ECONOMIC BULLETIN
of Cherkasy State Technological University Vol. 26. Issue 3(76)2025 141–151

UDC 336.71
DOI: 10.24025/2306-4420.76(3).2025.342955

JEL Classification Code: M 41, H83, M 15
Article's History:
Received: 12.05.2025; Revised: 21.05.2025; Accepted: 02.06.2025.

Nataliya Poliova*
Candidate of Economic Sciences, Associate Professor
Private Higher Education Establishment "European University"
03115, 16V, Academician Vernadsky Blvd., Kyiv, Ukraine
https://orcid.org/0000-0002-5140-2136

Applying the results of FinCEN typological studies in improving the financial monitoring system of Ukraine

Abstract. The article examines the main typologies of money laundering and terrorist financing that were published by the US National Financial Intelligence Service in 2024 and in the first half of 2025. The relevance of the topic is due to the globalisation of capital movement and legislative requirements for reporting entities in the field of financial monitoring to include the results of typological studies in internal risk management systems. The purpose of the work is to single out indicators of suspicion that can be used by Ukrainian reporting entities to improve the effectiveness of internal financial monitoring systems from the typologies. To achieve the goal, the article used the methods of analysis, synthesis and comparison. The main task of the study was to identify indicators of suspicion that have a significant correlation with current conditions of customer servicing by subjects of primary financial monitoring in Ukraine. The results of the study identified 20 indicators of suspicion of money laundering and terrorist financing, characteristic of financial transactions of Ukrainian reporting entities. Eight indicators concerned cash and goods smuggling, four indicators were related to terrorist financing, and the remaining indicators of suspicion belonged to fraudulent schemes when carrying out due diligence measures and using the name of a specially authorised body. It is established that, considering the widespread implementation of remote sales channels by financial entities and the lack of specific video verification requirements, the indicators of suspicion concerning the use of generative artificial intelligence are universal and can be applied by reporting entities in any jurisdiction without serious modification. The possibility of implementing the identified indicators of suspicion into automation systems of Ukrainian reporting entities in the field of financial monitoring is the practical significance of the study. Prospects for further research concern the analysis of typological studies in other jurisdictions with highly effective national systems for combating money laundering and terrorist financing (especially in European Union countries) for the further unification of European and Ukrainian approaches in the field of financial monitoring

Keywords: money laundering, terrorist financing, reporting entities, indicators of suspicion, remote sales channels, financial intelligence unit

*Corresponding author

Наталія Польова
Кандидат економічних наук, доцент
ПВНЗ «Європейський університет»
03115, бульв. Академіка Вернадського, 16В, м. Київ, Україна
https://orcid.org/0000-0002-5140-2136

Використання результатів типологічних досліджень FinCEN у вдосконаленні системи фінансового моніторингу України

Анотація. У статті досліджено основні типології відмивання грошей та фінансування тероризму, які були опубліковані Національною службою фінансової розвідки США у 2024 р. та у першій половині 2025 р. Актуальність теми зумовлена глобалізацією руху капіталу та законодавчими вимогами до звітних установ у сфері фінансового моніторингу щодо включення результатів типологічних досліджень до внутрішніх систем управління ризиками. Метою роботи є виокремлення з типологій індикаторів підозрілості, які можуть бути використані українськими звітними установами для підвищення ефективності внутрішніх систем фінансового моніторингу. Для досягнення мети в статті використано методи аналізу, синтезу та порівняння. Головним завданням дослідження було визначення індикаторів підозрілості, які мають значну кореляцію з поточними умовами обслуговування клієнтів суб'єктами первинного фінансового моніторингу України. Результати дослідження виявили 20 індикаторів підозрілості відмивання коштів та фінансування тероризму, характерних для фінансових операцій українських звітних установ. Вісім індикаторів стосувалися контрабанди готівки та товарів, чотири індикатори були пов'язані з фінансуванням тероризму, решта індикаторів підозрілості належали до шахрайських схем при здійсненні заходів належної перевірки та при використанні імені спеціально уповноваженого органу. Встановлено, що, зважаючи на широке впровадження дистанційних каналів продажу фінансовими установами та відсутність специфічних вимог до відеоверифікації, індикатори підозрілості, які стосуються використання генеративного штучного інтелекту, є універсальними та можуть бути застосовані звітними установами в будь-якій юрисдикції без серйозної модифікації. Практичним значенням дослідження є можливість імплементації виявлених індикаторів підозрілості до систем автоматизації українських звітних установ у сфері фінансового моніторингу. Перспективи подальших досліджень стосуються аналізу типологічних досліджень в інших юрисдикціях з високоефективними національними системами протидії відмиванню коштів та фінансуванню тероризму (особливо в країнах Європейського Союзу) для подальшої уніфікації європейських та українських підходів у сфері фінансового моніторингу

