тематики, порушеної у статті, полягають у вивченні потенційних можливостей застосування новітніх технологій не лише у процесах ідентифікації та верифікації клієнтів, але й моніторингу фінансових транзакцій та побудови систем управління ризиками легалізації коштів незаконного походження у фінансових інституціях.

Список використаної літератури:

1. Leuprecht C., Jenkins C., Hamilton R. Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*. 2022. Vol. 30 No. 4, pp. 1036-1054. doi: https://doi.org/10.1108/jfc-07-2022-0161.

2. Dupuis D., Gleason K. Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*. 2020. Vol. 28 No. 1, pp. 60-74. doi: https://doi.org/10.1108/jfc-06-2020-0113.

3. Sinno, R.M., Baldock, G., Gleason, K., Zaher, Z.The regulatory dialectic and innovation in service-based money laundering. *Journal of Financial Crime*. 2024. Vol. 32 No. 1, pp. 245-254. doi: https://doi.org/10.1108/jfc-03-2024-0110.

4. Benson V., Turksen U., Adamyk B. Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*. 2023. Vol. 32 No. 1, pp. 80-97. doi: https://doi.org/10.1108/jfrc-04-2023-0065.

5. Smith M., Tiwari M. The implications of national blockchain infrastructure for financial crime. *Journal of Financial Crime*. 2023. Vol. 31 No. 2, pp. 236-248. doi: https://doi.org/10.1108/jfc-01-2023-0006.

6. Pavlidis G. Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*. 2023. Vol. 26, No 7. pp. 155–166. doi: https://doi.org/10.1108/jmlc-03-2023-0050.

7. FIU - FinTech Cooperation and Associated Cybercrime Typologies and Risks. Egmont Group of Financial Intelligence Units. URL: https://egmontgroup.org/wp-

content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc.-Crimes.pdf.

8. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Official Journal of the European Union*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366.

9. Buckley R. P., Arner D. W., Barberis J. REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation. Wiley & Sons, Incorporated, John, 2019.

10. Duarte F. Fintech Market Size & Future Growth (2025–2029). *Exploding Topics*. URL: https://explodingtopics.com/blog/fintech-market

11. MONEYVAL. Typologies Report: Risks of Money Laundering and Terrorist Financing in the World of Virtual Assets. 2023. URL: http://www.coe.int/moneyval.

12. FATF. Professional Money Laundering. Paris: FATF. 2018. URL: https://www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html.

13. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX (станом на 9 січ. 2025 р.). URL: https://zakon.rada.gov.ua/laws/show/361-20#Text

14. Фінансовий моніторинг. *Національний банк України*. URL: https://bank.gov.ua/ua/supervision/monitoring

15. 2024 Global Financial Crime Report. *Nasdaq Verafin*. 2024. URL: https://www.nasdaq.com/global-financial-crime-report.

16. FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. Paris: FATF. 2024. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.

17. Financial Intelligence Units – Egmont Group. Egmont Group. URL: https://egmontgroup.org/about/financial-intelligence-units/

18. The Global RegTech Industry Benchmark Report 2019. *The Cambridge Centre for Alternative Finance*. URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-12-ccaf-global-regtech-benchmarking-report.pdf.

19. Broeders D., Prenio J. Innovative technology in financial supervision (suptech) – the experience of early users. *Bank for International Settlements*. URL: https://www.bis.org/fsi/publ/insights9.pdf

20. Зелена книга з розвитку регуляторних технологій на фінансовому ринку України. *Національний банк України*. 2025. URL: https://bank.gov.ua/ua/news/all/zelena-kniga-z-rozvitku-regulyatornih-tehnologiy-na-finansovomu-rinku-ukrayini.

Дата надходження статті: 25.01.2025
Дата прийняття статті: 03.02.2025
Дата публікації статті: 20.03.2025