Правова протидія використанню криптовалют як засобу фінансування терористичної діяльності

Лук'янюк Юлія Вікторівна

Опубліковано	Секція	УДК
28.02.2025	Право	343.326:336.74:004

DOI: https://doi.org/10.5281/zenodo.17657019

Анотація. Сучасні виклики міжнародної безпеки характеризуються трансформацією механізмів фінансування терористичних організацій, що активно адаптуються до технологічних інновацій. Криптовалюти, забезпечуючи анонімність транзакцій та децентралізовану структуру операцій, створюють принципово нові можливості для обходу традиційних систем фінансового моніторингу та контролю. Це дослідження аналізує сучасний стан правового регулювання цифрових валют у контексті протидії терористичному фінансуванню.

Методологічна основа дослідження включає компаративний аналіз національних законодавчих систем, вивчення міжнародних стандартів протидії відмиванню грошей та фінансуванню тероризму, а також аналіз судової практики у справах, пов'язаних із використанням криптовалюту у злочинних цілях. Особливу увагу приділяють вивченню технічних характеристик блокчейн-технологій, що визначають специфіку правового регулювання цифрових активів в антитерористичному законодавстві.

Дослідження виявляє суттєві прогалини у чинному правовому регулюванні, зумовлені динамічним розвитком криптовалютних технологій та недосконалістю механізмів міжнародного співробітництва у цій сфері. Аналізуються основні напрями вдосконалення нормативно-правової бази, включаючи розробку спеціалізованих процедур ідентифікації підозрілих транзакцій у децентралізованих мережах та створення ефективних механізмів міжвідомчої взаємодії.

Практична значимість роботи полягає у формулюванні конкретних пропозицій щодо модернізації антитерористичного законодавства з урахуванням особливостей функціонування криптовалютних систем. Пропонуються механізми гармонізації національних підходів до регулювання цифрових валют, що забезпечують баланс між потребами правоохоронних органів у ефективному контролі та збереженням інноваційного потенціалу фінансових технологій.

Результати дослідження демонструють необхідність комплексного підходу до правової протидії використанню криптовалют з терористичною метою, що передбачає інтеграцію технологічних рішень моніторингу блокчейн-мереж з традиційними методами фінансових розслідувань. Обґрунтовується важливість розвитку спеціалізованих компетенцій правоохоронних органів та створення міжнародних платформ обміну інформацією про підозрілі криптовалютні операції.

Висновки дослідження наголошують на критичній важливості своєчасної адаптації правових механізмів до викликів цифрової економіки, при цьому забезпечуючи дотримання фундаментальних принципів правової держави та захисту прав людини. Запропоновані рекомендації можуть бути основою для розробки ефективної стратегії

протидії терористичному фінансуванню в умовах глобальної цифровізації фінансових відносин.

Ключові слова: криптовалюти, терористичне фінансування, правове регулювання, блокчейн-технології, фінансовий моніторинг, міжнародна безпека, антитерористичне законодавство, цифрові активи, децентралізовані системи, фінансові розслідування, протидія відмиванню грошей, кібербезпека, правоохоронні органи, міжнародна співпраця.

Legal countermeasures against the use of cryptocurrencies as a means of financing terrorist activities

Annotation. Contemporary challenges to international security are characterised by the transformation of mechanisms for financing terrorist organisations, which are actively adapting to technological innovations. Cryptocurrencies, providing anonymity of transactions and a decentralised structure of operations, create fundamentally new opportunities to circumvent traditional financial monitoring and control systems. This study analyses the current state of legal regulation of digital currencies in the context of countering terrorist financing.

The methodological basis of the study includes a comparative analysis of national legislative systems, a study of international standards for combating money laundering and terrorist financing, as well as an analysis of judicial practice in cases related to the use of cryptocurrencies for criminal purposes. Particular attention is paid to the study of the technical characteristics of blockchain technologies that determine the specifics of the legal regulation of digital assets in anti-terrorism legislation.

The study reveals significant gaps in the current legal regulation, caused by the dynamic development of cryptocurrency technologies and the imperfection of mechanisms for international cooperation in this area. The main directions for improving the regulatory framework are analysed, including the development of specialised procedures for identifying suspicious transactions in decentralised networks and the creation of effective mechanisms for interagency cooperation.