Ключові слова: відмивання коштів, фінансування тероризму, звітні установи, індикатори підозрілості, дистанційні канали продажу, підрозділ фінансової розвідки

Вступ

Типологічні дослідження в сфері протидії легалізації злочинних доходів, фінансуванню тероризму або фінансуванню розповсюдження зброї масового знищення здійснюються службами фінансових розвідок, оскільки в них відображені типові способи скоєння злочинів, які було виявлено та задокументовано. Результуючою частиною типологічних досліджень є формування переліку індикаторів підозрілості, які допомагають працівникам, відповідальним за дотримання норм фінансового моніторингу, зробити висновок про ризик використання компанії у схемах відмивання коштів, фінансування тероризму або фінансування зброї масового знищення. Ці індикатори перетворюють абстрактні ризики на конкретні ознаки, які можуть бути виявлені при здійсненні транзакцій або при аналізі поведінки учасників фінансової операції. Кожен із них окремо не означає, що клієнт є частиною злочинної схеми. Однак суб'єкти первинного фінансового моніторингу можуть використовувати ці індикатори для вчасної ідентифікації підозрілих операцій та більш точного визначення загального ризик-

профілю клієнтів або їх операцій. Згідно з українським законодавством суб'єкт первинного фінансового моніторингу зобов'язаний враховувати типологічні дослідження при визначенні індикаторів підозрілості фінансових операцій (Верховна Рада України, 2019, Грудень 06). Розрахунок ризик-профілю є останнім етапом заходів належної перевірки клієнтів, який фіксує рівень впевненості звітної установи у сфері фінансового моніторингу в надійності свого клієнта або ефективності власної системи управління ризиками (Національний банк України, 2020). Тому від якості сформульованих індикаторів підозрілості напряму залежить якість всієї системи фінансового моніторингу звітної установи.

Враховуючи глобальний характер сучасних фінансових мереж та значне поширення дистанційних методів ідентифікації та верифікації клієнтів, аналіз типологічних досліджень національної служби фінансової розвідки США (Financial Crimes Enforcement Network – FinCEN) дозволить українським компаніям актуалізувати внутрішні переліки індикаторів підозрілості та підвищить ефективність внутрішніх систем фінансового моніторингу.

Огляд літератури

Сфера боротьби з легалізацією коштів та фінансуванням тероризму досліджується науковою спільнотою, в першу чергу, з позицій аналізу функціонування певних елементів системи фінансового моніторингу та можливих шляхів зростання їх ефективності. Зокрема, в роботі М. О. Перепелиці (2021) досліджується обіг віртуальної валюти, яка є об'єктом фінансового моніторингу. У праці А. Буряченко та А. Служенко (2024) розглядається скорингова модель, призначена для оцінювання ризиків фінансових злочинів. В. Літкевич (2022) проаналізував міжнародне співробітництво, яке здійснюється в сфері фінансових розслідувань. При дослідженні типологій відмивання коштів та фінансування тероризму науковці зосереджували увагу на проблемах глобального рівня. P. Reuter та M. Riccardi (2024) аналізували емпіричні й теоретичні матеріали стосовно вивчення поведінки правопорушників та причин вибору певних схем відмивання коштів. E. A. Akartuna *et al.* (2024) намагалися стандартизувати інформацію, яка використовувалась у типологічних дослідженнях Міжнародної групи з протидії відмиванню брудних грошей (Financial Action Task Force on Money Laundering – FATF). Таким чином, типології на рівні окремої юрисдикції, яка мала ефективну систему фінансового моніторингу та розвинену фінансову інфраструктуру, залишалися недостатньо дослідженими.

Метою статті є аналіз останніх типологічних досліджень, здійснених фінансовою розвідкою США, який дозволить суб'єктам первинного фінансового моніторингу України оновити внутрішній перелік індикаторів підозрілості та підвищити ефективність власних систем фінансового моніторингу.

Результати дослідження

Значна увага державних регуляторів та правоохоронних органів у США була прикута до проблеми контрабанди та репатріації готівки транснаціональними злочинними організаціями. До таких організацій у США, в першу чергу, належать мексиканські картелі, які отримують готівкові доходи на території Сполучених Штатів від широкого спектру незаконної діяльності, такої як торгівля наркотиками, торгівля людьми та контрабанда людей. Після первинного накопичення незаконних готівкових коштів відбувається їх вивезення зі Сполучених Штатів до Мексики шляхом використання кур'єрів-фізичних осіб або приватних транспортних засобів. За оцінками правоохоронних органів США, обсяг контрабандної готівки становить у середньому сотні тисяч доларів США щодня (Financial Crimes Enforcement Network, 2025, March 31). Готівкові кошти надсилаються підприємствам-співучасникам, які розташовані поблизу південно-західного кордону Сполучених Штатів. Частина таких підприємств здійснює активну економічну діяльність. Інші підприємства є компаніями-оболонками.

