УДК 351.746.1:336.711.65]:[343.35+343.34]:343.98
DOI https://doi.org/10.32782/ln.2024.24.17

Макаренков О.Л.
доктор юридичних наук, професор,
головний науковий співробітник Науково-дослідної частини
Запорізький національний університет

ДЕЛЕГАЛІЗАЦІЯ КОРУПЦІЙНИХ ДОХОДІВ І ФІНАНСУВАННЯ ТЕРОРИЗМУ КРИМІНАЛІСТИЧНИМИ ЦИФРОВИМИ ТЕХНОЛОГІЯМИ

Вступ. Поширення інформації у цифровому форматі давній висхідний тренд, що зростає експоненційно. Його традиційними напрямами залишаються сфери фінансів, міжнародних розрахунків, біржової торгівлі тощо. Корупційні чи інші злочинні доходи завжди присутні у цих сферах як у вигляді неправомірно набутих матеріальних благ внаслідок контрабанди, використання операцій страхових компаній, використання послуг ломбардів, використання платіжних систем і безтоварних операцій фіктивних угод, використання послуг банківських установ, застосування віртуальних активів, так й за наслідками надання їм видимості правомірності (нім. Unrecht Gut gedeiht nicht). Цифрові технології і створений ними кіберпростір інструменти і середовище відмивання злочинних коштів. Відслідковування, доказування і/або повернення злочинних матеріальних активів у фізичному світі завжди серйозний виклик для органів юстиції, з яким можуть впоратись тільки окремі з них й тільки у міжнародній співпраці, а також з посиленням їхніх криміналістичних спроможностей цифровими інструментами [1], «які дозволяють усувати недоліки правової системи, що … не має достатніх ресурсів для кількості справ», пов'язаних з делегалізацією корупційних доходів та фінансування тероризму [2, с. 122, 123].

У кібернетичному світі такі розслідування ускладнюються швидкістю і кількістю вчинюваних злочинцями операцій, фізичним перебуванням учасників і апаратного забезпечення таких операцій на територіях різних юрисдикцій, що ще більше актуалізує міжнародну співпрацю правоохоронних структур. Наприклад, у 2021 р. спільні операції правоохоронців з Німеччини, Австралії, Данії, Молдови, України, Великобританії (the National Crime Agency) і США (Drug Enforcement Administration, Federal Bureau of Investigation, Internal Revenue Service) за підтримки Європолу, в частині спеціального оперативного аналізу і координації транскордонної співпраці залучених країн, дозволили ліквідувати тіньовий незаконний ринок у прихованій інтернет мережі «DarkMarket», яка мала 500 000 користувачів, більше 2400 продавців, понад 320 000 транзакцій (в основному торгівлі усіма видами наркотиків, підробленими грошима, краденими або підробленими реквізитами кредитних карток, анонімними SIM-картами, шкідливим програмним забезпеченням), використала більше 4650 біткоїнів (Bitcoin) і 12 800 монеро (Monero / XMR – криптовалюта на основі блокчейну, на протоколі CryptoNote), що за поточним курсом більше 140 мільйонів євро [4].

Приховування неправомірно набутих активів в межах національної юрисдикції легко викривається і ще легше вони вилучаються, оскільки глибинна корупція заперечує верховенство права. Верховенство права власності так само виключається корупцією. Незаконність активу тільки посилює його незахищеність в умовах корумпованої нації, яка обрала замість правових стандартів стандарти обману, насильства, задоволення приватного інтересу за рахунок публічного інтересу та інші викривлення природного права (лат. male parta male dilabuntur). Ефект від правоохоронної роботи в межах іноземних юрисдикцій організаційно

вимагає більше часу, ніж еквіваленті зусилля правоохоронців в рамках національного правового простору. Забезпечена цифровими технологіями оперативність досудового слідства у справах з протидії відмиванню злочинних коштів передбачає залучення фахівців з цих технологій у кіберпросторі, зокрема на маркетплейсах дарктнету (англ. darknet market), біржах з торгівлі віртуальним активами, прихованих ресурсами ШІ, коли «технологія стає корисним слугою, але небезпечним господарем» (C. L. Lange 1921) [5, с. 162].

Мета статті – розкрити зміст делегалізації корупційних доходів і протидії фінансуванню тероризму криміналістичними цифровими технологіями.