The practical significance of the work lies in the formulation of specific proposals for modernising anti-terrorism legislation, taking into account the peculiarities of cryptocurrency systems. Mechanisms are proposed for harmonising national approaches to the regulation of digital currencies, ensuring a balance between the needs of law enforcement agencies for effective control and the preservation of the innovative potential of financial technologies.

The results of the study demonstrate the need for a comprehensive approach to legal counteraction to the use of cryptocurrencies for terrorist purposes, which involves the integration of technological solutions for monitoring blockchain networks with traditional methods of financial investigation. The importance of developing specialised competencies of law enforcement agencies and creating international platforms for exchanging information about suspicious cryptocurrency transactions is justified.

The study's conclusions emphasise the critical importance of timely adaptation of legal mechanisms to the challenges of the digital economy, while ensuring compliance with the fundamental principles of the rule of law and the protection of human rights. The proposed recommendations can serve as a basis for developing an effective strategy to counter terrorist financing in the context of the global digitalisation of financial relations.

Keywords: cryptocurrencies, terrorist financing, legal regulation, blockchain technologies, financial monitoring, international security, anti-terrorism legislation, digital assets, decentralised systems, financial investigations, anti-money laundering, cybersecurity, law enforcement agencies, international cooperation.

Вступ

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасні геополітичні процеси та ескалація міжнародного тероризму зумовлюють трансформацію механізмів фінансового забезпечення екстремістських організацій, які активно впроваджують інноваційні технології для обходу традиційних систем контролю. Криптовалютні системи, що характеризуються децентралізованою архітектурою, псевдонімністю учасників і транскордонним характером операцій, створюють нові можливості для прихованого переміщення фінансових ресурсів терористичними угрупованнями. Ця проблематика набуває особливої гостроти в умовах стрімкого зростання капіталізації криптовалютного ринку та розширення сфери застосування цифрових активів у глобальній економіці.

Технологічні особливості блокчейн-платформ забезпечують високий рівень анонімності транзакцій та ускладнюють застосування традиційних методів фінансового моніторингу, розроблених для централізованих банківських систем. Відсутність одноманітних міжнародних стандартів правового регулювання криптовалютних операцій створює правові лакуни, які експлуатуються терористичними організаціями для створення альтернативних каналів фінансування. Існуючі механізми протидії відмиванню грошей та фінансуванню тероризму виявляються недостатньо ефективними в умовах застосування децентралізованих фінансових інструментів, що потребує кардинального перегляду підходів до правового регулювання цієї сфери.

Практична значущість дослідження обумовлена необхідністю розробки ефективних правових механізмів протидії використанню криптовалюту в терористичних цілях при збереженні інноваційного потенціалу фінансових технологій. Міжнародна практика демонструє випадки використання цифрових валют для фінансування терористичних актів, що підтверджує реальність загроз національній безпеці держав. Відсутність адекватного правового регулювання може призвести до подальшого розширення використання криптовалютних інструментів деструктивними силами та підриву ефективності міжнародних систем фінансової безпеки.

Наукова актуальність теми визначається недостатньою розробленістю теоретичних засад правової протидії криптовалютному фінансуванню тероризму та необхідністю формування концептуальних підходів до гармонізації національних законодавств у цій сфері. Динамічний розвиток технологій розподілених реєстрів випереджає темпи адаптації правових систем, що створює дисбаланс між технічними можливостями зловмисників та правоохоронним потенціалом державних органів. Дослідження цієї проблематики сприяє формуванню науково обґрунтованих рекомендацій щодо вдосконалення антитерористичного законодавства та розвитку міжнародного співробітництва у сфері протидії цифровому фінансуванню екстремістської діяльності.

Аналіз останніх досліджень і публікацій.Сучасна наукова література демонструє зростання інтересу до проблематики правового регулювання криптовалютних технологій у контексті протидії терористичному фінансуванню. Фундаментальні дослідження *(Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023))* [1] розкривають механізми використання децентралізованих фінансових інструментів терористичними організаціями, наголошуючи на необхідності модернізації міжнародних стандартів фінансового моніторингу. Роботи *(Ментух, Н.Ф, Шевчук О. Р. (2019))* [2] та *(Givens, A.D. (2025))* [3] акцентують увагу на технічних аспектах анонімізації транзакцій у блокчейн-мережах та їх вплив на ефективність правоохоронної діяльності.

