МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНА НАВЧАЛЬНО-НАУКОВА УСТАНОВА
«АКАДЕМІЯ ФІНАНСОВОГО УПРАВЛІННЯ»

ДЕРЖАВНА НАВЧАЛЬНО-НАУКОВА УСТАНОВА
«АКАДЕМІЯ ФІНАНСОВОГО УПРАВЛІННЯ»

Кваліфікаційна наукова
праця на правах рукопису

ДМИТРЕНКО ТЕТЯНА ЛЕОНІДІВНА

УДК 336.744; 330.131

ДИСЕРТАЦІЯ

РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ДО РЕГУЛЮВАННЯ ОБОРОТУ ЦИФРОВИХ АКТИВІВ У СФЕРІ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ І ФІНАНСУВАННЮ ТЕРОРИЗМУ

Спеціальність 08.00.08. - Гроші, фінанси і кредит

Подається на здобуття наукового ступеня доктора економічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело



Т. Л. Дмитренко

(підпис, ініціали та прізвище здобувача)

Науковий консультант:
Єфименко Тетяна Іванівна,
доктор економічних наук, професор
академік НАН України

Київ – 2025

АНОТАЦІЯ

Дмитренко Т.Л. Ризик-орієнтований підхід до регулювання обороту цифрових активів у сфері протидії відмиванню коштів і фінансуванню тероризму. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.08 – гроші, фінанси і кредит. – Державна навчально-наукова установа «Академія фінансового управління». Міністерство освіти і науки України, Київ, 2025.

Дисертація присвячена комплексному дослідженню теоретичних засад оцінки та управління ризиками обороту цифрових активів у сфері протидії відмиванню доходів, отриманих злочинним шляхом, та фінансуванню тероризму.

На основі систематизації та критичного аналізу наукових досліджень закордонних і вітчизняних вчених розкрито економічну сутність понять «ризику» і «невизначеності», проведена класифікація поняття «ризику» за його типами та в різних галузях науки.

У дослідженні визначено, що класичні економічні теорії ризику, такі як теорія ризику та невизначеності Френка Найта, теорія очікуваної корисності фон Неймана-Моргенштерна, портфельна теорія Гаррі Марковіца та економічна теорія регулювання ризиків Стіглера-Пельцмана, можуть ефективно адаптуватися до сучасних умов цифрової економіки. Зокрема, у сфері регулювання обігу цифрових активів для протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) запропоновано міждисциплінарний підхід, який інтегрує економічні концепції з новітніми технологічними засобами аналізу, такими як блокчейн-аналітика, штучний інтелект і поведінкова економіка. Підкреслено необхідність продовження міждисциплінарних досліджень для вироблення оптимальних механізмів регулювання цифрових активів, що дозволить знизити ризики для фінансової безпеки на національному та глобальному рівнях. Обґрунтовано, що ефективність ризик-орієнтованого

підходу значною мірою залежить від гармонізації міжнародних регуляторних стандартів, посилення прозорості криптовалютних трансакцій, а також впровадження інноваційних інструментів контролю і оцінки ризиків.

У дисертації складена послідовність процесу оцінки ризику відмивання доходів, отриманих злочинним шляхом, та фінансуванню тероризму через його причинно-наслідковий фактор, який в подальшому набув складової секторальної та національної оцінки ризиків щодо цифрових активів в сфері ПВК/ФТ.

У дисертації здійснено обґрунтований аналіз міжнародних і стандартів у сфері ПВК/ФТ щодо операцій із цифровими активами та діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів. Ці стандарти стали основою для розробки методики оцінки та управління відповідними ризиками. Дослідження значення ризик-орієнтованого підходу засвідчує не лише поступове підвищення ефективності протидії легалізації незаконних доходів і фінансуванню тероризму, а й оптимізацію ресурсів для здійснення цих заходів. В дослідженні обґрунтовано, що завдяки обміну інформацією про діяльність учасників крипторинку, узгодженню нормативно-правових актів із процедурами ПВК/ФТ, спрямованості на забезпечення швидких і результативних процедур без дублювання функцій, розвиток віртуальних активів і запровадження цифрових валют центральних банків цифрові активи стануть інноваційними інструментами як глобальної, так і національної економіки, обіг яких одночасно відповідатиме міжнародним стандартам ПВК/ФТ.

На основі європейської таксономії віртуальних активів в дисертації надано авторське визначення «цифрових активів» та проведено аналіз дефініцій національного законодавства щодо обороту цифрових активів. Впровадження концепції цифрових валют центральних банків на глобальному рівні призвело до перегляду традиційних підходів до розуміння природи грошей, їх функцій і ролі центральних банків у здійсненні монетарної політики. У цьому аспекті цифрові валюти центральних банків виступають як новий інструмент грошового обігу, який компенсує характеристики цифрових активів із гарантіями державної

підтримки. Відокремлення стейблкоїнів та інвестиційних токенів в окремі групи віртуальних активів дало можливість економічній науці глибше проаналізувати цифрову вартість, а також механізми її збереження та передачі, що сприяло активному вивченню поведінкових аспектів використання.

Завдяки проведеному кластерно-порівняльному аналізу ризиків використання цифрових активів в злочинній діяльності розглянуті показники ризику («червоні прапорці») в легалізаційній, терористичній, корупційній діяльності, в шахрайстві (маніпулювання цифровими активами), розмиванні бази оподаткування з використанням віртуальних активів, розроблені критерії для оцінки ризику використання віртуальних активів в зазначеній кримінальній діяльності.

Зростання ролі криптоактивів у злочинній діяльності вимагає комплексного підходу до регулювання, моніторингу та запобігання ризикам їх використання. Використання критеріїв ризику («червоних прапорців») для оцінки операцій із криптоактивами сприятиме ранньому виявленню та запобіганню злочинних схем, тому в досліджені саме на основі розроблених критеріїв ризику використання віртуальних активів у відмиванні доходів, отриманих злочинним шляхом, та фінансування тероризму розроблена методологія оцінки зазначеного ризику з використанням сучасних методів аналізу, а саме класифікації, експертних оцінок, регресійного аналізу, гравітаційного моделювання. Запропоновано додати до застосування метод Байесових мереж на стадії діяльності вже легалізованого ринку через показники економічної діяльності професійних операторів криптоіндустрії. Розроблена методика може бути застосована і для критеріїв ризику іншої нелегальної діяльності, і запропонована до включення до Програм ПВК/ФТ постачальників послуг, пов’язаних з оборотом цифрових активів.

У результаті дослідження встановлено, що інтеграція нових технологічних рішень, зміцнення міжнародного співробітництва та встановлення ліцензійних вимог для провайдерів криптосервісу сприятимуть мінімізації ризиків

відмивання коштів, фінансування тероризму та фінансових злочинів у цифровому середовищі.

Технологія блокчейн продемонструвала високу ефективність в управлінні ідентифікацією, адмініструванні прав на землю, відстеженні походження та логістиці, що призвело до зниження витрат на трансакції та покращення відстеження коштів. Надійне підтвердження особи стало наріжним каменем фінансової доступності. Блокчейн був запропонований як технологія, здатна забезпечити безпечну ідентифікацію, з пілотними проектами, які зараз реалізуються в країнах, що розвиваються. Оцифрування державних реєстрів і надання цифрових публічних послуг визначено ключовими заходами для підвищення прозорості. Крім того, захист цих реєстрів за допомогою технології блокчейн може запобігти корупції та маніпуляції записами.

У дисертації досліджено вплив ринку віртуальних активів на ключові макроекономічні показники світової економіки, зокрема рівень інфляції, відкритість капіталу, контроль корупції, реальний ВВП на душу населення, кількість відділень комерційних банків, середнє співвідношення грошових переказів до ВВП, кількість захищених інтернет-серверів.

Багатофакторний регресійний аналіз показників із застосуванням підходу від загального до конкретного емпірично підтверджує зв’язок між впровадженням криптовалюти, рівнем корупції та посиленням контролю над капіталом. Враховуючи зростаючу макроекономічну роль криптоактивів, результати обґрунтовують необхідність регуляторного нагляду, зокрема через впровадження процедур ідентифікації клієнтів фінансовими посередниками.

Проведений аналіз також підкреслює необхідність покращення якості даних для більш глибокого розуміння чинників, що визначають динаміку впровадження криптоактивів. Більшість наукових досліджень зосереджуються на питанні, чи сприяють криптоактиви корупції або, навпаки, допомагають у її подоланні. Однак комплексне вивчення множинного впливу крипторинку на макроекономічні показники залишається актуальним напрямом подальших

досліджень. Використання технології блокчейн для боротьби з корупцією можливе, проте лише за наявності відповідних передумов.

Високий рівень прозорості блокчейну відкриває недооцінені можливості для державного та приватного секторів у виявленні й запобіганні незаконній діяльності, зокрема ухиленню від санкцій через використання віртуальних активів.

У дисертації проведено огляд міжнародних санкцій, запроваджених проти банків, компаній та фізичних осіб рф та рб з боку США, Європейського Союзу та Великої Британії. Проаналізовано вразливі аспекти національної санкційної політики та розроблено рекомендації для підвищення ефективності впровадження міжнародних обмежень. Особливу увагу приділено необхідності оперативних і оптимальних рішень щодо легалізації діяльності ринку віртуальних активів та впровадження ризик-орієнтованого підходу до взаємодії операторів крипто- і фінансового ринку в Україні.

З огляду на актуальні виклики, процес регулювання законодавства вимагає швидких і ефективних заходів. Доцільним є ухвалення пропозицій щодо застосування секторних економічних та інших обмежувальних заходів (санкцій) до постачальників послуг, пов’язаних з оборотом віртуальних активів, які співпрацюють з банками рф, рб та пов’язаними особами. Ці заходи включають блокування активів, їх стягнення на використання держави, обмеження торговельних операцій із криптоактивами, запобігання відтоку капіталу за кордон, анулювання або зупинення ліцензій і дозволів на здійснення певних видів фінансової діяльності, а також обмеження чи припинення надання електронних комунікаційних послуг та доступу до використання електронних комунікаційних мереж.

Тісна співпраця з наглядовими та правоохоронними органами, повідомлення про будь-які підозрілі дії та операції, що здійснюються постачальниками послуг, пов’язаних з оборотом віртуальних активів та фінансових послуг, які працюють в Україні та за її межами є потужним інструментом для зупинення російської

агресії. Витрати, пов'язані з підвищеною обачністю, є однією з форм підтримки України та безпеки в Європі та США.