Аналіз останніх досліджень та публікацій. Дослідження проблеми протидії відмиванню корупційних доходів і фінансування тероризму криміналістичними цифровими технологіями присутнє у працях з теорії права, бухгалтерського обліку та аудиту, кримінально-правових наук – криміналістики, кримінології тощо, комп'ютерних систем та інформаційних технологій, тобто між- і трансдисциплінарного змісту. Брогі, М., Лагасіо, В. дослідили еволюцію неправомірної поведінки у фінтех; Гранді, С., Селлар, К., Джафрі, Дж. – глобальні фінансові системи; Занд, А., Орвеллі, Дж., Пфлюгель, Е. – безпечну структуру для боротьби з відмиванням грошей за допомогою машинного навчання та обміну секретами; Миненко С. – трансформацію системи протидії легалізації кримінальних доходів в умовах діджиталізації національної економіки; Павлідіс Г. – розгортання штучного інтелекту для боротьби з відмиванням грошей і повернення активів; Піт М., Аткінсон П., Горедема К., Бакарезе А., Ласіч Т. – відстеження викрадених активів; Сакс К., Клопец М., Хеммал Й., Кальюсте К. Е., Петерманн А. – використання Інтернету дітьми; Судеал Л. – делегалізацію у підходах до правової реформи; Сузан, Б. – публічні дані про злочини; Такеї Ю., Шудо К. – технічні проблеми і таксономію рішень у правилах переміщень віртуальних активів; Хуперс К., Зубен М., Гомес Х. – правила безпеки в Інтернеті; Чайка І. – кримінологічну характеристику та запобігання шахрайству в Україні; Ю Ю., Ву Дж., Лін Д., Фу К. – відмивання грошей на Ethereum; тощо. Водночас порушені у цій роботі питання виявились розкритими не повністю, що актуалізує її виконання.

Виклад основного матеріалу. Детерміновані національною культурою режими і стилі роботи, політична кон'юнктура історії транснаціональних й регіональних зв'язків, питання фінансової, комерційної і/або іншої глобальної політики впливають на перебіг та результат протидії відмиванню коштів, отриманих внаслідок вчинення злочинів. Наприклад, при зростанні рівня діджиталізації на 1% рівень розвитку регулювання ринку фінансових послуг зростає на 0,30%, а правоохоронної системи – на 0,93%. Наразі зміни системи протидії легалізації доходів в Україні не призвели до значного ефекту. Зростання кількості покарань й обсягів повернутих грошей до державного бюджету не спостерігалось. Час, який проходить від початку вчинення злочину з метою легалізації незаконних доходів до винесення судом обвинувального вироку часто триває роками [6, с. 159, 160, 162, 163]. Відстеження злочинних доходів передбачає ідентифікацію активів з їх злочинним походженням або від них через усі мутації, якщо такі є, до кінцевої форми та стану, в якому вони існують на момент їх знаходження. Під час мутації доходи змішуються з законно накопиченими ресурсами і можуть зменшуватися, зростати в кількості або збільшуватися в ціні. Інструментом для глобального збору інформації є дослідження корпоративної розвідки (Corporate Intelligence Research) [3, с. 23, 112].

Досудове слідство у цих справах бере до уваги приватні інтереси «корпоративних фінансів, фінансових ринків та посередників, … уряду», які воно зачіпає; виміри цих інтересів у «нерухомості, географії фінансових потоків, фінансових центрах та мережах,

фінансових технологіях (FinTech); їхній вплив на «фінансову рівність, її зв'язок із соціальною справедливістю, кризами, відповідальним інвестуванням» та інші макроекономічні показники, а також залучені до обслуговування цих інтересів «транснаціональні консалтингові і бухгалтерські фірми», рейтингові агенції, страхові компанії тощо [7, с. 15]. Наприклад, відмивання коштів через підприємців зі сфери фінтеху і/або їхня залученість до фінансування тероризму означитиме для правоохоронців (financial intelligence units) необхідність роботи з алгоритмами програм, великими даними, ШІ та машинним навчанням (Machine Learning), що відзначається неперевершеною інноваційністю [8, с. 57, 58]. Відповідно успіх виявлення цих правопорушень у розрахунках та інших комерційних операціях фінтеху вкрай складне завдання без залучення низки потрібних фахівців з інформаційних технологій (information technology) і т. п. Досягненню цілей досудового слідства може заважати будь-що з перерахованого ще більшою мірою, якщо до злочинних схем з відмивання коштів залучені публічні чиновники (persons with top executive functions), тобто організована злочинність є мафіозною (олігархічною), і/або якщо вони представляють фінансові центри країни, світу, зокрема в особі глобально передових інвестиційних компаній, системно важливих банків [9], і/або у них використані цифрові технології, ШІ. Відповідно на міжнародному рівні країни без світових фінансових центрів, з периферійною чи напівпериферійною фінансовою системою поступаються інтересам фінансових центрів, які об'єктивно містять у собі корупційні ризики глобального рівня, де правовий інтерес слабшого порушується неправовим інтересом сильнішого.