Європейські дослідники *(Badawi, E., Jourdan, G.-V., & Onut, I.-V. (2023))* [4] проводять компаративний аналіз національних підходів до регулювання цифрових активів, виявляючи суттєві відмінності у правозастосовній практиці країн Європейського Союзу.

На особливу увагу заслуговують роботи В.І. *(Maurushat, A., & Halpin, D. (2022))* [5] та *(Mirkamol, S., & Mansur, E. (2023))* [6], які досліджують особливості імплементації міжнародних стандартів протидії відмиванню грошей до національного законодавства з урахуванням специфіки криптовалютних операцій.

Американські дослідники *(Oladipupo, A. O., & Oladeji, T. N. (2025))* [7] представляють комплексний аналіз судової практики у справах, пов'язаних з використанням криптовалюту в терористичних цілях, демонструючи еволюцію правозастосовних підходів федеральних судів США. Роботи учених *(Волинець В.В.(2025))* [8] та *(Phillips, R., & Wilder, H. (2020))* [9], розкривають специфіку регулювання цифрових активів у юрисдикціях з розвиненою криптовалютною екосистемою та аналізують ефективність превентивних заходів протидії терористичному фінансуванню.

Міжнародні організації активно розробляють рекомендації щодо вдосконалення правового регулювання криптовалютних технологій. Доповіді FATF (2023-2024) [10, 11] містять оновлені стандарти щодо протидії відмиванню грошей та фінансуванню тероризму стосовно віртуальних активів. Дослідження ООН (2024) [12] та Ради Європи (2023) [13] наголошують на необхідності гармонізації національних підходів до регулювання цифрових валют та розвитку міжнародного співробітництва в даній сфері.

Разом з тим аналіз існуючих публікацій виявляє недостатню розробленість теоретичних основ інтеграції традиційних правових механізмів протидії тероризму з інноваційними підходами до регулювання децентралізованих фінансових систем. Відсутність комплексних досліджень, що поєднують технічні, правові та кримінологічні аспекти проблеми, зумовлює актуальність цього дослідження та визначає його наукову новизну.

Метою дослідження є комплексний аналіз правових механізмів протидії використанню криптовалют як інструменту фінансування терористичної діяльності.

Результати

Міжнародна правова система протидії терористичному фінансуванню базується на фундаментальних принципах, закріплених у Міжнародній конвенції про боротьбу з фінансуванням тероризму 1999 року [14] та резолюціях Ради Безпеки ООН 1267 (1999) [15] та 1373 (2001) Дані документи встановлюють зобов'язання держав щодо криміналізації актів фінансування тероризму та створення ефективних механізмів фінансового моніторингу, проте їх положення розроблялися в епоху домінування традиційних банківських систем та не враховують специфіки криптовалютних технологій.

Розвиток цифрових фінансових інструментів вимагає перегляду підходів до правового регулювання терористичного фінансування. Рекомендації FATF щодо віртуальних активів (2019, оновлені у 2023) [17] вперше встановили міжнародні стандарти регулювання криптовалютних операцій у контексті протидії відмиванню грошей та фінансуванню тероризму. Документ вводить поняття "постачальників послуг віртуальних активів" (VASP) та встановлює вимоги щодо їх ліцензування, моніторингу операцій та міжнародного співробітництва.

Європейський підхід до регулювання криптовалют характеризується комплексністю та системністю. Регламент ЄС про ринки криптоактивів (MiCA) 2023 року [18] створює однакову правову рамку для всіх держав-членів, встановлюючи суворі вимоги до емітентів криптоактивів та постачальників криптопослуг. Директива ЄС (EU) 2018/843 [19] розширила сферу застосування законодавства про запобігання відмиванню коштів на криптовалютні біржі та гаманці, зобов'язавши їх дотримуватись процедур належної перевірки клієнтів та повідомляти про підозрілі транзакції.

Американська модель регулювання ґрунтується на застосуванні існуючих фінансових законів до криптовалютних операцій. Закон про банківську таємницю (Bank

Secrecy Act) [20] в інтерпретації Міністерства фінансів США поширюється на операції з віртуальними валютами, вимагаючи від учасників ринку дотримання антивідмивних процедур. Патріотичний акт США *(USA PATRIOT Act)* [21] надає правоохоронним органам розширені повноваження щодо моніторингу фінансових операцій, включаючи криптовалютні транзакції.