Отримавши незаконні кошти, мексиканські компанії, під виглядом «законного» бізнесу, намагаються репатріювати готівкові долари США до Сполучених Штатів. Готівка

транспортується авіатранспортом або наземним транспортом. Крім того, можливе використання авіатранспорту з Мексики до Канади з подальшим трансфером готівки з Канади до США. Для транспортування використовуються офіційні служби інкасації. На території США служба інкасації отримує інструкції по доставці коштів до фінансової установи США або до Федерального резервного банку, де фінансова установа американської служби інкасації має доларовий рахунок. У багатьох випадках готівка може переміщуватися кількома службами інкасації до кількох місць на території Сполучених Штатів, перш ніж кошти будуть депоновані на рахунок. Додатковою складністю є наявність у деяких служб інкасації США послуг зарахування вартості готівки без її фізичної доставки до фінансової установи. У таких випадках служба інкасації може «купити» готівку у клієнта та зарахувати її еквівалент на банківський рахунок клієнта в США.

Після зарахування коштів фінансовою установою в США відбувається трансфер безготівкових коштів до фінансових установ, розташованих у Мексиці. Альтернативним варіантом є придбання товарів у Сполучених Штатах або на міжнародному ринку для їх подальшого продажу в Мексиці чи в інших країнах у рамках схеми відмивання грошей, що базується на торгівлі.

Контрабанда готівки злочинними організаціями Мексики містить такі головні індикатори злочинної схеми: доставка великих обсягів готівки від мексиканських компаній до фінансової установи в США службами інкасації та відмова надавати інформацію щодо походження транспортованої валюти; отримання мексиканською компанією значної суми коштів як кредиту від американської служби інкасації, яка зараховується на рахунок американської фінансової установи; розмір або профіль бізнесу компанії, яка виступає ініціатором переказу готівки, не відповідає обсягам транспортованої валюти. Українські суб'єкти первинного фінансового моніторингу, враховуючи результати типологічного дослідження FinCEN щодо контрабанди готівки, можуть використовувати для моніторингу клієнтів перелік індикаторів підозрілості, зазначений у таблиці 1.

Таблиця 1. Індикатори підозрілості, пов'язані з контрабандою готівки

Предмет типологічного дослідження FinCEN	Індикатори підозрілості	Профіль діяльності компанії, яка аналізує індикатори підозрілості
контрабанда готівки	клієнт надає запит на трансфер великих обсягів готівки без надання інформації про походження коштів	банк або інша нефінансова установа з ліцензією на послуги інкасації
контрабанда готівки	розмір бізнесу клієнта не відповідає обсягам транспортованої валюти	банк або інша нефінансова установа з ліцензією на послуги інкасації
контрабанда готівки	вид діяльності клієнта не відповідає обсягам транспортованої валюти	банк або інша нефінансова установа з ліцензією на послуги інкасації
контрабанда готівки	зарахування на рахунок клієнта великих обсягів готівкових коштів від декількох служб інкасації	банк або інша фінансова установа, яка має право відкривати поточні валютні рахунки
контрабанда готівки	транскордонний переказ безготівкових коштів клієнта на рахунок іншої юридичної особи без зрозумілої мети або без підтверджуючих документів	фінансові установи, банки, оператори платіжних систем
контрабанда готівки	купівля клієнтом-юридичною особою на міжнародному ринку різнорідних груп товарів, які не відповідають його виду діяльності, та подальший продаж таких товарів оптовим компаніям всередині країни	фінансові установи, банки, оператори платіжних систем

Джерело: розроблено автором на основі (Financial Crimes Enforcement Network, 2025, March 31)

Останніми роками найвагомішим незаконним джерелом доходів для мексиканських картелів, яке не було пов'язане з наркотиками, стали крадіжки та контрабанда сирої нафти. Нафтопереробні заводи Мексики не мають достатньої потужності для переробки видобутої кислої та важкої сирої нафти. В результаті Мексика експортує таку нафту до більш потужних нафтопереробних заводів у США, а звідти імпортує перероблений бензин, дизельне та інші види палива. Транснаціональні злочинні організації експлуатують цей потік сирої нафти між Мексикою та США.