«Банківський і фінансовий сектор має довгу історію неправомірної та неетичної поведінки, а також скандали, які заплямували репутацію звичайних фінансових установ. Приклади включають маніпулювання ринком, інсайдерську торгівлю, зловживання фінансовими продуктами, відмивання грошей, скандал Libor (London Interbank Offered Rate) та іпотечну кризу. Це призвело до недовіри громадськості та посилення регуляторного контролю. Неправомірна поведінка на фінансовому ринку щороку зачіпає близько 15% компаній, що зареєстровані на біржі, що призводить до значних штрафів за маніпуляції цінами, обмінним курсом і відсотковими ставками, що може серйозно вплинути на організацію» [10]. Особливо це стосується випадків, коли залучені корупційні доходи політичних та економічних еліт, або якщо доходи переміщуються через кордон [3, с. 24]. Динаміка кримінальних проваджень про легалізацію (відмивання) майна, одержаного злочинним шляхом, фінансування тероризму, розповсюдження зброї масового знищення за останні 14 років в Україні проілюстрована на графіку (рис. 1) [11; 12].

Дані графіків доводять, що спеціалізація правоохоронного органу на економічних злочинах в особі Бюро економічної безпеки дозволила збільшити з 2022 р. кількість виявлених злочинів з легалізації одержаного внаслідок злочину доходу, фінансування тероризму, розповсюдження зброї масового знищення. Під час повномасштабної війни зовнішнього агресора проти України кількість таких справ зросла у десятки разів. Таке зростання частково пояснюється фактичними можливостями нейтралізації в умовах цієї війни корумпованих топ-чиновників (олігархів), які до її початку протидіяли виявленню і/або розслідуванню цих злочинів, приховували їх.

Кримінально-правові норми з протидії відмиванню злочинних коштів чутливі до точності й вичерпності юридичних формулювань. Найвлучніше і найбільш вичерпне формулювання таке: «злочинні активи» або «отримані внаслідок злочину активи». «Дивергентність фінансування тероризму з відмиванням грошей у тому, що відмивач грошей зосереджений насамперед на утриманні злочинних доходів і подальшому доступі до них, а фінансист терористів зосереджений на тому, щоб спря-

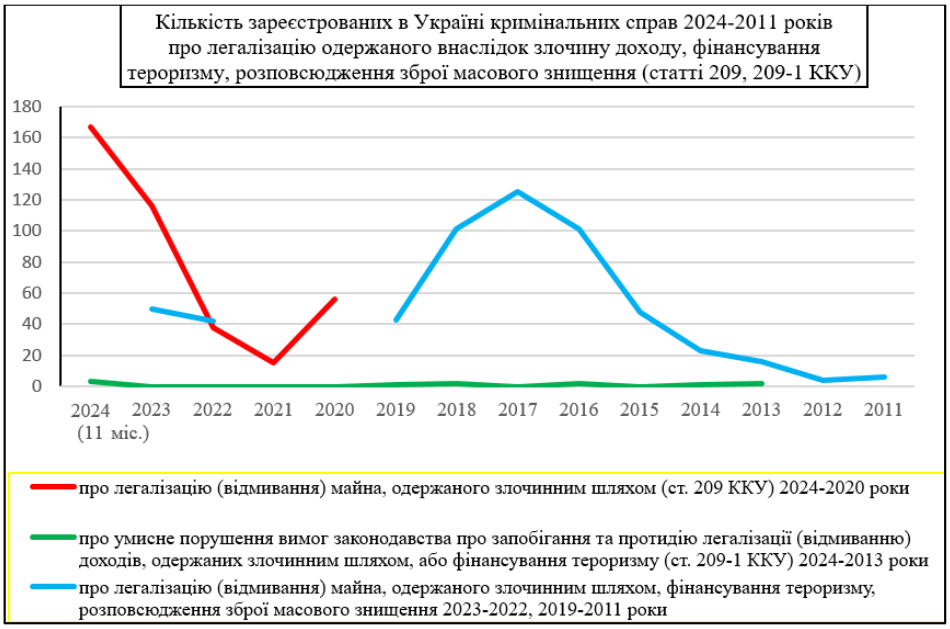

Рис. 1. Кількість зареєстрованих в Україні кримінальних справ 2024–2011 років про легалізацію одержаного внаслідок злочину доходу, фінансування тероризму, розповсюдження зброї масового знищення (статті 209, 209-1 ККУ)