Також, в дисертаційній роботі розглянуто та проаналізовано процес формування законодавства України щодо обігу віртуальних активів, оподаткування операцій з віртуальними активами, пілотний проєкт НБУ щодо запуску національної CBDC – е-гривні, відповідність діючого та розробленого законодавства щодо імплементації оновлених Рекомендацій FATF та європейського законодавства відповідно до Стратегії цифрових активів у ЄС.

Держави-члени Європейського Союзу активно впроваджують заходи щодо усунення нормативно-правових прогалин з надання регулювання обігу віртуальних активів. У цьому застосуванні відбувається процес правової аналогії через єдину методологію ідентифікації віртуальних активів і розширення на них дії суміжного законодавства, особливо якщо ці активи мають спільні риси з фінансовими інструментами чи електронними грошима.

Для криптовалютних інструментів, які не мають аналогів серед фінансових інструментів ЄС, розроблені нові нормативно-правові акти, зокрема Регламент ЄС MiCA (Markets in Crypto-Assets). Також було впроваджено законодавство, яке імплементує в європейське право 16-ту рекомендацію FATF, так зване «Правило подорожі» (Travel Rule), закріплене в Регламенті ЄС TFR (Transfer of Funds Regulation), що передбачає супровід трансакцій із віртуальними активами інформацією про її учасників.

З огляду на зростання загроз кіберзлочинності, Європейська Комісія розробила низку регуляторних актів для фінансових установ і професійних операторів крипторинку. Серед них — Регламент про цифрову стійкість DORA, стратегія розвитку DLT-технологій, оновлені Директиви ЄС щодо запобігання відмиванню коштів та фінансуванню тероризму (AMLD6), а також Директива щодо обміну податковою інформацією, що охоплює й учасників крипторинку (DAC8). Це свідчить про комплексний підхід європейських законодавців до розвитку цифрової економіки та боротьби з кіберзлочинністю як у межах ЄС, так

і у взаємодії з країнами, що не є його членами. З набуттям Україною статусу кандидата в члени ЄС легалізація ринку віртуальних активів з урахуванням міжнародних стандартів FATF стала складовою необхідних кроків для членства у європейській спільноті.

В дисертації надані пропозиції щодо підвищення прозорості та ефективності регулювання криптоіндустрії, які включають пропозиції щодо впровадження ризик-орієнтованого підходу в сфері ПВК/ФТ як взірця для побудови державного регулювання загалом.

Ефективний ризик-орієнтований підхід має враховувати природу, різноманітність та рівень розвитку криптоіндустрії в країні, оцінку ризиків цього сектора та його учасників, а також специфіку національного правового та регуляторного середовища. З огляду на транскордонний характер криптовалютного ринку та глобальну доступність більшості видів діяльності з віртуальними активами, такий підхід є ключовим для збалансованого регулювання.

Регульована криптоекономіка здатна забезпечувати податкові надходження до державного бюджету, сприяти залученню та утриманню талантів у сфері стартапів, а також зміцнювати позиції країни як конкурентного гравця на світовому цифровому ринку. Чітко розроблене законодавство щодо криптоактивів сприятиме виведенню криптоіндустрії з так званої «сірої зони» у правове поле, що підвищить її легітимність і рівень довіри до цього динамічного ринку. Впровадження чіткої податкової політики щодо оподаткування криптоактивів та інтеграція України в систему автоматичного обміну податковою інформацією є ключовими вимогами для гармонізації законодавства України з нормами ЄС.

У дисертації проаналізовано залучення Україною інноваційних FinTech-стартапів для створення регульованих платформ торгівлі криптоактивами, які відповідають міжнародним стандартам, зокрема MiCA. Встановлено, що українські FinTech-компанії активно розробляють технологічні рішення для

автоматизації комплаєнсу та ПВК/ФТ-процедур, що сприяє підвищенню прозорості фінансових потоків і мінімізації ризиків відмивання коштів.

У рамках дослідження проаналізовано ініціативи Національного банку України щодо можливого впровадження цифрової гривні (eUAH) на основі блокчейн-технологій. Визначено, що такий крок може значно підвищити ефективність платежів та фінансову прозорість. Крім того, проаналізовано впровадження регуляторних та наглядових технологій (SupTech/RegTech) в Україні як важливих інструментів моніторингу та нагляду за криптовалютним ринком. Зокрема, розглянуто можливості автоматичного обміну даними між державними регуляторами та міжнародними організаціями, такими як FATF, MONEYVAL і ЄС, у контексті оцінки санкційних ризиків.

На основі емпіричних даних досліджено застосування штучного інтелекту та аналітики великих даних (Big Data) Національним банком України, НКЦПФР та Держфінмоніторингом для оперативного виявлення підозрілих операцій з криптоактивами. Також проаналізовано ефективність використання блокчейн-аналітики для відстеження нелегальних фінансових потоків у сфері віртуальних активів. Вивчено розвиток цифрових технологій ідентифікації, зокрема Mobile ID та BankID, які сприяють спрощенню доступу до криптоактивів при дотриманні регуляторних вимог.

У дисертації також досліджено впровадження українськими криптобіржами та фінансовими установами RegTech-рішень для автоматизованого аналізу клієнтів і перевірки їхніх операцій на предмет фінансових ризиків. Виявлено, що застосування машинного навчання та штучного інтелекту у процесах комплаєнсу дозволяє підвищити ефективність прогнозування фінансових загроз та виявлення шахрайських схем.

Окрему увагу приділено необхідності посилення співпраці між державними органами, фінансовими установами та криптосектором для боротьби з фінансовими злочинами, відмиванням коштів та фінансуванням тероризму. Обґрунтовано на прикладі співпраці блокчейн-аналітичних компаній Global

Ledger, Crystal, AMLbot, Chainalysis, Elliptic з державними правоохоронними та регуляторними органами, що розвиток публічно-приватного партнерства у сфері ПВК/ФТ сприятиме створенню безпечного фінансового середовища, мінімізації ризиків ухилення від санкцій та відмивання коштів, а також посиленню міжнародної довіри до України як прозорої та технологічно розвиненої фінансової юрисдикції.

Розвиток освітніх ініціатив та цифрової фінансової інклюзії також корелює з теорією регулювання ризиків, оскільки зменшує інформаційну асиметрію між учасниками ринку та регуляторами. Це сприяє створенню більш прозорого ринкового середовища, в якому регулятори та учасники ринку можуть приймати обґрунтовані рішення щодо управління ризиками.

Запропонована в дисертації модель, заснована на технологічних інноваціях, міжсекторальній кооперації та освітніх програмах, відповідає ключовим принципам економічної теорії фінансового ризик-менеджменту, яка виступає фундаментом для ефективного регулювання криптоактивів у сфері ПВК/ФТ.

Ключові слова: ризик-орієнтований підхід, цифрові активи, віртуальні активи, криптовалюта, цифрові валюти центральних банків, фінансові установи, фінансова безпека, національна система оцінки ризиків, протидія відмивання коштів і фінансування тероризму, легалізація доходів, отриманих злочинним шляхом.

ABSTRACT

Dmytrenko T.L. Risk-Based Approach to the Regulation of Digital Asset Turnover in the Field of Anti-Money Laundering and Counter-Terrorist Financing. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Economic Sciences on the specialty 08.00.08 – money, finance and credit. – The State Educational and Scientific Establishment «Academy of Financial Management». Kyiv, 2025.

The dissertation is dedicated to a comprehensive study of the theoretical foundations of risk assessment and management in digital asset turnover within the framework of anti-money laundering and counter-terrorist financing (AML/CTF). Based on the systematization and critical analysis of scientific research conducted by both foreign and domestic scholars, the economic essence of the concepts of «risk» and «uncertainty» is revealed. The dissertation classifies the concept of «risk» across its types and various scientific disciplines.

The study identifies that classical economic theories of risk, such as Frank Knight's theory of risk and uncertainty, the von Neumann-Morgenstern expected utility theory, Harry Markowitz's portfolio theory, and the Stigler-Peltzman economic theory of risk regulation, can be effectively adapted to the modern conditions of the digital economy.

In particular, in the field of regulating digital asset circulation to counter money laundering and terrorist financing, an interdisciplinary approach has been proposed. This approach integrates economic concepts with cutting-edge technological analysis tools, such as blockchain analytics, artificial intelligence, and behavioral economics.

The study emphasizes the necessity of continuing interdisciplinary research to develop optimal regulatory mechanisms for digital assets, which will help mitigate financial security risks at both national and global levels. It is substantiated that the effectiveness of the risk-based approach largely depends on the harmonization of international regulatory standards, the enhancement of cryptocurrency transaction transparency, and the implementation of innovative risk control and assessment tools.

Additionally, a sequential risk assessment process is developed, considering its causal factor, which further evolves into sectoral and national risk assessments concerning digital assets in the AML/CTF domain.

The research substantiates that through the exchange of information on the activities of crypto market participants, the alignment of regulatory frameworks with AML/CTF procedures, and the focus on ensuring swift and effective processes without functional duplication, the development of virtual assets and the introduction of central bank digital currencies (CBDCs) will transform digital assets into innovative instruments of both the global and national economies while simultaneously complying with international AML/CTF standards.

Based on the European taxonomy of virtual assets, the dissertation presents an original definition of «digital assets» and conducts an analysis of national legislation regarding their circulation. The research substantiates that global implementation of the CBDC concept has led to a reassessment of traditional approaches to understanding the nature of money, its functions, and the role of central banks in monetary policy. In this context, CBDCs serve as a new monetary circulation instrument that balances the characteristics of digital assets with state-backed guarantees.

The classification of stablecoins and investment tokens as distinct categories of virtual assets has enabled economic science to conduct a deeper analysis of digital value, as well as the mechanisms for its preservation and transfer. This, in turn, has facilitated an active study of the behavioral aspects of digital asset usage.

Through a cluster-based comparative analysis of the risks associated with the use of digital assets in criminal activities, key risk indicators («red flags») have been examined in the context of money laundering, terrorist financing, corruption-related crimes, fraud (manipulation of digital assets), and tax base erosion through virtual assets. Based on this analysis, criteria for assessing the risk of virtual asset use in ML/FT criminal activities have been developed.

The growing role of crypto assets in illicit activities necessitates a comprehensive approach to regulation, monitoring, and risk prevention. The use of risk indicators

(«red flags») to assess crypto-asset transactions will contribute to the early detection and prevention of criminal schemes. Therefore, the study develops a risk assessment methodology for virtual assets in AML/CTF based on the identified risk criteria, utilizing advanced analytical methods such as classification, expert evaluation, regression analysis, and gravity modeling.

Additionally, it is proposed to incorporate Bayesian network methods at the stage of an already legalized market by analyzing economic activity indicators of professional crypto industry operators. The developed methodology can also be applied to risk criteria for other illicit activities and is recommended for inclusion in the AML/CTF programs of service providers involved in digital asset circulation.