На першому етапі відбувається викрадення нафти. Для цього злочинці використовують різні способи, включаючи незаконне врізання в паливні трубопроводи, крадіжки з нафтопереробних заводів та захоплення автоцистерн. Також застосовується підкуп працівників мексиканських нафтовидобувних компаній та місцевих чиновників. Сира нафта зазвичай транспортується автоцистернами через південно-західний кордон США, маркована як «відпрацьоване мастило» або інші небезпечні матеріали, пов'язані з процесом переробки нафти та природного газу. Це маркування дозволяє уникати додаткових перевірок та ухилятися від податків і регулювань. Отримувачами нафти виступають американські імпортери-спільники. В ланцюжку передачі сирої нафти від Мексики до США використовується мережа фіктивних компаній, а імпортери в США частину свого бізнесу ведуть у легальній площині, що створює додаткові труднощі для ідентифікації схеми відмивання коштів. Отримавши мексиканську нафту, американські компанії здійснюють її продаж як сиру нафту марки West Texas Intermediate (WTI) або як інші види сирої нафти з великою знижкою на енергетичному ринку США або на міжнародних ринках, а незаконні прибутки репатріюють до Мексики. За оцінками правоохоронних органів США, американські імпортери можуть отримувати понад п'ять мільйонів доларів США прибутку від кожного танкерного відправлення сирої нафти зі Сполучених Штатів до іноземних юрисдикцій. При цьому щомісяця в дорозі перебуває кілька танкерів таких імпортерів (Financial Crimes Enforcement Network, 2025, May 01).

Стосовно контрабанди нафти «червоним прапорцем» може бути розміщення на вебсайті американської нафтогазової, імпортної або транспортної компанії інформації, що така компанія є лише покупцем або продавцем сирої нафти. Водночас компанія надсилає банківські перекази мексиканським або американським компаніям за купівлю відпрацьованої нафти або інших небезпечних речовин. Також індикатором є ситуація, коли американська компанія надсилає банківські перекази за купівлю відпрацьованої нафти або інших небезпечних речовин, не маючи відповідних дозволів від Агентства з охорони навколишнього середовища США.

До індикатора підозрілості, що пов'язаний з контрабандою товарів та який може бути використаний звітними установами з фінансового моніторингу в Україні, можна віднести отримання клієнтом установи безготівкових коштів від контрагентів за товари, які не характерні для виду економічної діяльності клієнта. Інформація щодо задекларованого клієнтом профілю бізнесу міститься в державних реєстрах, довідках з податкових органів, опитувальниках, підписаних уповноваженими особами клієнта. Також очевидним «червоним прапорцем» для українських звітних установ може бути продаж клієнтом товарів за цінами, які є значно нижчими за ринкові.

Типологічне дослідження, пов'язане з фінансуванням тероризму, стосувалося виявлення грошових потоків, призначених для фінансування мережі «Хезболла», яку в США визнано іноземною терористичною організацією. Діяльність «Хезболли» має глобальний масштаб і поширюється на Африку, Азію, Європу та Західну півкулю. У повідомленні FinCEN у травні 2024 р. було зазначено, що Іран щорічно надає «Хезболлі» фінансову підтримку у розмірі близько 700 мільйонів доларів США (Financial Crimes Enforcement Network, 2024, October 23). «Хезболла» також виступає каналом для коштів, що надходять з Ірану до інших пов'язаних з Іраном груп. Крім того, ця організація діяла на кордоні

Аргентини, Бразилії та Парагваю, а також у зонах вільної торгівлі Панами для отримання доходів за рахунок як законної, так і незаконної діяльності. Організація отримує доходи від широкого спектру незаконної діяльності, включаючи контрабанду нафти, відмивання грошей, обмін грошей на чорному ринку, підробку та незаконне придбання зброї.

Значна частина доходів отримується організацією за рахунок контрабанди та продажу іранської нафти й скрапленого нафтового газу покупцям в Азії та на Близькому Сході, часто у співпраці з Корпусом вартових Ісламської революції (КВІР) та мережами хуситів. Нафта контрабандою перевозиться через складну мережу посередників і судноплавних мереж, використовуючи судна, що зазвичай належать підставним компаніям у юрисдикціях третіх країн. У деяких випадках, щоб приховати походження нафти, мережі посередників змішують іранську нафту з нафтою з інших країн.

На Близькому Сході «Хезболла» отримує прибуток від контрабанди золота, електроніки та іноземної валюти з Ірану до сусідніх країн. Товари та валюта перевозяться контрабандою через кордони або продаються через підставні компанії. Отримані нелегальні доходи повертаються до Ірану, зазвичай через контрабанду готівки великих обсягів, або відмиваються за допомогою підставних компаній. Крім того, «Хезболла» отримує прибутки від численних бізнес-проектів у Лівані та інших країнах Близького Сходу.

«Хезболла» та її прихильники використовували розгалужену глобальну мережу підставних компаній та легального бізнесу в секторах нерухомості, міжнародної торгівлі, будівництва, торгівлі дорогоцінним камінням та творами мистецтва для переміщення та відмивання коштів. Згідно з Національною оцінкою ризиків фінансування тероризму США за 2024 р. «Хезболла» продовжувала використовувати фінансову систему США у своїх схемах відмивання грошей, контрабанди та торгівлі людьми. Зокрема, організація та її прихильники здійснювали перекази коштів через фінансову систему США та намагалися через фіктивні компанії придбати військове або експортно-контрольоване обладнання. Для уникнення санкцій та проведення платежів рахунки відкривалися на непов’язаних номінальних фізичних та юридичних осіб. Використовуючи результати типологічного дослідження FinCEN щодо протидії фінансуванню тероризму, сформовано наступні індикатори, які українські суб’єкти первинного фінансового моніторингу можуть використовувати при моніторингу діяльності власних клієнтів (таблиця 2).