Децентралізована архітектура блокчейн-мереж створює принципові виклики для традиційних механізмів фінансового контролю. На відміну від централізованих платіжних систем, де транзакції проходять через контрольовані посередники, криптовалютні мережі дозволяють здійснювати прямі peer-to-peer перекази без участі фінансових інститутів [22]. Ця особливість ускладнює застосування стандартних процедур моніторингу, заснованих на звітності банків та небанківських фінансових організацій.

Псевдонімність криптовалютних адрес є додатковим викликом для ідентифікації учасників підозрілих транзакцій. Хоча більшість публічних блокчейнів забезпечують прозорість усіх операцій, зв'язок між криптовалютними адресами та реальними особистостями часто залишається невстановленим [23]. Терористичні організації активно використовують цю особливість, створюючи численні адреси та застосовуючи техніки обфускації для приховування слідів фінансування.

Розвиток технологій конфіденційності, таких як міксери (тумблери) та криптовалюти з підвищеною анонімністю *(privacy coins),* ще більше ускладнює завдання правоохоронних органів. Дослідження показують, що терористичні групи все частіше використовують подібні інструменти для розмивання ланцюжків транзакцій та утруднення їхнього відстеження [24]. Правові системи поки що не виробили ефективних механізмів протидії використанню таких технологій у злочинних цілях.

Транскордонний характер криптовалютних операцій створює додаткові юрисдикційні проблеми. Транзакції в блокчейн-мережах можуть здійснюватися між учасниками, що перебувають у різних державах, без участі традиційних фінансових посередників, що ускладнює застосування національних законів та міжнародних угод про правову допомогу [25]. Відсутність одноманітних міжнародних стандартів регулювання створює можливості регуляторного арбітражу з боку терористичних організацій.

Сінгапурський підхід до регулювання криптовалюту характеризується збалансованістю інтересів фінансової безпеки та технологічних інновацій. Закон про платіжні послуги *(Payment Services Act)* 2019 року [26] встановлює ліцензійні вимоги для постачальників криптовалютних послуг та зобов'язує їх дотримуватися антивідмивних процедур. Валютне управління Сінгапуру (MAS) розробило детальні посібники з ідентифікації підозрілих криптовалютних транзакцій, які стали взірцем для інших юрисдикцій.

Японська модель регулювання ґрунтується на інтеграції криптовалютних бірж до існуючої системи фінансового нагляду. Закон про платіжні послуги Японії (у редакції 2020 року) [27] класифікує криптовалюти як "криптоактиви" і встановлює суворі вимоги до їх зберігання, торгівлі та звітності. Японське агентство фінансових послуг (FSA) регулярно проводить інспекції криптовалютних бірж та вимагає надання детальної інформації про клієнтів та транзакції.

Швейцарська правова система демонструє прагматичний підхід регулювання цифрових активів. Федеральний закон про адаптацію федерального права до розвитку технології розподіленого реєстру *(DLT Act)* 2021 [28] створює спеціальну правову категорію для токенізованих активів і встановлює чіткі правила їх регулювання. Швейцарське управління з нагляду за фінансовими ринками (FINMA) розробило функціональний підхід до класифікації токенів, що визначає застосовні регуляторні вимоги.

Канадський досвід характеризується активним використанням існуючих законів про цінні папери регулювання криптовалютних операцій. Канадські адміністратори цінних паперів (CSA) розглядають багато криптоактивів як цінних паперів, що підлягають реєстрації та дотримання відповідних вимог [29]. Центр аналізу фінансових операцій та звітності Канади (FINTRAC) зобов'язує постачальників криптовалютних послуг реєструватися та виконувати антивідмивальні зобов'язання.

Механізми виявлення та припинення криптовалютного фінансування тероризму

Сучасні системи моніторингу блокчейн-транзакцій ґрунтуються на методах аналізу графів та машинного навчання для виявлення підозрілих патернів активності. Спеціалізовані аналітичні платформи, такі як Chainalysis, Elliptic та CipherTrace, розробляють алгоритми кластеризації адрес та деанонімізації учасників криптовалютних мереж [30]. Дані інструменти дозволяють правоохоронним органам відстежувати рух коштів від відомих терористичних адрес та виявляти пов'язані з ними гаманці.