As a result of the dissertation, it has been established that the integration of new technological solutions, the strengthening of international cooperation, and the establishment of licensing requirements for crypto service providers will contribute to minimizing the risks of money laundering, terrorist financing, and financial crimes in the digital environment.

Blockchain technology has demonstrated high efficiency in identity management, land rights administration, provenance tracking, and logistics, leading to reduced transaction costs and improved fund traceability. Reliable identity verification has become a cornerstone of financial accessibility. Blockchain has been proposed as a technology capable of ensuring secure identification, with pilot projects currently being implemented in developing countries. The digitization of government registries and the provision of digital public services are identified as key measures for enhancing transparency. Furthermore, securing these registries through blockchain technology can prevent corruption and record manipulation.

The dissertation investigates the impact of the virtual asset market on key macroeconomic indicators of the global economy, including inflation rates, capital openness, corruption control, real GDP per capita, the number of commercial bank branches, the average ratio of remittances to GDP, and the number of secure internet servers.

A cross-regional regression analysis, applying the general-to-specific approach, empirically confirms the relationship between cryptocurrency adoption and both the perceived level of corruption and the tightening of capital controls. Given the growing macroeconomic role of crypto assets, the findings substantiate the necessity of regulatory oversight, particularly through the implementation of customer identification procedures by financial intermediaries.

The conducted analysis also highlights the necessity of improving data quality to gain a deeper understanding of the factors influencing the dynamics of crypto asset adoption. Most academic studies focus on whether crypto assets facilitate corruption or, conversely, help combat it. However, a comprehensive examination of the multifaceted impact of the crypto market on macroeconomic indicators remains a relevant area for further research. The use of blockchain technology to combat corruption is feasible but only under the right preconditions.

The high transparency of blockchain presents underestimated opportunities for both the public and private sectors in detecting and preventing illicit activities, particularly sanction evasion through virtual assets.

This study includes a review of international sanctions imposed against banks, companies, and individuals from the russian federation and belarus by the United States, the European Union, and the United Kingdom. It analyses the vulnerabilities in national sanction policies and provides recommendations to enhance the effectiveness of implementing international restrictions. Special attention is given to the need for prompt and optimal decisions regarding the legalization of the virtual asset market and the adoption of a risk-based approach to the interaction between crypto and financial market operators in Ukraine.

Given the current challenges, the process of regulating legislation requires swift and effective measures. It is advisable to adopt proposals for applying sectoral economic and other restrictive measures (sanctions) to service providers involved in the circulation of virtual assets who cooperate with russian and belarus banks, and associated entities. These measures include asset freezing, confiscation for state use,

restricting trading operations with crypto assets, preventing capital outflows abroad, canceling or suspending licenses and permits for specific types of financial activities, as well as limiting or halting the provision of electronic communications services and access to electronic communications networks.

Close collaboration with regulatory and law enforcement agencies, along with reporting any suspicious activities and operations carried out by service providers engaged in virtual asset and financial services operating within Ukraine and abroad, is a powerful tool for halting russian aggression. The costs associated with enhanced vigilance represent one form of support for Ukraine and security in Europe and the United States.

Additionally, the dissertation explores and analyses the process of legislative development in Ukraine concerning the circulation of virtual assets, the taxation of virtual asset transactions, the National Bank of Ukraine's pilot project for launching the national CBDC – the e-hryvnia, and the alignment of current and drafted legislation with the updated FATF Recommendations and European legislation in accordance with the Digital Assets Strategy for EU.

European Union member states are actively implementing measures to address regulatory gaps in the circulation of virtual assets. This process involves legal analogy, as the lack of national regulators requires a unified methodology for identifying virtual assets and expanding the applicability of related legislation, particularly when these assets share characteristics with financial instruments or electronic money.

For cryptocurrency instruments that do not have analogues among EU financial instruments, new regulations have been developed, including the EU Regulation MiCA (Markets in Crypto-Assets). Additionally, legislation has been implemented to incorporate the 16th FATF recommendation, known as the «Travel Rule,» into European law, which is enshrined in the EU Regulation TFR (Transfer of Funds Regulation). This regulation requires the inclusion of participant information in transactions involving virtual assets.

In response to the growing threats of cybercrime, the European Commission has developed a series of regulatory acts for financial institutions and professional crypto market operators. These include the Digital Operational Resilience Act (DORA), the strategy for developing DLT technologies, updated EU Directives on preventing money laundering and terrorist financing (AMLD6), and the Directive on the exchange of tax information, which covers crypto market participants (DAC8). This reflects the comprehensive approach of European legislators toward developing the digital economy and combating cybercrime both within the EU and in interaction with non-member countries. With Ukraine obtaining candidate status for EU membership, the legalization of the virtual asset market in line with FATF international standards has become an integral part of the necessary steps toward EU membership.

The dissertation provides proposals for enhancing the transparency and effectiveness of regulating the crypto industry, which include suggestions for implementing a risk-based approach in the field of AML/CFT as a model for building state regulation as a whole.

An effective risk-based approach must consider the nature, diversity, and level of development of the crypto industry in the country, the risk assessment of this sector and its participants, as well as the specifics of the national legal and regulatory environment. Given the cross-border nature of the cryptocurrency market and the global accessibility of most activities involving virtual assets, this approach is key to balanced regulation.

A regulated crypto economy can ensure tax revenues to the state budget, promote the attraction and retention of talent in the start-up sector, and strengthen the country's position as a competitive player in the global digital market. Well-developed cryptocurrency legislation will help move the crypto industry from the so-called «grey zone» into the legal framework, which will enhance its legitimacy and the level of trust in this dynamic market. The implementation of a clear tax policy regarding the taxation of crypto assets and Ukraine's integration into the system of automatic exchange of tax

information are key requirements for harmonizing Ukraine's legislation with EU standards.

The dissertation analyses Ukraine's engagement with innovative FinTech start-ups to create regulated cryptocurrency trading platforms that comply with international standards, particularly MiCA. It is established that Ukrainian FinTech companies are actively developing technological solutions to automate AML/KYC procedures, which contributes to enhancing the transparency of financial flows and minimizing money laundering risks.

The study also assesses the initiatives of the National Bank of Ukraine regarding the potential implementation of the digital hryvnia (eUAH) based on blockchain technologies. It is determined that such a step could significantly enhance the efficiency of payments and financial transparency. Furthermore, the implementation of regulatory and supervisory technologies (SupTech/RegTech) in Ukraine is analysed as important tools for monitoring and supervising the cryptocurrency market. Specifically, the potential for automatic data exchange between state regulators and international organizations, such as FATF, MONEYVAL, and the EU, is examined in the context of assessing sanctions risks.

Based on empirical data, the research explores the use of artificial intelligence and big data analytics by the National Bank of Ukraine, the National Securities and Stock Market Commission (NSSMC), and the State Financial Monitoring Service for the prompt detection of suspicious cryptocurrency transactions. The effectiveness of blockchain analytics for tracking illegal financial flows in the virtual assets sphere is also analysed. The development of digital identification technologies, particularly Mobile ID and BankID, which facilitate access to crypto assets while adhering to regulatory requirements, is studied.

The dissertation also explores the implementation of RegTech solutions by Ukrainian cryptocurrency exchanges and financial institutions for the automated analysis of clients and verification of their transactions for financial risks. It is found that the use of machine learning and artificial intelligence in compliance processes

enhances the effectiveness of forecasting financial threats and detecting fraudulent schemes.

Special attention is given to the need for strengthening cooperation between government agencies, financial institutions, and the crypto sector to combat financial crimes, money laundering, and terrorism financing. The example of cooperation between blockchain analytics companies such as Global Ledger, Crystal, AMLbot, Chainalysis, and Elliptic with state law enforcement and regulatory bodies is highlighted. The development of public-private partnerships in the AML/CFT sphere is argued to promote the creation of a secure financial environment, minimize the risks of sanctions evasion and money laundering, and strengthen international trust in Ukraine as a transparent and technologically advanced financial jurisdiction.

The development of educational initiatives and digital financial inclusion also correlates with the theory of risk regulation, as it reduces information asymmetry between market participants and regulators. This contributes to the creation of a more transparent market environment in which both regulators and market participants can make well-informed decisions regarding risk management.

The model proposed in the dissertation, based on technological innovations, cross-sectoral cooperation, and educational programs, corresponds to the key principles of the economic theory of financial risk management, which serves as the foundation for effective regulation of crypto-assets in the field of AML/CFT.

Keywords: risk-based approach, digital assets, virtual assets, cryptocurrency, central bank digital currencies, financial institutions, financial security, national risk assessment system, anti-money laundering and contr terrorism financing, legalization of criminal proceeds.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, які відображають основні наукові результати дисертації

1) Дмитренко Т. Л., Любіч О.О. Упровадження міжнародних стандартів регулювання ринку віртуальних активів в Україні. *Фінанси України.* 2020. № 9. С. 65-79. DOI: https://doi.org/10.33763/finukr2020.09.065 (0,71 друк. арк.). Особистий внесок: обґрунтовано концептуальні засади управління ризиками використання віртуальних активів в протиправній діяльності в умовах інформаційного суспільства (0,6 друк. арк.).

2) Дмитренко Т. Л., Любіч О. О., Пархоменко Ю. В. Регулювання ринку віртуальних активів: глобальний та національний рівні імплементації міжнародних стандартів ПВК/ФТ. *Фінанси України*. 2021. № 7. С. 31-52. DOI: https://doi.org/10.33763/finukr2021.07.031 (1,06 друк. арк.). Особистий внесок: проаналізовано міжнародне та європейське законодавство в сфері ПВК/ФТ (0,9 друк. арк.)

3) Дмитренко Т. Л., Волкова В. М. Особливості регулювання операцій із віртуальними активами щодо діяльності у сфері майнінгу. *Наукові праці НДФІ.* 2021. № 2. С. 85-95. https://doi.org/10.33763/npndfi2021.02.085 (0,61 друк. арк.). Особистий внесок: проаналізовано міжнародне та європейське законодавство щодо майнінгової діяльності (0,5 друк. арк.)

4) Дмитренко Т.Л., Волкова В.М. «Децентралізовані фінанси: їх розвиток у сучасній фінансовій системі та ризики, які вони спричиняють.» *Наукові праці НДФІ.* 2022. № 1. С. 55-68. DOI: https://doi.org/10.33763/npndfi2022.01.055 (0,75 друк. арк.). Особистий внесок: проаналізовано сучасні тенденції розвитку децентралізованих фінансів (0,6 друк. арк.)