Таблиця 2. Індикатори підозрілості, пов’язані з фінансуванням тероризму

Предмет типологічного дослідження FinCEN	Індикатори підозрілості	Профіль діяльності компанії, яка аналізує індикатори підозрілості
фінансування тероризму	клієнт здійснює фінансові операції, учасником яких є компанії, пов'язані з «сірим» танкерним флотом	фінансові установи, банки, оператори платіжних систем
фінансування тероризму	клієнт здійснює продаж нафти чи нафтопродуктів на світовому ринку за цінами, які є значно нижчими за ринкові	фінансові установи, банки, оператори платіжних систем
фінансування тероризму	юридична особа-нерезидент здійснює безготівкові трансфери в значних обсягах на рахунки клієнта-резидента. Водночас відсутня інформація про наявність значного обсягу бізнесу компанією-нерезидентом на її внутрішньому ринку або інших закордонних ринках	фінансові установи, банки, оператори платіжних систем
фінансування тероризму	клієнт є учасником фінансових операцій з придбання військового або експортно-контрольованого обладнання. Водночас клієнт не володіє необхідними дозвільними документами на здійснення цієї діяльності та / або не є відомою компанією на цьому ринку згідно з відкритими джерелами інформації	фінансові установи, банки, оператори платіжних систем

Джерело: розроблено автором на основі (Financial Crimes Enforcement Network, 2024, October 23)

Типологічне дослідження FinCEN, опубліковане в листопаді 2024 р., акцентує увагу на проблемі використання контенту, створеного за допомогою інструментів генеративного штучного інтелекту. Цей контент становить нові загрози фінансовим установам при здійсненні процедур ідентифікації та верифікації клієнтів. Для виокремлення даних такого типу зазвичай використовують поняття «діпфейк-контент», або просто «діпфейк». Діпфейки можуть створювати ілюзію реальних подій, наприклад, коли людина робить або говорить те, чого насправді не робила чи не казала. Провідні розробники генеративного штучного інтелекту зобов'язалися впроваджувати нагляд і контроль, які спрямовані на зменшення кількості шкідливих діпфейків та інших зловживань. Однак злочинці розробляють методи для обходу таких запобіжників. Крім того, деякі інструменти штучного інтелекту мають відкритий код, що дозволяє користувачам змінювати його та потенційно обходити встановлений контроль.

Фінансові установи США, починаючи з 2023 р., інформували FinCEN у звітах про підозрілу діяльність про факти використання шахраями штучного інтелекту для зміни або генерації зображень, які потім розміщувалися на ідентифікаційних документах клієнтів. Злочинці створювали діпфейкові зображення шляхом модифікації автентичного вихідного зображення або повністю синтетичне зображення. При наявності у шахраїв викраденої особистої ідентифікаційної інформації щодо клієнта в паспортах або водійських посвідченнях такі дані містилися разом зі згенерованою фотографією. Якщо доступу до фактичних ідентифікаційних даних у злочинців не було, така інформація створювалася штучним інтелектом. Аналіз FinCEN показав, що зловмисники успішно відкривали рахунки, використовуючи шахрайські ідентифікатори, створені за допомогою генеративного штучного інтелекту. Надалі такі рахунки використовувалися для зарахування на них коштів від інших нелегальних схем, включаючи шахрайство з чеками, кредитними картками, авторизованими push-платежами, позиками, допомогою по безробіттю (Financial Crimes Enforcement Network, 2024, November 13). Для отримання необхідних даних від клієнтів або співробітників фінансових установ злочинці використовували складні моделі соціальної інженерії, в яких містився голос або відеофайл, створений штучним інтелектом. Наприклад, у схемах «сімейної надзвичайної ситуації» шахраї використовували згенеровані голоси або відео, щоб видавати себе за члена сім'ї жертви, друга чи іншу довірену особу. Схожим способом злочинці користувалися й при спробах корпоративного шахрайства, видаючи себе за керівника або іншого співробітника компанії. Метою такої діяльності було надання жертвам інструкцій щодо переказу коштів компанії на певні рахунки.

Перелік «червоних прапорців» щодо шахрайства на етапі здійснення звітною установою належної перевірки клієнта не залежить від юрисдикції, оскільки злочинці використовують однакові методи генеративного штучного інтелекту. Приклади індикаторів підозрілості, які запропоновано використовувати звітним установам з фінансового моніторингу як у США, так і в Україні, наведені в таблиці 3.