мувати те, що спочатку може бути чистим, у руки тих, хто підтримує його чи її власні ідеологічні чи релігійні переконання у формі прямого фінансування насильницьких актів, навчальних заходів, пропаганді переконань, подорожах. Фінансисти терористів насамперед зацікавлені в безпосередньому використанні банківської системи та отриманні прибутку від швидкості переказу коштів» [3, с. 81]. Використанню віртуальних активів, також відомих як децентралізовані системи цифрових валют чи криптовалюти, як засобу легалізації злочинних доходів і/або фінансування тероризму, війн, протидіють Правила подорожей для переказів віртуальних активів від Групи розробки фінансових заходів боротьби з відмиванням грошей (the Financial Action Task Force), якими біржі та інших постачальників послуг віртуальних активів (virtual asset service provider) зобов'язано збирати інформацію про відправників і одержувачів цих активів, мати ліцензію, відповідати іншим юридичним вимогам [13, с. 784; 14].

Діяльність з відмивання грошей пов'язана з різними видами злочинів, і ефективне виявлення цієї діяльності значною мірою сприяє запобіганню та переслідуванню цих злочинів. Існує кілька категорій відмивання грошей, включаючи використання власності, азартні ігри та бізнес для приховування справжнього джерела коштів [17, с. 1]. Комп'ютерна криміналістика зазвичай використовує системний підхід до видобутку великих обсягів електронної інформації. Традиційні методи інтелектуального аналізу даних, такі як аналіз асоціацій, класифікація та прогнозування, кластерний аналіз і аналіз викидів, визначають шаблони в структурованих даних. Нові методи, такі як семантичний аналіз, ідентифікують шаблони як із структурованих, так і з неструктурованих даних. У семантичній мережі дані визначаються, зберігаються та зв'язуються таким чином, щоб забезпечити пошук і отримання інформації з більшою точністю, контекстне ранжування результатів пошуку та інтеграцію з іншими системами з підвищеною релевантністю [3, с. 79, 80].

Велика Британія, країни ЄС, Китай та інші високорозвинені країни широко використовують інформаційні технології для запобі-

гання злочинності, а саме: 1) картографування кримінологічно значимої інформації з метою візуалізації та аналізу моделей злочинів; 2) аналіз цифрових зображень у режимі онлайн, отриманих із відеокамер високої роздільної здатності; 3) використання хмарних технологій для збору, аналізу та зберігання оперативної інформації, що надходить із різних джерел, у т.ч. відеоматеріалів у режимі онлайн від громадськості щодо вчинених злочинів; 4) моніторинг інформації в соціальних мережах; 5) підвищення рівня правової обізнаності громади щодо суспільної безпеки та запобігання злочинності з використанням можливостей мережі Інтернет; 6) підвищення рівня комунікації громадськості з поліцією, зокрема розроблення програм для швидкого надання громадянами інтернет-повідомлень (E-Watch) щодо стану злочинності на вулицях, громадських місцях [16, с. 85–86].

Мережі, що складаються із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку, також дозволяють інтенсифікувати протидію відмиванню грошей і фінансуванню тероризму. Це системи оцінки, генерування і передачі даних (Інтернету речей / Internet of Things, IoT), наприклад, системи точок продажу (Point of sale, POS), банкомати та мобільні гаманці. Їхній потік даних сприяє швидшому реагуванню на підозрілу неправомірну активність, дозволяючи суб'єктам фінансового моніторингу і/або органам кримінальної юстиції своєчасно виявляти, блокувати, контролювати злочинні транзакції, припиняти легалізацію злочинних коштів, фінансування тероризму, війни, шпигунів тощо. Інтеграція «Інтернету речей» з кримінологічними та криміналістичними рішеннями протидії цим злочинам складає невід'ємну частину процедур відповідності (compliance) фінансів та управління організацій вимогам правових актів держав [8, с. 57; 18].

Роботі з даними (обробці, аналізу, пошуку, збереження, централізованого моніторингу та керування) відеокамер центрального, регіонального і місцевого рівнів, метаданими, архівами, повідомленнями про події та іншою суміжною інформацією в режимі реального часу в Україні присвячено програмно-апаратний комплекс «Безпечна країна», що наразі запроектовано як чергову функціональну підсистему Єдиної інформаційної системи МВС, відповідно до Положення «Про єдину інформаційну систему Міністерства внутрішніх справ», затв. пост. КМУ 14.11.2018 р. № 1024. Серед очікуваних результатів впровадження цього е-комплексу підвищення ефективності діяльності служб правопорядку усіх рівнів, запобігання шахрайству, зменшення загрози проведення терористичних актів тощо [19, с. 7].