5) Дмитренко Т. Л. Регулювання ринку віртуальних активів як інструмент протидії уникненню міжнародних санкцій проти рф. *Фінанси України.* 2022. №4. С. 107-128. DOI: https://doi.org/10.33763/finukr2022.04.107 (1,14 друк. арк.).

6) Єфименко Т.І., Дмитренко Т.Л. Сучасні пріоритети у сфері протидії відмиванню коштів та фінансуванню тероризму. *Наукові праці НДФІ.* 2022. №2

DOI: https://doi.org/10.33763/npndfi2022.02.005 (0,80 друк. арк.). Особистий внесок: проаналізовано критерії ризиків використання віртуальних активів в злочинній діяльності (0,7 друк. арк.)

7) Дмитренко Т.Л. Особливості імплементації Європейських Директив щодо обігу віртуальних активів в національне законодавство України. *Фінанси України*. 2022. № 10. DOI: https://doi.org/10.33763/finukr2022.12.056 (0,92 друк. арк.).

8) Дмитренко Т. Л., Терещенко Г. М. Підвищення рівня освіти у сфері кібербезпеки, фінансової та цифрової грамотності як чинник зниження ризиків на ринку віртуальних активів. *Освітня аналітика України*. 2023. №1(22). DOI: https://doi.org/10.32987/2617-8532-2023-1-38-50 (0,62 друк. арк.) Особистий внесок: розкрито міжнародний та європейський досвід розробки і впровадження освітніх проєктів щодо протидії використання криптоактивів в злочинній діяльності (0,5 друк. арк.)

9) Дмитренко Т.Л., Волкова В.М., Гавриленко С.В., Пархоменко Ю.В. Огляд нових пропозицій щодо регулювання ринку криптоактивів в Європі та шляхи імплементації їх в Україні. *Наукові праці НДФІ*. 2023. №2 (23) DOI: https://doi.org/10.33763/npndfi2023.01.030 (0,66 друк. арк.) Особистий внесок: проаналізовано міжнародне та європейське законодавство щодо впровадження зарубіжної законодавчої бази в національне законодавство (0,5 друк. арк.).

10) Hudima T., Kamyshanskyi V., Dmytrenko T., & Shmyhov M. Optimal CBDC design for Ukraine through the lens of privacy and security. *Amazonia Investiga*, 2023. 12(69). С.73-83. (**Web of Science**) DOI: https://doi.org/10.34069/AI/2023.69.09.6 (0,80 друк. арк.). Особистий внесок: досліджено можливі напрями впровадження е-гривні в фінансово-економічні процеси (0,3 друк. арк.).

11) Олійник Я., Кучерява М., Коритник Л., Дмитренко Т., Кузьмінська О., & Лагунов К. Формування інформаційного забезпечення управління фіскальними ризиками в умовах криз. *Financial and Credit Activity Problems of*

Theory and Practice. 2023. 6(53). С. 432–450. (**Web of Science**) DOI: https://doi.org/10.55643/fcaptp.6.53.2023.4219 (1,48 друк. арк.). Особистий внесок: викладено європейські стандарти щодо обміну інформацією про оподаткування операцій з віртуальними активами (0,5 друк. арк.)

12) Дмитренко Т. Л. Географічні кореляції щодо контролю над капіталом, криптоактивами та корупцією. *Фінанси України.* 2023. № 12. С. 114-128. DOI: https://doi.org/10.33763/finukr2023.12.114 (0,68 друк. арк.) Особистий внесок: досліджено вплив діяльності ринку віртуальних активів на макропоказники глобальної економіки (0,5 друк. арк.).

13) Iefymenko T., Dmytrenko T. Development and integration of digital currencies in the activity of the virtual asset market. *Science and Innovation.* 2025. № 2. С. 114-128. (**Scopus**) DOI: https://doi.org/10.15407/scine21.02.003 (0,70 друк. арк.). Особистий внесок: зроблено огляд міжнародних пілотних проєктів щодо розвитку CBDC країн, які їх розробляють; надані пропозиції щодо ефективного впровадження е-гривні (0,5 друк. арк.)

14) Дмитренко Т. Л. Методологічні підходи до розробки моделей оцінки ризиків використання цифрових активів у легалізації та злочинних операціях. *Фінанси України.* 2024. 12. С.75-92. DOI: https://doi.org/10.33763/finukr2024.12.075 (0,94 друк. арк.)

15) Дмитренко Т. Л., Терещенко Г. М. «Підвищення інвестиційної грамотності на крипторинку. *Освітня аналітика України*. 2024 № 5. DOI: https://doi.org/10.32987/2617-8532-2024-5-55-65 (0,54 друк. арк.) Особистий внесок: розкрито зв'язок між цифровою та фінансовою інклюзією з метою протидії шахрайству з використанням криптоактивів (0,4 друк. арк.)

16) Дмитренко Т.Л., Волкова В.М. Сучасні прогалини у регуляторній політиці щодо майнінгу криптовалют в системі віртуальних активів, наслідки та шляхи подолання їх. *Наукові праці НДФІ.* 2024. №3 (28). DOI: (0,88 друк. арк.) Особистий внесок: надано пропозиції щодо впровадження економічної

класифікації майнінгової діяльності (0,45 друк. арк.).

17) Дмитренко Т. Л. Визначення сутності віртуальних активів як чинник формування методологічних підходів до оподаткування їх обороту. *Вісник Чернівецького торговельно-економічного інституту.* 2024. Вип. IV (96). С. 125-150. DOI: http://doi.org/10.34025/2310-8185-2024-4.96.08 (1,13 друк. арк.)

18) Dmytrenko T., Hudima T. Risk assessment models for cryptocurrency use in fraud and criminal proceeds legalization. *Фінанси України.* 2025. №1. С.75-92. DOI: https://doi.org/10.33763/finukr2025.01.110 (1,13 друк. арк.) Особистий внесок: застосовано математичну модель оцінки ризику використання криптоактивів в злочинних легалізаційних операціях (1 друк. арк.).

19) Волкова В., Дмитренко Т. (2022). Децентралізовані фінанси: їх розвиток у сучасній фінансовій системі та ризики, які вони спричиняють. *Grail of Science*/ 2022. №12-13. С. 71–80. DOI: https://doi.org/10.36074/grail-of-science.29.04.2022.007 (0,33 друк. арк.) Особистий внесок: проаналізовані загрози та вразливості операцій з токенами на децентралізованих платформах (0,2 друк. арк.).

20) Дмитренко Т. Л. Особливості регулювання операцій із віртуальними активами щодо протидії легалізації доходів, отриманих злочинним шляхом. *Фінанси України.* 2020. № 3. С. 112-126. DOI: https://doi.org/10.33763/finukr2020.03.112 (0,72 друк. арк.)

Наукові праці, які додатково відображають наукові результати дисертації

21) О.О. Любіч, Т.Л. Дмитренко. Актуальні проблеми безпеки застосування віртуальних активів в Україні. *Матеріали І Міжнар. наук.-практ. конф., Херсон, 08-11 вересня 2021 р.* – Херсон: Морський інститут імені контр-адмірала Ф.Ф. Ушакова, 2021. – С. 81 – 83. (0,2 д.а.).

22) Т.Л. Дмитренко, Волкова В.М. Розвиток майнінгу віртуальних активів в національній економічній системі. *Матеріали І Міжнародної науково-*

практичної інтернет-конференції «Вплив пандемії COVID-19 на розвиток сучасного світу: загрози та можливості», Дніпро, 9-10 вересня 2021р. Дніпро: Міжнародний електронний науково-практичний журнал «WayScience». 2021. С. 75 – 78. (0,2 д.а.).

23) Дмитренко Т.Л., Волкова В.М. Ризики від майнінгу криптовалют в економічній системі України. *Матеріали II Міжнародна науково-практична конференція Multidisziplinäre forschung: perspektiven, probleme und muster Відень, 26 листопада 2021р.* Відень: LLC International Centre Corporative Management (Republic of Austria) та NGO European Scientific Platform (Ukraine). С. 75-78. (0,2 д.а.).

24) Дмитренко Т.Л. Протидія глобальним викликам, пов'язаним з використанням інноваційних технологій у злочинних цілях, шляхом підвищення стандартів кримінального аналізу. *Матеріали Міжвідомчої науково-практичної конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» НАВС (м. Київ, серпень, 2022р.)* (0,2 д.а.).

25) Дмитренко Т.Л. Впровадження міжнародних стандартів FATF щодо легалізації ринку віртуальних активів як складова економічного зростання України. *Матеріали Всеукраїнської науково-практичної інтернет-конференції «Актуальні питання бухгалтерського обліку, аналізу, аудиту та оподаткування в умовах воєнного стану і післявоєнного відновлення» (м. Київ, 15 червня 2023р.)* (0,2 д.а.).

26) Дмитренко Т. Оцінка макрофінансових ризиків щодо діяльності з криптоактивами. *Матеріали Міжнародної науково-практичної конференції «Фіскальна та монетарна безпека національної економіки в умовах глобальних викликів і загроз» (м. Київ, 31 жовтня 2023р.)* (0,2 д.а.).

27) Dmytrenko T. Legalization of the virtual assets market is often considered a crucial element in enhancing Ukraine's financial security. *Матеріали Науково-практичної конференції аспірантів та докторантів «Забезпечення*

резилієнтності економіки України в умовах військової агресії та повоєнного відновлення» (м. Київ, 12 грудня 2023р.) (0,2 д.а.).

28) Дмитренко Т.Л. Інноваційні підходи до розвитку теорії грошей Михайла Туган-Барановського та сучасність. *Матеріали академічних читань "Наукова спадщина Михайла Туган-Барановського для відбудови України", ДУ «Інститут економіки та прогнозування НАН України», (м. Київ, 18 січня 2024р.)* (0,2 д.а.).

29) Дмитренко Т.Л., Волкова В.В. Аналіз ризиків безпеки у використанні майнінгу криптовалют в операціях з відмиванням доходів, отриманих злочинним шляхом, та перспективи їх подолання. *Матеріали Першого Міжнародного фінансового форуму «Модерні фінанси: глобальні виклики і сучасні тренди». (м. Тернопіль, 19-23 червня 2024р.)* (0,2 д.а.).

30) Дмитренко Т.Л. Оподаткування криптовалют: світова практика та ситуація в Україні. *Матеріали ІІ Науково-практичної конференції аспірантів та докторантів «Забезпечення резилієнтності економіки України в умовах військової агресії та повоєнного відновлення». ДННУ Академія фінансового управління (м. Київ, 17 липня 2024 р.)* (0,2 д.а.).