Останньою еволюцією шахрайства, що впливає на FinCEN, є зловживання назвою, символікою або повноваженнями фінансової розвідки США задля отримання фінансової вигоди. Одна з типологій шахрайства полягає в тому, що зловмисники переконують компанії сплатити «збір» за те, щоб третя сторона (тобто шахрай) направила «звіт про бенефіціарних власників» такої компанії до FinCEN. Для зв'язку з потенційними жертвами застосовуються текстові повідомлення, електронна пошта або пошта США. В повідомленнях акцентується увага на ризиках отримання суворих штрафів або судових позовів від FinCEN та уряду США у разі відмови від сплати коштів. Насправді ж законодавством США не встановлено жодної плати за надання такого звіту. А нещодавнє рішення федерального суду встановило відсутність обов'язку компаній подавати звіт про бенефіціарних власників. Відповідно, у компаній відсутня відповідальність за ненадання такого звіту, поки рішення суду залишається в силі. Після реалізації схеми шахраї отримують гроші, але ніколи не подають документи до FinCEN.

Таблиця 3. Індикатори підозрілості, пов'язані з використанням фальшивих ідентифікаційних даних клієнтів

Предмет типологічного дослідження FinCEN	Індикатори підозрілості	Профіль діяльності компанії, яка аналізує індикатори підозрілості
використання фальшивих ідентифікаційних даних клієнтів	клієнт надає ідентифікаційний документ, в якому фотографія має візуальні ознаки зміни або не відповідає іншій ідентифікаційній інформації щодо такого клієнта	всі види суб'єктів первинного фінансового моніторингу
використання фальшивих ідентифікаційних даних клієнтів	надання клієнтом кількох ідентифікаційних документів, які не відповідають один одному	всі види суб'єктів первинного фінансового моніторингу
використання фальшивих ідентифікаційних даних клієнтів	використання клієнтом стороннього плагіну для вебкамери під час відеоверифікації	всі види суб'єктів первинного фінансового моніторингу
використання фальшивих ідентифікаційних даних клієнтів	відмова клієнта від здійснення багатофакторної автентифікації	всі види суб'єктів первинного фінансового моніторингу
використання фальшивих ідентифікаційних даних клієнтів	невідповідність даних геолокації з пристрою клієнта його ідентифікаційним документам	всі види суб'єктів первинного фінансового моніторингу

Джерело: розроблено автором на основі (Financial Crimes Enforcement Network, 2024, November 13)

Поширеною схемою шахрайства, що пов'язана з використанням імені та повноважень служби фінансової розвідки США, є реєстрація компанії у FinCEN як «підприємства, що надає послуги з обігу грошових коштів» (Money Services Business – MSB). За невеликими винятками компанії, які відповідають визначенню MSB, зобов'язані зареєструватися в FinCEN протягом 180 днів з дати заснування MSB. Після реєстрації в FinCEN MSB включається до загальнодоступного реєстру суб'єктів, зареєстрованих у FinCEN. Злочинці використовують подальшу появу своєї компанії на «Сторінці пошуку зареєстрованих MSB FinCEN», щоб створити у потенційних жертв враження легітимності. На корпоративних сайтах таких компаній часто використовуються твердження, що організація перевірена, схвалена або ліцензована FinCEN, тоді як насправді сам факт реєстрації MSB не надає жодного типу схвалення. Після реєстрації компанія використовується як частина схеми з інвестування коштів у віртуальні активи (Financial Crimes Enforcement Network, 2024, December 18). В рамках цих схем шахраї можуть інструктувати жертв купувати віртуальну валюту через постачальників послуг віртуальних активів та направляти жертв до переказу коштів шахрайським MSB.

Крім того, злочинці намагаються видавати себе за співробітників фінансової розвідки або інших урядових установ. Така типологія передбачає контакт шахраїв з людьми за допомогою підроблених телефонних дзвінків, текстових повідомлень, електронних листів або пошти США. У багатьох випадках для переконання у легітимності шахраями можуть бути використані викрадені особисті ідентифікаційні дані урядових працівників та потенційних жертв. Наприклад, шахраї зв'язуються з жертвами, вже знаючи їхні імена, номери соціального страхування та номери банківських рахунків. Шахраї також стверджують, що вони є працівниками FinCEN, і вимагають платежі за нібито порушення у сфері фінансового моніторингу або за непогашені борги. У рамках таких схем шахраї надають жертвам фіктивну документацію, включаючи документи нібито від директора або заступника директора FinCEN. При несплаті коштів на вказані рахунки жертви отримують погрози про арешт їхніх рахунків, якщо платежі не будуть здійснені. В інших випадках

шахраї стверджують, що жертви мають право на фінансовий грант від Міністерства фінансів США, але для його отримання вони повинні надати інформацію про свій банківський рахунок та здійснити переказ коштів до FinCEN.

Транспонуючи типологічне дослідження на діяльність українських звітних установ, можна виокремити наступні індикатори підозрілості, пов'язані з шахрайством від імені спеціально уповноваженого органу (таблиця 4).