Перспективним для багатьох країн стає використання успішного досвіду США з картографування (crime mapping) інформації про злочини, які пов'язані з нападами, крадіжками, незаконним використанням зброї, вандалізмом та ін. Інформація має відкритий характер та базується на даних, що надаються відповідними правоохоронними органами та надходять із засобів масової інформації. Будь-хто може отримати доступ до цих карт і мати змогу зареєструватися для отримання безплатних попереджень про злочини через електронну пошту та SMS-повідомлення. У сповіщенні електронною поштою, зокрема, містяться відомості про карту та злочини, які відбулися на певній визначеній території. У США до цього залучені приватні компанії, наприклад, SpotCrime.com [16, с. 87–88] (Towson, Maryland 21204, US). Це заснований у 2007 р. найбільший геолокатор даних про злочини в США, який агрегує і наносить дані з відділів поліції та перевірених новин про злочини на карти Google та інших програм (Application Programming Interface) і надсилає сповіщення через електронну пошту,

Facebook, Twitter, SMS, RSS та безліч інших платформ, з метою надати громадськості найточнішу та своєчасну геокодовану інформацію про злочини [20].

Інститут віртуальних поліцейських (естон. Veebipolitseinike) став вдалим інструментом використання Естонією кіберпростору для профілактики шахрайства, кіберзлочинності та інших злочинів, захисту дітей від образ у соціальних мережах, підтримки безпеки громадян і потерпілих, отримання інформації про підготовку і вчинення злочинів тощо. Віртуальні поліцейські, зокрема й «осередки у вигляді акаунтів та електронних адрес для комунікації з громадянами, перш за все з молоддю, на найчастіше відвідуваних і популярних серед молоді веб-порталах»: Facebook, Instagram, WhatsApp, Snapchat та ін. [16, с. 88]. Онлайн-поліція працює в Інтернеті, відповідаючи на повідомлення та листи, надіслані людьми в Інтернеті, і навчаючи дітей і дорослих про безпеку в Інтернеті. Мета онлайн-поліцейських – давати поради, вони самі не переслідують злочини [21; 22]. Онлайн-поліцейські підтвердили, що багато молодих людей також дуже наївні: вони схильні вірити в щирість намірів співрозмовника і не схильні підозрювати, що співрозмовник може бути зовсім не тим, за кого себе видає [15, с. 94].

Природа корупційного чи іншого злочину, від якого отримано дохід, а також злочинів з легалізації таких доходів, вимагає пристосування зазначених технологічних рішень таким чином, щоб злочинам можна було запобігти, швидко розкрити їх і притягти винних до відповідальності тощо. «Банки генерують криптографічний код для кожної транзакції. Ці коди спільно використовуються в реєстрі за допомогою відповідного дискретного протоколу для введення в процес виявлення підозрілої діяльності та підготовки звітів про це (suspicious activity reports). Деталі будь-якої транзакції, включеної до цих звітів, розкриваються лише уповноваженій стороні через необхідний криптографічний процес, таким чином зберігаючи конфіденційність. Запропонована система здатна виробляти для кожної транзакції оцінку ймовірності того, що вона пов'язана з діяльністю з відмивання грошей, водночас обмежуючи видимість цієї оцінки лише пов'язаними банками та деталі пов'язаної транзакції, як визначено параметри секретного протоколу обміну. Оцінка кожної транзакції може бути включена поряд з оцінками, отриманими з інших підходів, поза межами аналізу транзакцій, як частину загального процесу для точного та своєчасного виявлення діяльності з відмивання грошей» [17, с. 1]. Підходящим ресурсом стає технологія розподіленої цифрової книги у вигляді численних вузлів, які ретельно записують важливу інформацію про різні транзакції, включаючи хеші транзакцій, суми, позначки часу, залучених сторін та інші дані в мережі, таким чином досягаючи децентралізованого зберігання та механізмів перевірки (blockchain) [23, с. 1759]. Використання ШІ може допомогти виявити та запобігти відмиванню грошей шляхом аналізу величезних обсягів фінансових даних і швидкого й точного виявлення підозрілої діяльності [5, с. 162]. Великі обсяги даних про транзакції можливо обробити за допомогою програмного забезпечення криміналістичних технологій: Account Analyser, ACL, InfoZoom, IDEA та інші, що дозволяють виявляти шаблони і аномалії у даних транзакцій; перевіряти облікові дані шляхом виділення дебетових і кредитових записів у системі бухгалтерського обліку; враховувати те, як підозрілі на вигляд банківські операції були враховані в процесі бухгалтерського обліку, оскільки вони, наприклад, прикриваються фальшивими дебетовими проводками на рахунку витрат [3, с. 105–106]. Ефективність досліджуваній злочинності сприяє система керування справами (case management system), оскільки вона пришвидшує обмін даними у справі та доказовими документами у базі даних IT, документування процедур та іншою інформацією [3, с. 74, 76–77].