Техніки кореляційного аналізу транзакцій дозволяють виявляти приховані зв'язки між різними криптовалютними адресами на основі тимчасових патернів, сум переказів та поведінкових характеристик [31]. Дослідження показують, що навіть за використання технік обфускації терористичні організації залишають цифрові сліди, які можна виявити з допомогою сучасних аналітичних методів. Розвиток штучного інтелекту та методів глибокого навчання відкриває нові можливості для автоматизованого виявлення аномальних транзакцій.

Міжнародне співробітництво у сфері моніторингу криптовалютних операцій потребує створення спеціалізованих механізмів обміну інформацією між правоохоронними органами різних держав. Європол та Інтерпол розробляють бази даних відомих криптовалютних адрес, пов'язаних з терористичною діяльністю, та забезпечують їх доступність для національних правоохоронних органів [32]. Створення глобальної системи моніторингу криптовалютних транзакцій потребує гармонізації технічних стандартів та правових процедур обміну інформацією. (Таблиця 1)

Таблиця 1 Механізми виявлення та припинення криптовалютного фінансування тероризму

Категорія	Методи та технології	Застосування та ефективність	Обмеження та виклики
Аналіз графів транзакцій	- Побудова directed acyclic graphs (DAG) для візуалізації потоків коштів.	- Дозволяє відстежити ланцюжки транзакцій від відомих терористичних адрес.	- Низька ефективність при використанні міксерів та privacy-коінів (Monero, Zcash).
Машинне навчання (ML)	- Виявлення кластерів адрес із загальними властивостями (taint analysis).	- Використовується у платформах Chainalysis, Elliptic для деанонімізації.	- Висока обчислювальна складність великих графів.
Кореляційний аналіз	- Застосування алгоритмів PageRank визначення ключових вузлів.	- Автоматизація виявлення підозрілих активностей (наприклад, peeling chains).	- Необхідність постійного оновлення навчальних даних.
Міжнародне співробітництво	- навчання моделей на розмічених даних	- Класифікація гаманців за поведінковими	- Ризик хибнопозитивних спрацьовувань через

	(аномальні vs легітимні транзакції).	ознаками (Elliptic Dataset).	складність інтерпретації ML-моделей.
Регуляторні заходи	- використання методів NLP для аналізу метаданих (мемпули, коментарі).	- Виявлення прихованих зв'язків між адресами (наприклад, через загальні посередники).	- Обмеженість під час роботи з cross-chain перекладами.

Джерело. Складено автором за матеріалами: https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Превентивні заходи протидії криптовалютному фінансуванню тероризму включають вимоги щодо верифікації особи користувачів (KYC) та моніторинг транзакцій постачальниками криптовалютних послуг. Імплементація "правила подорожей" (Travel Rule) для криптовалютних переказів зобов'язує постачальників послуг передавати інформацію про відправника та одержувача під час транзакцій, що перевищують встановлені пороги [33]. Розвиток технологій програмованих грошей та смарт-контрактів відкриває можливості для автоматизованого дотримання регуляторних вимог на рівні протоколу блокчейну.

Висновки

Проведене дослідження дозволило встановити, що сучасна система суб'єктів інформаційної безпеки в правоохоронній сфері України характеризується складною багаторівневою структурою, яка включає спеціалізовані підрозділи Національної поліції, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, а також інші правоохоронні органи. Аналіз нормативно-правової бази засвідчив наявність розгалуженої системи законодавчих та підзаконних актів, що регламентують діяльність зазначених суб'єктів, проте виявив значні прогалини у визначенні чітких меж їхньої компетенції. Встановлено, що правовий статус окремих суб'єктів інформаційної безпеки потребує уточнення з огляду на динамічний розвиток інформаційних технологій та появу нових видів кіберзагроз.