Таблиця 4. Індикатори підозрілості, пов'язані зі здійсненням шахрайських дій від імені підрозділу фінансової розвідки

Предмет типологічного дослідження FinCEN	Індикатори підозрілості	Профіль діяльності компанії, яка аналізує індикатори підозрілості
шахрайські дії від імені підрозділу фінансової розвідки	клієнт-юридична особа намагається залучити клієнтів шляхом рекламування себе як надзвичайно стабільної компанії. На підтвердження юридична особа демонструє документи щодо її перебування на обліку в спеціально уповноваженому органі	всі види суб'єктів первинного фінансового моніторингу
шахрайські дії від імені підрозділу фінансової розвідки	клієнт є учасником фінансових операцій, в яких іншими учасниками є постачальники послуг віртуальних активів, внесені до «чорних» списків	всі види суб'єктів первинного фінансового моніторингу
шахрайські дії від імені підрозділу фінансової розвідки	зловмисники під виглядом співробітників підрозділу фінансової розвідки вимагають від звітних установ здійснення платежів за нібито порушення у сфері фінансового моніторингу або за непогашені штрафні санкції, накладені державними регуляторами	всі види суб'єктів первинного фінансового моніторингу

Джерело: розроблено автором на основі (Financial Crimes Enforcement Network, 2024, December 18)

Висновки

До головних індикаторів підозрілості, які національні суб'єкти первинного фінансового моніторингу можуть включити до своїх систем управління ризиками після аналізу типологічного дослідження служби фінансової розвідки США стосовно контрабанди готівки, належать: запит на переміщення значних готівкових коштів без підтверджуючих документів про походження грошей; розмір бізнесу або вид економічної діяльності клієнта, що не відповідає обсягам готівкових транзакцій; зарахування на рахунок клієнта значних сум коштів від декількох служб інкасації; транскордонний трансфер коштів без очевидної економічної мети; здійснення клієнтом імпортних операцій щодо різних груп товарів та перепродаж їх оптовим компаніям на внутрішньому ринку. Стосовно контрабанди товарів, українським установам варто впровадити «червоні прапорці» при отриманні безготівкових коштів клієнтом за продукцію, до якої він не має відношення згідно з офіційними документами про види його економічної діяльності, та у випадку реалізації клієнтом продукції за демпінговими цінами.

Враховуючи типологію FinCEN щодо фінансування мережі «Хезболла», індикаторами підозрілості фінансування тероризму для звітних установ України можуть бути: участь клієнта в операціях, пов'язаних з напівлегальним танкерним флотом; продаж клієнтом нафти або продуктів із неї за зниженими цінами на міжнародному ринку; надходження суттєвих сум коштів від закордонної компанії, яка не має значної ринкової ваги в країні реєстрації; купівля клієнтом зброї або товарів подвійного значення без необхідних дозвільних документів.

Типологія FinCEN щодо використання генеративного штучного інтелекту при здійсненні належної перевірки клієнта містить такий перелік індикаторів підозрілості, корисних у використанні як для американських, так і для українських звітних установ у сфері фінансового моніторингу: фото в наданому клієнтом документі, яке не відповідає

іншій ідентифікаційній інформації про клієнта; надання клієнтом декількох ідентифікаційних документів, які не відповідають один одному; використання клієнтом при відеоверифікації стороннього плагіну для вебкамери; відмова проходження клієнтом багатофакторної ідентифікації; геолокаційні дані з пристрою клієнта, що не відповідають наявній в установі інформації щодо місцезнаходження клієнта.

Новітнім видом шахрайства є використання даних самого підрозділу фінансової розвідки для отримання коштів від піднаглядних установ. До індикаторів підозрілості, які можуть використовувати українські суб'єкти первинного фінансового моніторингу з метою уникнення ризику бути використаними в шахрайських схемах, належать: рекламування клієнтом своєї діяльності через поширення інформації про перебування клієнта на обліку в спеціально уповноваженому органі; участь клієнта у фінансових операціях, учасниками яких є підозрілі постачальники послуг віртуальних активів; надходження вимог від осіб, які видають себе за співробітників спеціально уповноваженого органу, про сплату штрафів у сфері фінансового моніторингу.

Подяки

Немає.

Конфлікт інтересів

Немає.