Висновки. Отже, делегітимізувати корупційні доходи і елімінувати фінансування тероризму дозволяють наступні криміналістичні технології цифрового формату. Первинною стала система керування справами у підрозділах фінансової розвідки органів кримінальної юстиції. Ці органи спираються на цифрові дані картографування злочинів, наприклад, за зразком успішного досвіду США, де для цього залучаються інформаційні ресурси ліцензованих приватних компаній. Для розслідування злочинних активів використовується концепція семантичної бази даних і семантичної мережі. Будучи ключовими серед суб'єктів фінансового моніторингу, банки та інші фінансові організації використовують електронні системи обробки інформації у блокчейні, що дозволяє ефективно оцінювати ймовірності відмивання грошей / фінансування тероризму серед транзакцій клієнтів. Потенціал для таких оцінок містять також системи Інтернету речей, оскільки аналіз їхніх даних формує знання про типові фінансові, купівельні і/або інші господарські моделі поведінки людей у режимі реального часу, полегшуючи виявлення делінкветних відхилень у них. Чіткі структури управління даних, надійні протоколи безпеки та масштабування інфраструктури цих систем в межах фінансових установ сприяє вирішенню питань комплайнсу фінансових транзакцій вимогам чинних законів у державі, управління і контролю над ними. Не менш важливим стає функціонал створеного за прикладом Естонії інституту віртуальних поліцейських, який може бути розширений на профілактику і нейтралізацію зазначених злочинів.

У глобальному контексті ефективність правоохоронних органів більшості країн залежить від залучення аудиторських, консалтингових, юридичних та інших компаній, які надають спеціалізовані експертні послуги про події, потоки платежів, бенефіціарів, посередників та іншу цінну підтримку через свою всесвітню мережу. Інформація з камер відеоспостереження у публічних місцях довели свою ефективність у покращенні кримінологічної обстановки у США, Китаї, Японії, країнах ЄС та низці інших високорозвинених країн, зокрема й у частині недопущення втягнення працівників органів кримінальної юстиції у сфері протидії корупції та іншим економічним злочинам. Дані відеокамер, як і результати роботи ШІ для допомоги суб'єктам фінансового моніторингу з протидією відмиванню злочинних коштів, порушують проблеми відповідальності, дискримінації, упередженості та інших правових вимог для усунення порушень конфіденційних даних (банківської, нотаріальної таємниці тощо), своєчасного і злагодженого обміну потрібною інформацією, справедливості ухвалених рішень, фактичних можливостей надання пояснень та нагляду у юрисдикційних процесах. У цьому контексті важливо, щоб гарантії банківської таємниці дозволяли зберігати чесне підприємництво, його конкурентоспроможність. Безпека обігу віртуальних валют та інших операцій у кіберпросторі дозволяє користуватись його ресурсами, а не протидіяти їм, як наслідку взаємопосилення злочинів – корупції, яка передує відмиванню злочинних коштів; відмиванню цих коштів, фінансування тероризму і/або агресивних війн; використання ШІ зі злочинними намірами та інших комп'ютерних злочинів. Питання комплайнсу використання даних з юридичними вимогами потребують унормування.

Інтеграція інструментів цифрової криміналістики у єдиний механізм протидії легалізації корупційних доходів і фінансуванню тероризму формально юридично відображається у відповідній стратегії, яка має містити розділи про напрями впровадження і види цифрових технологій, що використовуються для такої протидії. В Україні цю стратегію доцільно об'єктивувати у вигляді подальшого розвитку програмно-апаратного комплексу «Безпечна країна». Дані графіків зазначених злочинів в Україні ілюструють висхідний тренд їх розслідування. Актуальним

є цифрові системи, спроможні забезпечити ефективність таких розслідувань, зокрема й в частині використання для вчинення злочину віртуальних активів у кіберпросторі. Парламент має визначити поняття «кіберпростір», інакше відсутні кордони поширення державного суверенітету на злочинну діяльність у кібернетичному середовищі, відносно криптовалют тощо. В межах юрисдикцій різних держав таке використання формалізується у вигляді цифрової галузі міжнародного публічного кримінального права, що стосується умов транснаціональних розслідувань економічних злочинів, корупції, фінансування тероризму, де бере участь безліч осіб і різні складні фінансові механізми.