31) Дмитренко Т.Л., Волкова В.В. Пруденційний нагляд та оподаткування діяльності майнінгу криптовалют в Україні. *Матеріали Х Міжнародній науково-практичній конференції «Актуальні проблеми управління соціально-економічними системами». Луцький національний технічний університет (м. Луцьк, 6 грудня 2024 р.)* (0,2 д.а.).

32) Дмитренко Т.Л., Волкова В.В. Європейська інтеграція майнінгу криптовалют та ринку віртуальних активів в Україні та національний аспект імплементації європейських стандартів щодо протидії відмиванню доходів, отриманих злочинним шляхом. *Матеріали ІІ Міжнародної науково-практичної конференції «Економічна аналітика: сучасні реалії та прогностичні можливості», Київський національний економічний університет імені Вадима Гетьмана (м. Київ, 24 січня 2025р.)* (0,2 д.а.).

33) Дмитренко Т.Л., Волкова В.В. Теорія криз Туган-Барановського як підґрунтя розвитку цифрової економіки та регулювання на глобальному рівні. *Матеріали Міжнародної науково-практичній конференції «Наукова спадщина Михайла Туган-Барановського як концептуальне підґрунтя суспільного розвитку» ДУ «Інститут економіки та прогнозування НАН України» (м. Київ, 29 січня 2025р.)* (0,2 д.а.).

ЗМІСТ

ВСТУП 30

1 РОЗДІЛ. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В СФЕРІ ПВК/ФТ ДО РЕГУЛЮВАННЯ ОБОРОТУ ЦИФРОВИХ АКТИВІВ

1.1. Ризик-орієнтований підхід як модель ефективного регулювання..…. 50

1.2. Міжнародні та європейські стандарти ПВК/ФТ в операціях з цифровими активами та діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів …… 75

1.3. Сутність та таксономія цифрових активів……..…….. 132

Висновки до 1 розділу ……. 169

2 РОЗДІЛ. МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ВПРОВАДЖЕННЯ МІЖНАРОДНИХ ТА ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ПВК/ФТ НА НАЦІОНАЛЬНОМУ РІВНІ

2.1. Міжнародні та європейські методологічні стандарти оцінки та управління ризиком в сфері ПВК/ФТ та їх впровадження на наднаціональному, національному та секторальному рівнях …….. 173

2.2. Кластерно-порівняльний аналіз ризиків використання цифрових активів в злочинній діяльності ……. 215

2.3. Математичні моделі оцінки ризику використання цифрових активів в легалізаційних та кримінальних операціях ……. 249

Висновки до 2 розділу …… 279

3 РОЗДІЛ. ЛЕГАЛІЗАЦІЯ ДІЯЛЬНОСТІ РИНКІВ ЦИФРОВИХ АКТИВІВ В УКРАЇНІ

3.1. Регулювання діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів …… 283

3.2. Удосконалення механізмів тестування української цифрової валюти та перспективи її впровадження ……..... 305
3.3. Декларування цифрових активів як елемент антикорупційної політики…….. 325
3.4. Методологічні засади запобігання порушенням, пов'язаним із використанням криптоактивів у процесі застосування санкцій.…… 357
Висновки до 3 розділу ……. 387
4 РОЗДІЛ. СТРАТЕГІЇ ПОДАЛЬШОЇ ЛЕГАЛІЗАЦІЇ ТА РЕГУЛЯТОРНОГО ВДОСКОНАЛЕННЯ РИНКІВ ЦИФРОВИХ АКТИВІВ В УКРАЇНІ В КОНТЕКСТІ ПВК/ФТ
4.1. Фіскально-правові та обліково-звітні аспекти національного регулювання операцій з віртуальними активами відповідно до європейських стандартів: оподаткування, майнінг та бартерні операції …….…… 391
4.2. Інтеграція сучасних технологічних рішень у систему управління ризиками обігу віртуальних активів у антилегалізаційній сфері …… 425
4.3. Посилення фінансово-цифрової інклюзії в умовах розвитку ринку цифрових активів як складова ПВК/ФТ …… 463
Висновки до 4 розділу ……. 482
ВИСНОВКИ ……...……...…….. 485
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……..…… 497
ДОДАТКИ ……..……..…….. 557

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВК/ФТ/РЗМЗ – відмивання коштів/ фінансування тероризму/ розповсюдження зброї масового знищення

ВА – віртуальні активи

ЄДІС – Єдина державна інформаційна система

ДСФМУ – Державна служба фінансового моніторингу України

ЗСК («Знай свого клієнта») – KYC (“Know you client”)

ЗСТ («Знай свою трансакцію») – KYT (“Know you transaction”)

ККУ – Кримінальний кодекс України

МВС – Міністерства внутрішніх справ України

МФУ – Міністерство фінансів України

Мін’юст – Міністерство юстиції України

Мінцифри – Міністерство цифрової трансформації України

МСФЗ (IFRS) – Міжнародні стандарти фінансової звітності

НАБУ – Національне антикорупційне бюро України

НБУ – Національний банк України

НКЦПФР – Національна комісія з цінних паперів та фондового ринку

НОР – Національної оцінки ризиків у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом і фінансуванню тероризму

ПВК/ФТ (Протидія відмивання коштів/ фінансування тероризму) – AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism)

ППВА – постачальники послуг, пов’язаних з оборотом віртуальних активів

План дій реформ оподаткування транснаціональних корпорацій **BEPS** – Base Erosion and Profit Shifting (BEPS) Action Plan

ПФР (підрозділи фінансової розвідки Групи «Егмонт» – FIU (Financial Intelligence Units EGMONT GROUP)

ПсБО План національних стандартів бухгалтерського обліку

СБУ – Служби безпеки України

СДФМ – суб’єкти державного фінансового моніторингу

СПФМ - суб’єкти первинного фінансового моніторингу

ФАТФ (Міжнародна група з протидії відмиванню брудних грошей) – FATF (Financial Action Task Force)

ЦКУ – Цивільний кодекс України

BIS (Bank for International Settlements) – БМР (Банк міжнародних розрахунків)

CBDC (Central bank digital currency) Цифрові валюти центральних банків

EU (European Union) – ЄС (Європейський Союз)

IMF (International Monetary Fund) – МВФ (Міжнародний валютний фонд)

G7 (Group of Seven) – «Велика сімка» економічно розвинених країн

MONEYVAL (Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism) – МАНІВЕЛ (Обраний Комітет експертів Ради Європи з оцінки заходів боротьби з відмиванням грошей)

OECD (Organization for Economic Cooperation and Development) – ОЕСР (Організації економічного співробітництва та розвитку)

OSCE (Organization for Security and Co-operation in Europe) – ОБСЄ (Організація з безпеки та співробітництва в Європі)

FATCA (Foreign Account Tax Compliance Act) – Закон про податкові вимоги до іноземних рахунків

FSB (Financial Stability Board) – РФС (Рада фінансової стабільності)

StR – сумнівна операція

UN (United Nation) – ООН (Організація Об'єднаних Націй)

UNODC (United Nations Office on Drugs and Crime) – УНП ООН (Управління ООН по наркотикам і злочинності)

WB (World Bank) – СБ (Світовий Банк)

ВСТУП

Швидкий розвиток глобалізаційних та інноваційних процесів у цифровій економіці призводить до зростання обсягів і різноманітності крипто-фінансових операцій, що створює нові виклики та загрози, пов’язані з легалізацією нелегальних крипто-фінансових активів.

Завдяки глобальній доступності через комп’ютерні мережі, оборот цифрових активів має міжнародний характер, і злочинні організації, пов'язані з наркотиками та іншими правопорушеннями, використовують його можливості. Ключовими завданнями національної системи протидії відмиванню коштів, отриманих злочинним шляхом, є створення дієвого механізму оцінки та управління ризиками, що виникають через функціонування тіньового капіталу.

У цьому контексті актуальним стає запобігання використанню фінансових і цифрових інструментів, які впливають на легітимність фінансових операцій для відмивання доходів у фінансових установах, що є пріоритетом національної фінансової безпеки. Однак, для легалізації крипторинку існують проблеми, пов’язані з неодночасністю впровадженням міжнародних та європейських стандартів в сфері ПВК/ФТ щодо обміну інформацією про учасників трансакції та правових підстав здійснення такої трансакції, що унеможливлює моніторинг і аналіз підозрілих трансакцій. Щодо легалізації діяльності української криптоіндустрії, першим завданням залишається визначення фіскальної політики та оподаткування операцій з віртуальними активами для завершення розробки нормативно правових актів та перехід до впровадження законодавства в діяльність національного ринку віртуальних активів. Також, враховуючи прийняту на державному рівні європейську інтеграцію, вимогами набуття членства в Європейському Союзі є приведення у відповідність до європейських норм національного законодавства, в тому числі і правової бази діяльності крипторинку. Залишається відкритим питання щодо сфери впровадження

національної цифрової валюти - е-гривні.

Систематичний моніторинг і аналіз підозрілих трансакцій як безперервного економічного процесу є важливим для підтримання довіри інвесторів до криптоіндустрії та фінансового ринку, а також для забезпечення бездоганної ділової репутації перед вкладниками та клієнтами. Проблеми оцінки ризику використання віртуальних активів в протидії легалізації доходів, отриманих злочинним шляхом, з використанням інновацій та новітніх технологій досліджувались такими зарубіжними вченими, як Дж. Бонно, А. Міллер, Дж. Кларк, А. Нараянан, Дж. А. Кролл, Е. В. Фелтен, І. Стюарт, Д. Ілі, А. Замятін, С. Вернер, М. Ф. Торшизі та В. Дж. Ноттенбелт, С. Ма, В. Хао, Н.-Н. Дай, С. Ченг, Р. Йі та Т. Ван, К. Чен, К. Чен, Дж. Ю, В. Ву та Д. Ву, Н. Дрлевич, Д. А. Аранда, Ст. Станчев, М. Саад, Дж. Сполдінг, Л. Нджілла, К. Камхуа, С. Шетті, Д. Д. Ньянг, Н.Т. Тонг, В.Л. Лем'є, Х. Мучліс Газалі, К.М. Хафіз Бін Че Ісмаїл, Т. Амбоала та інші.

Проблемами захисту споживачів та інвесторів, цілісності ринку, ухилення від сплати податків, відмивання грошей і фінансування тероризму займаються такі зарубіжні науковці та аналітики як, Е. С. Прасад, К. Рогофф, К. Граф фон Люкнер, Кармен М. Рейнхарт, Р. Чу, А. Ібрагімі, А. Беса. Економетричним моделям визначення ризику присвячені наукові роботи вітчизняних вчених Б. Грабовецького, Ю. Шевцової, П. Берзіна, О. Шишкіної, О. Кузьменка, Г. Яровенка, Л. Долінського, О. Бережного, С. Дмитрова, О. Меренкової, Т. Медвідь, О. Ващенко, Ж. Андрійченко, Н. Внукової.