Дослідження функціональних повноважень суб'єктів інформаційної безпеки у правоохоронній сфері виявило проблему дублювання компетенцій та недостатньої координації діяльності між різними відомствами. Встановлено, що відсутність єдиної методології розподілу повноважень призводить до неефективного використання ресурсів та зниження результативності протидії інформаційним загрозам. Особливо гострою є проблема розмежування повноважень у сфері розслідування кіберзлочинів, захисту критичної інформаційної інфраструктури та забезпечення кібербезпеки державних інформаційних систем. Аналіз практики застосування чинного законодавства засвідчив необхідність створення більш чіткої системи правового регулювання взаємодії між різними суб'єктами інформаційної безпеки.

Компаративний аналіз вітчизняного та зарубіжного досвіду організації діяльності суб'єктів інформаційної безпеки в правоохоронній сфері показав, що європейські країни демонструють більш високий рівень інституційної спроможності та координації у цій сфері. Встановлено, що адаптація українського законодавства до стандартів Європейського Союзу вимагає суттєвого перегляду існуючих підходів до розподілу повноважень та створення ефективних механізмів міжвідомчої взаємодії. Особливу увагу слід приділити імплементації принципів пропорційності, субсидіарності та взаємного визнання у сфері забезпечення інформаційної безпеки, що сприятиме підвищенню ефективності правоохоронної діяльності та зміцненню довіри громадян до державних інституцій.

На основі проведеного аналізу сформульовано комплекс рекомендацій щодо вдосконалення правового регулювання діяльності суб'єктів інформаційної безпеки у правоохоронній сфері України. Запропоновано прийняття уніфікованого нормативно-правового акта, який би чітко визначив компетенцію кожного суб'єкта інформаційної безпеки та встановив ефективні механізми координації їхньої діяльності. Обґрунтовано необхідність створення спеціалізованого міжвідомчого органу координації у сфері інформаційної безпеки, який би забезпечував стратегічне планування, моніторинг загроз та координацію оперативного реагування. Практична реалізація запропонованих рекомендацій сприятиме підвищенню ефективності системи забезпечення інформаційної безпеки України та зміцненню її національної безпеки в цілому.

Список використаних джерел:

1. Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. Social & Legal Studios, 6(4), 123-131. doi: 10.32518/sals4.2023.123.

2. Ментух, Наталія Фелікіссімівна, and Оксана Романівна Шевчук. Гармонізація законодавства України про фінансові послуги з правом європейського союзу в рамках угоди про асоціацію між Україною та ЄС. *Актуальні проблеми правознавства*, no. 1, Apr. 2017, pp. 68-72, https://appj.wunu.edu.ua/index.php/appj/article/view/14.

3. Givens, A.D. Cryptocurrencies as a Threat to U.S. Homeland Security Interests. *Laws* **2025**, *14*, 2. https://doi.org/10.3390/laws14010002

4. Badawi, E., Jourdan, G.-V., & Onut, I.-V. (2023). The "Bitcoin Generator" scam. *Blockchain: Research and Applications*, 3(1), article number 100084. doi: 10.1016/j.bcra.2022.100084.

5. Maurushat, A., & Halpin, D. (2022). Investigation of cryptocurrency enabled and dependent crimes. In D. Goldbarsht & L. de Koker (Eds.), *Financial Technology and the Law: Combating Financial Crime* (pp. 235-267). doi: 10.1007/978-3-030- 88036-1_10.

6. Mirkamol, S., & Mansur, E. (2023). Cryptocurrencies as the money of the future. In Y. Koucheryavy & A. Aziz (Eds.), *Internet of things, smart spaces, and next generation networks and systems: Proceedings of 22nd international conference, NEW2AN 2022* (pp. 244-251). Cham: Springer. doi: 10.1007/978-3-031-30258-9_21.

7. Oladipupo, A. O., & Oladeji, T. N. (2025). Cryptocurrency and global finance: Intersections of international security, terrorist financing, and financial development. *International Journal of Cryptocurrency Research*, *5*(1), 102–121. https://doi.org/10.51483/IJCCR.5.1.2025.102-121

8. Волинець В.В. Державний контроль за обігом віртуальних активів в Україні / В.В. Волинець // Науковий вісник Ужгородського національного університету. Серія: Право. – 2025. – Вип. 88, ч. 2. – С. 26. – DOI: https://doi.org/10.24144/2307-3322.2025.88.2.3.