Анотація

У статті досліджено делегалізацію корупційних доходів і фінансування тероризму криміналістичними цифровими технологіями. Встановлено, що первинне значення має система керування справами у підрозділах фінансової розвідки органів кримінальної юстиції. Воно спираються на цифрові дані, зокрема з картографування злочинів, де для цього залучаються інформаційні ресурси ліцензованих приватних компаній. Для розслідування злочинних активів використовується концепція семантичної бази даних і семантичної мережі. Будучи ключовими серед суб'єктів фінансового моніторингу, банки та інші фінансові організації використовують електронні системи обробки інформації у блокчейні, що дозволяє ефективно оцінювати ймовірності відмивання грошей / фінансування тероризму серед транзакцій клієнтів. Потенціал для таких оцінок містять також системи Інтернету речей, оскільки аналіз їхніх даних формує знання про типові фінансові, купівельні і/або інші господарські моделі поведінки людей у режимі реального часу, полегшуючи виявлення делінкветних відхилень у них. Чіткі структури управління даних, надійні протоколи безпеки та масштабування інфраструктури цих систем в межах фінансових установ сприяє вирішенню питань комплайнсу фінансових транзакцій вимогам чинних законів у державі, управління і контролю над ними. Не менш важливим стає функціонал створеного за прикладом Естонії інституту віртуальних поліцейських, який може бути розширений на профілактику і нейтралізацію зазначених злочинів.

Підсумовано, що інтеграція інструментів цифрової криміналістики у єдиний механізм протидії легалізації корупційних доходів і фінансуванню тероризму формально юридично відображається у відповідній стратегії, яка має містити розділи про напрями впровадження і види цифрових технологій, що використовуються для такої протидії. В межах юрисдикцій різних держав таке використання формалізується у вигляді цифрової галузі міжнародного публічного кримінального права, що стосується умов транснаціональних розслідувань економічних злочинів, корупції, фінансування тероризму, де бере участь безліч осіб і різні складні фінансові механізми.

Ключові слова: бухгалтерський облік, відмивання доходів, інтернет речей, картографування, кіберпростір, тероризм, транзакція, ФАТФ, фінтех.

Makarenkov O.L. Delegalization of corruption proceeds and terrorist financing using forensic digital technologies

Summary

The article reveals the countering of corrupt proceeds and the financing of terrorism using forensic digital technologies. It is established that the case management system within the financial intelligence units of criminal justice bodies plays a primary role. This system relies on digital data, particularly crime mapping, following the successful example of the United States, where licensed private companies' information resources are employed for such purposes. The investigation of criminal assets

uses the concept of a semantic database and semantic network. As key actors in financial monitoring, banks and other financial organizations utilize electronic information processing systems based on blockchain technology, which enables effective assessment of the likelihood of money laundering or terrorism financing among client transactions. The potential for such assessments is also found in Internet of Things (IoT) systems, as their data analysis generates knowledge about typical financial, purchasing, and other business behavior patterns in real time, facilitating the detection of delinquent deviations. Clear data management structures, robust security protocols, and scalable infrastructure within financial institutions address compliance issues for financial transactions under current laws, ensuring governance and oversight. The functionality of a virtual police institution, modeled after Estonia's example, could be expanded to prevent and neutralize these crimes.

It has been determined that in the global context, the efficiency of law enforcement in most countries depends on involving auditing, consulting, legal, and other companies that provide specialized expert services. These services include information on events, payment flows, beneficiaries, intermediaries, and other valuable support through their global networks. Data from law enforcement body cameras and public surveillance cameras have proven effective in improving the criminological situation. However, it is crucial to ensure that banking secrecy guarantees uphold honest entrepreneurship and its competitiveness.

In conclusion, integrating digital forensic tools into a unified mechanism to counteract the legalization of corrupt proceeds and terrorism financing is formally and legally reflected in a corresponding strategy. This strategy should include sections outlining the areas of implementation and types of digital technologies used for such counteraction. The concept of "cyberspace" must be defined by law, as its absence creates gaps in extending state sovereignty to criminal activities in the cyber environment, including cryptocurrencies. Across different jurisdictions, such integration is formalized as a digital branch of international public criminal law, which addresses the conditions for transnational investigations of economic crimes and terrorism financing involving multiple actors, complex financial mechanisms.