Теоретичні й практичні питання визначення ризику як економічного феномена, гносеології, класифікації та методів вимірювання ризику присвятили свої праці такі класики, як В. Варкалло, О. Ланге, Я. Данґель, Т. Бачкаї, Д. Месен і Д. Мико, Дж. фон Нейман, О. Моргенштерн, В. Меклінг, М. Дженсен, К. Френч, Дж. Гелбрайт, Н. Й. Тетенс, Фр. Найт, А. Віллетт, К. Маркс.

Проблеми сутності цифрових активів та їх таксономії досліджують вітчизняні й зарубіжні вчені. На сьогодні більшість вчених виділяє п’ять груп

понять, що лежать у площині визначення цифрових активів: перша група – цифрові активи (Дж. П. Бантінкс, Г. Х. Грей, Е. Харбінджа, А. Кудь та І. Пипенко, М. Д. Уокер); друга – активи даних (Р.Е. Петерсон, Лі Яксіонг та Ні Шань, Ши Ай-сінь, Гао Дін, Се Цзін, Цінь Ронгшен); третя – цифрова валюта або криптовалюта (О. Велика, Д. Ленц, Дж. Оуенс, С. Вінк); четверта – токени (З. Пестовська, Б. Хайнс, Б. Москвін), п’ята – віртуальні активи (Т. Гудима, О. Черних).

Певні науковці сконцентрувались на ризиках та моделях впровадження центральних валют центральних банків. Один з напрямків це, як центральні банки повинні створювати роздрібні цифрові гроші і чи бажано, щоб CBDC замінили фізичну готівку досліджують Т. Кейстер, Д. Санчес, М.К. Бруннермаєр, Х. Джеймс і Дж. П. Ландау. Про системні наслідки впровадження такої валюти і про те, як впоратися з пов'язаними з ними ризиками та нестабільністю, які вони можуть спричинити присвячені наукові дослідження таких науковців як Ф. Аллен, Х. Гу, Дж. Ю. Бруннермайер, Х. Джеймс та Дж. П. Ландау, Д. Ніпельт, Дж. Фернандес-Віллаверде, Д. Санчес, Л. Шиллінг та Х. Уліг, А. Венеріс, А. Парк, Ф. Лонг та П. Пурі, Н. Почер, А. Венеріс, Т. Єфименко, О. Любіч, Ю. Коваленко, В. Міщенко, С. Науменкова, С. Міщенко, С. Аржевітін, А. Александров, А. Колдовский. Так, на даному етапі розвитку наукової думки ми можемо спостерігати «змішування» понятійного апарату та наявні теоретичні суперечності.

Не заперечуючи значущість наукових праць згаданих дослідників, слід відзначити брак комплексних досліджень, спрямованих на аналіз проблем запобігання та протидії легалізації (відмиванню) доходів, отриманих незаконним шляхом із використанням цифрових активів. Зокрема, недостатньо уваги приділяється оцінці ризиковості цифрових активів та їх гібридів, що застосовуються у схемах легалізації незаконних доходів.

Причини й наслідки використання віртуальних активів у відмиванні злочинних коштів досліджуються досить обмежено, попри те, що оцінка ризиків

нових інноваційних продуктів є невід'ємною складовою Національної оцінки ризиків легалізації злочинних доходів. Цей напрям також рекомендовано міжнародними організаціями, які займаються регулюванням і розвитком світової економіки.

Отже, дослідження теоретичних та організаційно-правових засад управління ризиками використання цифрових активів у злочинних схемах відмивання коштів, запобігання легалізації незаконних доходів у фінансовому секторі, а також розроблення пропозицій щодо вдосконалення цих процесів є актуальним як з наукової, так і з практичної точки зору.

Зв'язок з науковими програмами, планами, темами.

Дисертаційну роботу виконано в рамках науково-дослідних тем ДННУ «Академія фінансового управління»: «Розробка науково-методичних підходів до оцінки і управління ризиком використання в Україні віртуальних активів в схемах легалізації злочинних доходів та розмиванні бази оподаткування» (номер державної реєстрації 0121U110027); «Впровадження ризик-орієнтованого підходу на базі застосування AML в діяльність державних банків щодо використання віртуальних активів та цифрових валют центральних банків в періоди дії воєнного стану та відновлення економіки України» (номер державної реєстрації 0123U101613). У межах цих тем автором окреслено шляхи легалізації ринку віртуальних активів в Україні. Визначено напрями імплементації світового досвіду, передусім міжнародних законодавчих норм регулювання обігу цифрових активів з метою запобігання їх використанню в антилегалізаційних операціях та іншій злочинній діяльності.

Матеріали дисертаційної роботи використанні при підготовці науково-дослідної роботи «Удосконалення механізму фінансування системи освіти як чинника розвитку людського капталу та його роль у повоєнному відновленні України» (номер державної реєстрації 0124U001973), в частині обґрунтування впливу рівня фінансово-цифрової грамотності на розвиток людського капталу, а також наявності взаємозв'язку рівня фінансово-цифрової грамотності та ризиків

операцій на ринку цифрових активів. Матеріали дослідження щодо національних пріоритетів у сфері розвитку цифрових фінансів з обґрунтуванням необхідності колаборації обігу цифрових валют центральних банків та віртуальних активів для пом'якшення загроз, вразливостей та ризиків використання суб'єктів фінансово-банківського сектору та ринку віртуальних активів з метою відмивання коштів, отриманих злочинним шляхом, та фінансування тероризму використані в науковому проєкті Національного інституту стратегічних досліджень «Формування засад національно укоріненої стійкості та безпеки економічного розвитку України в умовах гібридної системи «мир-війна» (2 етап - Обґрунтування механізмів практичного забезпечення економічної стійкості та безпеки на засадах національної укоріненості економічного розвитку) (номер державної реєстрації 0124U001680).

Мета і завдання дослідження. Метою дисертаційної роботи є поглиблення теоретико-методологічних засад оцінки та управління ризиками, пов'язаними з використанням цифрових активів у фінансових та економічних злочинах, зокрема в процесах легалізації доходів, отриманих злочинним шляхом, та фінансування тероризму, а також розроблення практичних рекомендацій щодо впровадження ризик-орієнтованого підходу до державного регулювання цієї сфери.

Досягнення поставленої мети обумовило необхідність розв'язання таких завдань наукового і прикладного характеру:

– розглянути теоретичні підходи до поняття «ризик» за різними класичними економічними теоріями та запропонувати шляхи їхньої трансформації до обігу цифрових активів;

– визначити основні чинники ризик-орієнтованого підходу, методи ідентифікації ризиків, систематизувати процеси управління ризиками та

розмежувати поняття ризику і невизначеності найтівської теорії ризику через технічну оцінку ризику;

– розкрити засади оновлення міжнародних та європейських стандартів з розвитком функціонування ринку віртуальних активів та розробки та тестування центральних валют центральних банків;

– надати визначення та розкрити теоретичні підходи до поняття «цифрові активи» через розробку за їхньою сутністю відповідної таксономії;

– розробити критерії використання цифрових активів у ВК через аналіз «червоних прапорців», як складової ризик-орієнтованого підходу, для трансакцій з ВА.

– розкрити механізм оцінки цифрових активів, їхнього використання у легалізаційних трансакціях, застосовуючи науково-методичні підходи до визначення ризику та на підставі сучасних методів науково-технічного прогнозування;

– розробити на основі досліджень корупційних діянь з використанням криптовалютних операцій пропозиції зі зниження ризиків декларування цифрових активів як способу легалізації доходів, отриманих злочинним шляхом;

– здійснити аналіз міжнародного, європейського та національного законодавчо-нормативного забезпечення накладання санкцій на віртуальні активи та надати пропозиції з протидії уникнення санкцій для забезпечення впровадження рекомендацій FATF;

– розробити шляхи імплементації міжнародних стандартів ПВК/ФТ у розвиток діяльності національного ринку віртуальних активів та національної

цифрової валюти, взаємодії з фінансовим та фондовим ринками, застосовуючи найкращі міжнародні практики;

– проаналізувати напрямки впровадження е-гривні з метою підвищення ефективності функціонування Національної ПВК/ФТ в умовах обігу цифрових активів шляхом застосування ризик-орієнтованого підходу.

– поглибити науково-методичні засади бухгалтерського обліку операцій з цифровими активами шляхом уточнення їх економіко-правової природи, визначення підходів до оцінки легальності та ліквідності цифрових активів, а також впровадження ризик-орієнтованого підходу у сфері протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ), з урахуванням фіскально-правових вимог і обліково-звітних стандартів ЄС;

– розробити науково обґрунтовані пропозиції щодо застосування сучасних технологічних рішень в управлінні національних державних наглядових органів, професійних операторів та учасників ринку віртуальних і цифрових активів з метою вдосконалення процесів оцінки ризиків у сфері ПВК/ФТ і забезпечення ефективного подання звітності;

– обґрунтувати та розробити науково-методичні підходи до впровадження освітніх ініціатив у сфері фінансової та цифрової інклюзії як інструменту мінімізації ризиків ВК/ФТ у функціонуванні крипторинку України.

Об'єктом дослідження є фінансові процеси, що виникають у процесі обігу цифрових активів у контексті протидії відмиванню доходів, отриманих злочинним шляхом, та фінансуванню тероризму

Предметом дослідження є теоретико-методологічні засади та прикладні аспекти ризик-орієнтованого підходу до регулювання обігу цифрових активів у сфері протидії відмиванню коштів і фінансуванню тероризму, з урахуванням оцінки та управління фінансовими ризиками, пов'язаними з їх використанням.

Методи дослідження. Для досягнення поставленої мети використано загальнонаукові та спеціальні методи дослідження: діалектичний метод пізнання, що забезпечує аналіз фінансових явищ та процесів у їх розвитку,

взаємозв’язку та взаємозалежності; метод експертних оцінок; такі методи оцінки ризику як кваліфікація і квантифікація, Баєсові мережі; метод аналізу і синтезу; економіко-статистичні методи. Дослідження сутності ризик-орієнтованого підходу до обігу цифрових активів у сфері ПВК/ФТ, його форм та методів здійснено з використанням методів зіставлення, групування, типологізації, графічного аналізу. Методи системного узагальнення використані при дослідженні механізму оцінки й управління ризиком. Методи економіко-математичного моделювання застосовані при обробці даних для аналізу та оцінювання учасників обігу криптоактивів. Методи експертних оцінок і прогнозів використано для обґрунтування доцільності застосування оцінки значущості критеріїв ризику використання віртуальних активів у злочинних схемах і застосування окремих критеріїв ризику відповідно до Керівництва щодо ризик-орієнтованого підходу до обороту віртуальних активів і діяльності постачальників послуг, пов’язаних з оборотом віртуальних активів, розробленого для ефективного впровадження 40 Рекомендацій FATF, а саме оновленої 15 Рекомендації FATF. Баєсові мережі дозволяють прогнозувати ризики ВК/ФТ на основі історичних даних та ймовірнісних оцінок. Гравітаційне моделювання допомагає аналізувати рух нелегальних коштів у глобальному масштабі, оцінюючи взаємодію між фінансовими суб’єктами.