Список використаних джерел

Буряченко, А., & Служенко, А. (2024). Скорингова модель для оцінки ризиків фінансових злочинів. *Економіка та суспільство, 68*. doi: 10.32782/2524-0072/2024-68-66

Верховна Рада України. (2019, Грудень 06). *Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.* Закон України № 361-IX. Взято з https://zakon.rada.gov.ua/laws/show/361-20#Text

Літкевич, В. (2022). Міжнародне співробітництво у фінансових розслідуваннях – формування основних елементів. *Актуальні проблеми правознавства, 3(*31*),* 55–62. doi: 10.35774/app2022.03.055

Національний банк України. (2020, Липень 28). *Положення про здійснення установами фінансового моніторингу.* Постанова Правління Національного банку України № 107. Взято з https://zakon.rada.gov.ua/laws/show/v0107500-20#Text

Національний банк України. (2020, Травень 19). *Положення про здійснення банками фінансового моніторингу.* Постанова Правління Національного банку України № 65. Взято з https://zakon.rada.gov.ua/laws/show/v0065500-20#Text

Перепелиця, М. О. (2021). Віртуальна валюта як об'єкт фінансового моніторингу: врахування досвіду іноземних країн при формуванні національного законодавства. *Право та інновації*, *2*(34), 58–66. doi: 10.37772/2518-1718-2021-2(34)-7

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2024). Motivating a standardized approach to financial intelligence: A typological scoping review of money laundering methods and trends. *Journal of Experimental Criminology*, 1–47. doi: 10.1007/s11292-024-09623-y

Financial Crimes Enforcement Network (2024, December 18). *FinCEN Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain*. Retrieved from https://www.fincen.gov/sites/default/files/2024-12/Alert-FinCEN-Scams-FINAL508.pdf

Financial Crimes Enforcement Network (2024, November 13). *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions.* Retrieved from https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

Financial Crimes Enforcement Network (2024, October 23). *FinCEN Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities*. Retrieved from https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Hizballah-Alert-508C.pdf

Financial Crimes Enforcement Network (2025, March 31). *FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations.* Retrieved from https://www.fincen.gov/sites/default/files/shared/BCS-Alert-FINAL-508C.pdf

Financial Crimes Enforcement Network (2025, May 01). *FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels*. Retrieved from https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Oil-Smuggling-FINAL-508C.pdf

Reuter, P., & Riccardi, M. (2024). Introduction to special issue on "Understanding money laundering: Empirical and theoretical insights into offenders, typologies, and determinants of criminal behaviour". *European Journal on Criminal Policy and Research*, 1–6. doi: 10.1007/s10610-024-09604-x

References

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2024). Motivating a standardized approach to financial intelligence: A typological scoping review of money laundering methods and trends. *Journal of Experimental Criminology*, 1–47. doi: 10.1007/s11292-024-09623-y

Buryachenko, A., & Sluzhenko, A. (2024). Scoring model for assessing financial crime risks. *Economy and society, 68*. doi: 10.32782/2524-0072/2024-68-66

Financial Crimes Enforcement Network (2024, December 18). *FinCEN Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain*. Retrieved from https://www.fincen.gov/sites/default/files/2024-12/Alert-FinCEN-Scams-FINAL508.pdf

Financial Crimes Enforcement Network (2024, November 13). *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions*. Retrieved from https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

Financial Crimes Enforcement Network (2024, October 23). *FinCEN Alert to Financial Institutions to Counter Financing of Hizballah and its Terrorist Activities*. Retrieved from https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Hizballah-Alert-508C.pdf

Financial Crimes Enforcement Network (2025, March 31). *FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations.* Retrieved from https://www.fincen.gov/sites/default/files/shared/BCS-Alert-FINAL-508C.pdf

Financial Crimes Enforcement Network (2025, May 01). *FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels*. Retrieved from https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-Oil-Smuggling-FINAL-508C.pdf

Litkevych, V. (2022). International cooperation in financial investigations – formation of the basic elements. *Current Legal Problems, 3*(31), 55–62. doi: 10.35774/app2022.03.055

National Bank of Ukraine. (2020, July 28). *Regulations on the implementation of financial monitoring by institutions.* Resolution of the Board of the National Bank of Ukraine No. 107. Retrieved from https://zakon.rada.gov.ua/laws/show/v0107500-20#Text

National Bank of Ukraine. (2020, May 19). *Regulations on the implementation of financial monitoring by banks*. Resolution of the Board of the National Bank of Ukraine No. 65. Retrieved from https://zakon.rada.gov.ua/laws/show/v0065500-20#Text

Perepelytsiya, M. O. (2021). Virtual currency as an object of financial monitoring: Taking into account the experience of foreign countries in the formation of national legislation. *Law and innovations, 2*(34), 58–66. doi: 10.37772/2518-1718-2021-2(34)-7

Reuter, P., & Riccardi, M. (2024). Introduction to special issue on "Understanding money laundering: Empirical and theoretical insights into offenders, typologies, and determinants of criminal behaviour". *European Journal on Criminal Policy and Research*, 1–6. doi: 10.1007/s10610-024-09604-x

Verkhovna Rada of Ukraine. (2019, December 06). *On prevention and counteraction to the legalization (laundering) of proceeds of crime, financing of terrorism and financing of the proliferation of weapons of mass destruction*. Law of Ukraine No. 361-IX. Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text