Key words: accounting, money laundering, Internet of Things, mapping, cyberspace, terrorism, transaction, FATF, fintech.

Список використаних джерел:

1. Makarenkov, O., Kosa, V. Forensic technique for identifying corruption challenges to national security through digital technologies. BJES. 2024. Vol. 10. No. 4. P. 288–300. doi.org/10.30525/2256-0742/2024-10-4-288-300
2. Sudeall, L. Delegalization. Stanford Law Review. 2023. Vol. 75. P. 116–131.
3. Pieth, M., Atkinson, P., Goredema, C., Bacarese, A., Lasich, T., others. Tracing Stolen Assets: A Practitioner's Handbook. Basel: Basel Institute on Governance. 2009. 124 p.
4. DarkMarket: world's largest illegal dark web marketplace taken down. Europol's European Cybercrime Centre. 12.01.2021. URL: https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down
5. 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. 2023. P. 155–166. doi10.1108/JMLC-03-2023-0050
6. Миненко С. В. Трансформація системи протидії легалізації кримінальних доходів в умовах діджиталізації національної економіки. Дис. к.е.н. спец. 051 – економіка. Сумський ДУ. Суми. 2022. 204 с.

7. Grandi, S., Sellar, C., Jafri, J. Geofinance between Political and Financial Geographies. A Focus on the Semi-Periphery of the Global Financial System. Cheltenham: E. Elgar Publishing LLC. 2019. 264 p.
8. Opportunities and Challenges of New Technologies for AML/CFT. Paris: FATF. 2021. 76 p.
9. EBA updates list of other systemically important institutions. 11.07.2024. URL: https://www.eba.europa.eu/publications-and-media/press-releases/eba-updates-list-other-systemically-important-institutions-3
10. Brogi, M., Lagasio, V. New but naughty. The evolution of misconduct in FinTech. International Review of Financial Analysis. 2024. Vol. 95. P. B. P. 1–11. doi.org/10.1016/j.irfa.2024.103489
11. Статистика органів прокуратури України 2011–2019, 2022–2023. 31.12.2024. URL: https://gp.gov.ua/ua/posts/statistika
12. Єдині звіти про кримінальні правопорушення прокуратури України 2013–2024. 31.12.2024. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezulta-ti-yih-dosudovogo-rozsliduvannya-2
13. Takei, Y., Shudo, K. FATF Travel Rule's Technical Challenges and Solution Taxonomy. IEEE Inter. Conf. on Blockchain and Cryptocurrency. 27–31 May, 2024. C. 784–799. doi: 10.1109/ICBC59979.2024.10634360
14. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris: FATF. 2012–2023. 148 p.
15. Saks, K., Klopets, M., Hämmal, J., Kaljuste, K. E., Petermann, A. and others. Laste internetikasutus ning võimalused internetis toimuva laste seksuaalse väärkohtlemise ennetamiseks. Uuringu aruanne. Tallinn: Kantar Emor 2024. 138 p.
16. Чайка І. М. Кримінологічна характеристика та запобігання шахрайству в Україні. Дис. доктора філософії. спец. 081 – право. Донецький ДУВС. Кропивницький. 2023. 296 с.
17. Zand, A., Orwelly, J., Pfluegel, E. A Secure Framework for Anti-Money-Laundering using Machine Learning and Secret Sharing. Inter. Conf. on Cyber Security and Protection of Digital Services. 15-19 June, 2020. Dublin. C. 1–7. doi.org/10.1109/CyberSecurity49315.2020.9138889
18. Anti-Money Laundering: How IoT Can Help. AML. December 2, 2024. URL: https://www.iotforall.com/anti-money-laundering-iot
19. Концепція створення та впровадження програмно-апаратного комплексу «Безпечна країна». Київ: МВС України. 2021. 7 с.
20. Suszan, B. Public crime data becomes more open and transparent city by city. May 21, 2014. URL: https://opensource.com/government/14/5/spotcrime
21. Hoepers, C., Zuben, M., Gomez, H. Internetis võib olla väga lõbus, aga ära mängi oma turvalisusega. Tallinn: Profimeedia OÜ. 2024. 60 p.
22. Veebipolitsei tuleb appi.12.02.2020. URL: https://www.teeviit.ee/veebikonstaabel-tuleb-appi/
23. Yu, Y., Wu, J., Lin, D., Fu, Q. Money Laundering Detection on Ethereum: Applying Traditional Approaches to New Scene. IEEE 29th Inter. Conf. on Parallel and Distributed Systems. Ocean Flower Island, China. 2023. P. 1759–1766. doi.org/10.1109/ICPADS60453.2023.00244