Використання методу SEER (System for Evolutions and Review) та застосування статистичних методів (метрики Мінковського) дозволяє визначити рівень ризику операцій із криптовалютами. Метод логічного узагальнення застосовано для формування висновків.

Інформаційною базою дослідження є: закони України, постанови Кабінету Міністрів України, розпорядження і статистичні дані Державної служби фінансового моніторингу, Національного антикорупційного бюро України, Національного агентства з питань запобігання корупції, Національної поліції України, Національного банку України, ПФР Республіки Казахстан; керівництва, пояснювальні записки та матеріали Міжнародної групи з протидії

відмиванню брудних грошей (FATF), Обраного комітету експертів Ради Європи з оцінки заходів боротьби з відмиванням грошей (MONEYVAL), Робочої групи при Європейській комісії та Раді Європи, угоди Базельського комітету з банківського нагляду (Basel I-IV), Управління ООН з наркотиків і злочинності (UNODC), Директиви та Регламенти ЄС, що входять до Стратегічного пакету документів щодо цифрових активів та обміну інформацією; Рішення щодо накладання санкцій на осіб рф, рб щодо військової агресії в Україні; наукові праці вітчизняних і зарубіжних учених, дослідницькі та аналітичні матеріали, Інтернет-ресурси.

Наукова новизна одержаних результатів полягає у вирішенні наукової проблеми із поглиблення теоретико-методологічних засад, опрацювання методичних підходів та рекомендацій з розробки та впровадження ризик-орієнтованого підходу до регулювання обороту цифрових активів у сфері ПВК/ФТ. Найбільш вагомі наукові результати дослідження, які виносяться на захист, полягають в такому:

уперше:

– надано авторське визначення сутності ризик-орієнтованого підходу до регулювання обігу цифрових активів у сфері ПВК/ФТ, що полягає в забезпеченні систематичної оцінки ризиків використання цифрових активів у легалізаційних операціях та операціях маніпулювання віртуальними активами уповноваженими державними органами, учасниками обігу цифрових активів і особами, які обслуговують операції з ними, а також застосуванні сукупності методів фінансового контролю за їхнім обігом з метою виявлення операцій з легалізації (відмивання) доходів, ухилення від сплати податків, корупційної діяльності, фінансування тероризму, обходження санкцій, шахрайства для забезпечення фінансової цілісності та резильєнтності економічної системи, що уможливлює формування цілісного підходу до регулювання віртуальних активів в сфері ПВК/ФТ;

– класичні теорії ризику застосовано для розроблення поетапного механізму оцінки ризиків використання цифрових активів у відмиванні коштів, отриманих злочинним шляхом, та фінансуванні тероризму та злочинній діяльності загалом із метою впровадження ризик-орієнтованого підходу в діяльність Національної системи ПВК/ФТ щодо обігу таких активів;

– доведено, що еволюція дефініції «цифрові активи» відображає постійну цифрову трансформацію і зростаючу важливість цифрової власності та цінностей у глобальній економіці, що спричиняє юридичну визначеність цифрових активів та сприяє розвитку регуляторної бази з захисту учасників ринку;

– запропоновано інноваційний механізм процедур ідентифікації, верифікації, оцінки та управління ризиками у сфері ПВК/ФТ через інтегрований підхід до обмінних операцій криптоактивів із використанням центральних валют центральних банків, що забезпечує оптимізацію витрат на криптоактиви й оцінку ризиків завдяки прозорій ідентифікації учасників та підвищення рівня безпеки за підвищення прозорості ідентифікаційних даних, що сприяє зменшенню шахрайських операцій та фінансових злочинів, створюючи більш надійну інфраструктуру для використання криптоактивів;

– запропоновано впровадження в державне регулювання децентралізованих фінансових криптоплатформ із вбудованими механізмами ідентифікації та звітності обов’язкових регулярних процедур фінансового і технічного аудитів з виявлення вразливостей як превентивного заходу запобігання кіберзлочинності та шахрайству;

– розроблено методичні підходи до визначення ризику використання віртуальних активів у злочинних схемах відмивання коштів, отриманих злочинним шляхом, та фінансування тероризму за методом експертних оцінок, а саме встановлення важливості критеріїв, що визначають величину ризику, та вирахування за цими критеріями інтегрального показника ризику використання віртуальних активів у легалізаційних операціях та відстеженні руху нелегальних

коштів у глобальному масштабі, оцінюючи взаємодію фінансових суб'єктів. Впровадження оцінки віртуальних активів відповідно до ризик-орієнтованого підходу у сфері ПВК/ФТ сприятиме оптимізації ресурсів залежно від ступеня ризику використання цифрових активів у злочинних операціях, управління цим ризиком і зниження зусиль на здійснення процедур комплаєнсу та ПВК/ФТ легальних прозорих операцій з цифровими активами;

удосконалено:

– визначення терміна «цифрові активи» на основі їхньої таксономії, що доповнює національне законодавство міжнародною термінологією для кращого розуміння сутності явищ у контексті «віртуальних активів» та «цифрових валют центрального банку»;

– обґрунтування ефективності розроблення секторальної оцінки ризику використання цифрових активів у відмиванні коштів, отриманих злочинним шляхом та фінансуванні тероризму з розмежуванням понять ризику і невизначеності відповідності до методологічних рекомендацій МВФ та Світового банку з проведення оцінки ризиків у сфері ПВК/ФТ через критерії загроз, вразливостей та наслідків у співвідношенні з національною оцінкою ризиків;

– методологічні підходи до оцінки ризиків у сфері ПВК/ФТ шляхом розширення критеріїв визначення високоризикових фінансових інструментів, що використовуються в легалізації коштів, стосовно переліку наявних ризикових операцій шляхом включення цифрових активів, а саме визначення криптоактивів закритих блокчейнів як інструменту на пред'явника, подібного до готівки для розроблення Програми комплаєнсу та ПВК/ФТ суб'єктів фінансового моніторингу;

– наукові підходи до використання цифрових активів відносно фінансових інструментів у періоди фінансово-економічних криз, воєнних дій та забезпечення сталого розвитку завдяки легалізації національного ринку

віртуальних активів та впровадженню е-гривні, що може прискорити процес зменшення тіньової складової економіки, сприяти побудові прозорої інфраструктури обігу цифрових активів, розвитку міжнародних розрахунків, залученню інвестицій та міжнародній інтеграції шляхом упровадження вимог і рекомендацій європейського та міжнародного законодавства;

– формування механізмів зниження ризиків використання обігу цифрових активів у схемах легалізації (відмивання) доходів, отриманих злочинним шляхом, корупційній діяльності та при уникненні (обході) міжнародних і національних санкцій, розмиванні бази оподаткування завдяки впровадженню інформаційного обміну щодо звітності про сплату податків за операціями з цифровими активами, аналізу декларування цифрових активів, запровадження процедур комплаєнсу та ПВК/ФТ учасниками і професійними операторами ринку цифрових активів, наглядовими та правоохоронними органами, що сприятиме розбудові інфраструктури обігу цифрових активів та забезпеченню цифрової стійкості їхнього обороту за системою та процедурами ПВК/ФТ;

дістали подальшого розвитку:

– застосування новітніх методів управління та механізмів публічно-приватного партнерства в розвитку функціонування ринку віртуальних активів та обороту цифрових валют центральних банків, його взаємодії з фінансовим ринком, розвитку інновацій цифрової економіки та забезпеченні економічної безпеки на національному і глобальному рівнях, що оптимізує розподіл ресурсів для більш швидкого та ефективного реагування на загрози і виклики в сфері ПВК/ФТ;

– аргументація необхідності впровадження в освітній процес інтегрованої моделі цифрової та фінансової інклюзії, які поєднують освітні програми з використанням навчальних ліцензій з програмними продуктами оцінки обороту криптоактивів – аналітики для аналізу кейсів злочинної діяльності, оцінки ризиків і моделювання наслідків за такими ризиками із застосуванням

машинного навчання та штучного інтелекту. Такий підхід забезпечує оптимізацію використання ресурсів у сфері освіти, сприяє створенню безпечного цифрового середовища та формуванню високого рівня цифрової компетентності як школярів, так і дорослих, що відповідає сучасним викликам інформаційного суспільства.

Практичне значення одержаних результатів. Наукові результати дисертаційної роботи знайшли своє практичне застосування, що підтверджується відповідними довідками про впровадження, а саме:

– в частині визначення критеріїв та оцінці ризиків використання віртуальних активів в схемах відмивання коштів, отриманих злочинним шляхом, запровадження прозорого обігу віртуальних активів шляхом легалізації діяльності ринку віртуальних активів, запровадження ліцензування та пруденційного нагляду щодо професійних операторів ринку віртуальних активів, використані в аналітичній та законотворчій роботі *Національної комісії з цінних паперів та фондового ринку України*, а саме в обговорюванні пропозицій щодо зменшення ризиків та загроз відповідно до Звіту про проведення Національної оцінки ризиків, підготовленої з урахуванням міжнародних стандартів і відповідно до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та Стратегії розвитку фінансового сектору України до 2025 року, що мали відображення в зазначеному документі, а також визначення шляхів розбудови обігу цифрових активів в цілому (довідка № 04/6025 від 07.03.2024);

– в обговореннях вдосконалення національного законодавства щодо впровадження *санкцій Робочої групи при Раді національної безпеки і оборони України* щодо застосування спеціальних економічних та інших обмежувальних заходів (санкцій) до постачальників послуг, пов’язаних з оборотом віртуальних активів, які співпрацюють із банками російської федерації та республіки білорусь. Також були розглянуті представлені матеріали Розділу дисертаційної