9. Phillips, R., & Wilder, H. (2020). Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites. In *2020 IEEE international conference on blockchain and cryptocurrency (ICBC)*. doi: 10.1109/ICBC48266.2020.9169433

10. FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2023. URL: https://www.fatf-gafi.org/publications/virtualassets/documents/updated-guidance-virtual-assets-vasps.html

11. FATF. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. Paris: FATF, 2024. URL: https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets-red-flag-indicators.html

12. United Nations Office on Drugs and Crime. Money Laundering and Terrorist Financing through Virtual Assets. Vienna: UNODC, 2024. URL: https://www.unodc.org/documents/money-laundering/Publications/Virtual_Assets_Report_2024.pdf

13. Council of Europe. Guidelines on Virtual Currencies and Terrorist Financing. Strasbourg: CoE Publishing, 2023. URL: https://rm.coe.int/guidelines-virtual-currencies-terrorist-financing/1680a9c2b4
14. International Convention for the Suppression of the Financing of Terrorism. New York, 9 December 1999. United Nations Treaty Series, vol. 2178, p. 197. URL: https://treaties.un.org/doc/db/Terrorism/Conv12-english.pdf
15. UN Security Council Resolution 1267 (1999) of 15 October 1999. URL: https://www.un.org/securitycouncil/sanctions/1267/resolutions
16. UN Security Council Resolution 1373 (2001) of 28 September 2001. URL: https://www.un.org/securitycouncil/content/resolutions-adopted-security-council-2001
17. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris: FATF, 2023. URL: https://www.fatf-gafi.org/recommendations.html
18. Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets (MiCA). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114
19. Directive (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
20. Bank Secrecy Act, 31 U.S.C. §§ 5311-5332. URL: https://www.law.cornell.edu/uscode/text/31/subtitle-IV/chapter-53/subchapter-II
21. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). URL: https://www.congress.gov/bill/107th-congress/house-bill/3162
22. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. 2008. URL: https://bitcoin.org/bitcoin.pdf
23. Ментух, Н. Ф., & Шевчук, О. Р. (2022). Правові аспекти оподаткування господарської діяльності суб'єктів господарювання в Україні в умовах воєнного стану. *Наукові записки. Серія: Право, 12*, 64–69. https://doi.org/10.36550/2522-9230-2022-12-64-69
24. Європейське агентство з боротьби з наркотиками. Криптовалюти та незаконна торгівля наркотиками в даркнеті. Ліссабон: EMCDDA, 2024. URL: https://www.emcdda.europa.eu/publications/joint-publications/cryptocurrencies-darknet-drug-trade_en
25. Blockchain Association. Cross-Border Regulatory Challenges in Virtual Asset Transactions. Regulatory Compliance Quarterly. 2024. Vol. 8. No. 2. P. 34-52. URL: https://blockchain.org/research/cross-border-regulatory-challenges
26. Payment Services Act 2019 (Singapore), Act No. 2 of 2019. URL: https://sso.agc.gov.sg/Acts-Supp/2-2019
27. Payment Services Act (Japan), Act No. 59 of 2009, as amended in 2020. URL: https://www.japaneselawtranslation.go.jp/law/detail/?id=3078
28. Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (Switzerland), SR 958.1. URL: https://www.fedlex.admin.ch/eli/cc/2021/33/en
29. Canadian Securities Administrators. Staff Notice 21-327 Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets. 2023. URL: https://www.securities-administrators.ca/aboutcsa.aspx?id=1588
30. Chainalysis Inc. Crypto Crime Report 2024. New York: Chainalysis, 2024. URL: https://www.chainalysis.com/reports/2024-crypto-crime-report/
31. Шевчук, Оксана, and Роман Береза. "Правові засади регулювання ринку фінансових послуг у Європейському Союзі: концептуальні підходи, нормативно-правові

механізми та інституційна структура". *Актуальні проблеми правознавства*, no. 1, May 2025, pp. 62-68, https://appj.wunu.edu.ua/index.php/appj/article/view/2049.

32. Europol. Cryptocurrencies: Tracing the Evolution of Criminal Finances. The Hague: Europol, 2024. URL: https://www.europol.europa.eu/publications-documents/cryptocurrencies-tracing-evolution-of-criminal-finances

33. Basel Committee on Banking Supervision. Prudential Treatment of Cryptoasset Exposures. Basel: BIS, 2023. URL: https://www.bis.org/bcbs/publ/d545.htm