роботи «Санкційна політика як інструмент забезпечення фінансової та цифрової безпеки» щодо обходження санкцій з використанням криптоактивів та неліцензованих (незареєстрованих) обмінників криптовалют, розроблені пропозиції щодо підвищення впливу на впровадження і ефективність міжнародних санкцій, необхідності прийняття швидких та оптимальних дій щодо легалізації діяльності крипторинку та впровадження ризик-орієнтованого підходу в питаннях взаємодії операторів крипто та фінансового ринку в Україні на основі аналізу схем обходу міжнародних санкцій, застосованих до банків, компаній та фізичних осіб російської федерації. Щодо стимулювання сталого економічного зростання через розвиток діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів в Україні в відповідному розділі дисертації обґрунтовано, що заморожені та повернуті віртуальні активи, які знаходяться під санкціями міжнародних організацій, іноземних держав та України, накладені на суб'єкти рф та рб є джерелом наповнення державного бюджету Україні, ресурсами для повоєнного відновлення України та справедливою компенсацією скоєних злочинів проти українського народу (довідка 4524/14-15/2-24 від 26.12.2024);

– в частині визначення критеріїв та оцінці ризиків використання віртуальних активів в схемах корупційних злочинів, запровадження прозорого обігу віртуальних активів шляхом легалізації діяльності ринку віртуальних активів, запровадження процедур підтвердження справжності задекларованих віртуальних активів декларантами, проведення розслідувань *Національним антикорупційним бюро України* корупційних злочинів з використанням програмних продуктів аналітичних компаній дослідження операцій в блокчейнах та збору доказів (артефактів) використання віртуальних активів в злочинній діяльності (довідка б/н від 12.01.2024р.);

– в частині типологізації та оцінці ризиків використання віртуальних активів в схемах відмивання коштів, отриманих злочинним шляхом, запровадження прозорого обігу цифрових активів шляхом легалізації обігу таких активів,

впровадження пруденційного нагляду щодо професійних операторів ринку віртуальних активів та обігу цифрових валют центральних банків, використані в розробці та проведення тренінгів для представників правоохоронної системи та державних регуляторів проєкту *UNODC Global Program on Cybercrime*. Наведена аргументація щодо підвищення ефективності функціювання Національної системи боротьби легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення використана в проведенні в рамках проєкту освітніх заходах за участю автора (UNODC Certificate dated February, 22, 2024)

– в частині термінології та таксономії цифрових активів, міжнародних та європейських стандартів щодо ПВК/ФТ в операціях з цифровими активами та діяльності постачальників послуг, пов'язаних з обігом віртуальних активів та оцінки ризиків використання віртуальних активів у схемах відмивання грошей, запровадження прозорого обігу цифрових активів шляхом легалізації обігу таких активів, запровадження пруденційного нагляду за професійними операторами ринку віртуальних активів та обігом цифрових валют центральних банків, що використовуються в поточній діяльності *Міністерства цифрового розвитку, інновацій та аерокосмічної промисловості Республіки Казахстан*, а саме при підготовці та реалізації у співпраці з *Департаментом по боротьбі з організованою злочинністю та відмиванням незаконних грошей Управління ООН з наркотиків і злочинності (UNODC)* для представників правоохоронної системи, держава регулятори, банки, фінансові установи та криптоіндустрія Республіки Казахстан міжнародного тренінгу «Ризики, пов'язані з передовими технологіями блокчейн: DeFi, Smart contracts, NFT» в Астані, Республіка Казахстан. Наведено аргументи щодо вдосконалення національного законодавства відповідно до таксономії цифрових активів європейського законодавства з метою підвищення прозорості співпраці представників органів державного нагляду та представників криптобізнесу та банків країн Центральної Азії з іноземними, в тому числі європейськими партнерами (Ministry of Digital

Development, Innovations and Aerospace Industry of the Republic of Kazakhstan Certificate dated 18.04.2024);

– в частині розроблення підходів до впровадження оновлених Рекомендацій Міжнародної групи з протидії відмиванню брудних грошей (FATF), а саме ризик-орієнтованого підходу до обігу віртуальних активів і діяльності провайдерів послуг із віртуальними активами, взаємодії шляхом розробки та впровадження «Правила подорожей» (16 Рекомендація FATF) для фінансового сектору та ринку віртуальних активів щодо зменшення ризику використання їх у злочинних операціях (зокрема, ідентифікації й верифікації клієнтів, визначення інформації про відкриті ключі ініціаторів трансакцій із віртуальними активами та їх бенефіціарних власників), у законодавство України та практику Національної системи протидії відмиванню коштів, одержаних злочинним шляхом, та фінансуванню тероризму (ПВК/ФТ), спрямовані на підвищення ефективності процедур взаємодії представників правоохоронної та судової системи, державних наглядових органів і учасників ринку віртуальних активів шляхом цифровізації цих процесів. Наведена аргументація щодо оптимізації процедур збору статистичних даних діяльності правоохоронної, судової, державної наглядової систем та операторів ринку віртуальних активів сприятиме загальному прогресу оцінки ефективності заходів у сфері ПВК/ФТ (33 Рекомендація FATF). Результати проведеного дослідження дозволяють сформулювати рекомендації *Комітету цифрової трансформації Верховної Ради України* щодо розвитку ринку віртуальних активів в Україні, впровадження міжнародних стандартів FATF та ЄС у діяльність провайдерів послуг, пов'язаних з віртуальними активами, а також сприяти налагодженню співпраці між бізнесом, законодавчими й виконавчими органами, правоохоронними органами та громадянським суспільством на національному і глобальному рівнях (довідка 202д9/9-2024/259462 від 21.11.2024р.);

– в частині антикорупційної політики щодо декларування цифрових активів в операціях з цифровими активами та оцінці ризиків використання віртуальних

активів в схемах відмивання коштів, отриманих злочинним шляхом, запровадження прозорого обігу цифрових активів шляхом легалізації обігу таких активів та використання цифрових активів для підвищення прозорості формування місцевих бюджетів, особливо їх витратної складової, впровадження пруденційного нагляду обігу цифрових активів та методологічних підходів до оподаткування операцій з віртуальними активами. Наведена аргументація щодо вдосконалення національного законодавства у відповідність до таксономії цифрових активів європейського законодавства для зростання прозорості співпраці представників державних наглядових органів та представників криптобізнесу регіонального рівня *Кременчуцької міської ради Кременчуцького району Полтавської області України* (довідка від 18.06.2024р.);

– пропозиції по впровадженню ризик-орієнтованого підходу, спрямованого на підвищення фінансової безпеки в процесі антикризового регулювання та розвитку негрошових методів фінансування економіки було використано в роботі *Інституту економіко-правових досліджень НАН України ім. Мамутова* при викладанні наукових дисциплін для аспірантів в рамках дисципліни «Актуальні питання банківського права»; при проведенні спільних наукових досліджень з питань обігу цифрової валюти центрального банку, зокрема щодо вибору її оптимальної моделі для України; при формуванні спільних пропозицій для органів державної влади по застосуванню секторальних спеціальних економічних та інших обмежувальних заходів (санкцій) до постачальників послуг, пов'язаних з обігом віртуальних активів, які співпрацюють із банками російської федерації та республіки білорусь (довідка 299/32/25 від 21.01.2025);

– при підготовці науково-дослідної роботи *ДНУ «Інститут освітньої аналітики»* «Удосконалення механізму фінансування системи освіти як чинника розвитку людського капталу та його роль у повоєнному відновленні України» (номер державної реєстрації 0124U001973), в частині обґрунтування впливу рівня фінансово-цифрової грамотності на розвиток людського капталу, а також наявності взаємозв’язку рівня фінансово-цифрової грамотності та ризиків

операцій на ринку цифрових активів. В розділі дисертації «Кластерно-порівняльний аналіз ризиків використання цифрових активів в злочинній діяльності» обґрунтовано, що низький рівень фінансово-цифрової грамотності зумовлює ризик інвестицій в шахрайські проєкти; панічний продаж/купівлю цифрових активів через нерозуміння ринкової волатильності ринку; ризик втрати персональних даних; ризик стати жертвами фальшивих криптовалютних платформ або ненадійних криптовалютних гаманців, що призводить до втрати коштів. Доведено, що підвищення рівня фінансово-цифрової грамотності дозволяє людям краще розуміти ризики операцій з цифровими активами та загалом є ключовими елементами у розвитку людського капіталу, оскільки вони сприяють економічній активності, підвищенню кваліфікації, розвитку підприємництва та інновацій, а також захищають людей від ризиків (довідка від 18.06.2024р.);

– результати дослідження застосовуються в освітньому процесі *ДВНЗ «Чернівецький торговельно-економічний інститут Державного торговельно-економічного університету»* при викладанні дисциплін «Фінансовий ринок», «Аналіз фінансових ринків», «Фінансовий моніторинг», «Державна фінансова стратегія» та «Державний фінансовий контроль». Це стосується студентів, які здобувають освітній ступінь «бакалавр» за напрямом підготовки освітньої програми «Фінанси, банківська справа, страхування та фондовий ринок» та студентів, які здобувають освітній ступінь «магістр» за напрямом підготовки освітньої програми «Фінансовий моніторинг та податковий менеджмент» спеціалізації 072 «Фінанси, банківська справа, страхування та фондовий ринок» (довідка від 18.12.2024).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою роботою. Наукові результати, які виносяться на захист, одержані автором самостійно і викладені в опублікованих працях. З наукових праць, опублікованих у співавторстві, в роботі використано лише ті ідеї і положення,

які є результатом власних розробок автора.

Апробація результатів дослідження. Основні положення дисертаційної роботи отримали апробацію на міжнародних і всеукраїнських наукових та науково-практичних конференціях, зокрема: І Міжнародна науково-практична конференція (Херсон, 08-11 вересня 2021 р.); І Міжнародна науково-практична інтернет-конференція «Вплив пандемії COVID-19 на розвиток сучасного світу: загрози та можливості» (Дніпро, 9-10 вересня 2021р.); ІІ Міжнародна науково-практична конференція Multidisziplinäre forschung: perspektiven, probleme und muster (Відень, 26 листопада 2021р.); Міжвідомча науково-практична конференція «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, серпень, 2022р.); Всеукраїнська науково-практична інтернет-конференція «Актуальні питання бухгалтерського обліку, аналізу, аудиту та оподаткування в умовах воєнного стану і післявоєнного відновлення» (м. Київ, 15 червня 2023р.); Міжнародна науково-практична конференція «Фіскальна та монетарна безпека національної економіки в умовах глобальних викликів і загроз» (м. Київ, 31 жовтня 2023р.); Науково-практична конференція аспірантів та докторантів «Забезпечення резилієнтності економіки України в умовах військової агресії та повоєнного відновлення» (м. Київ, 12 грудня 2023р.); Академічні читання “Наукова спадщина Михайла Туган-Барановського для відбудови України”, ДУ «Інститут економіки та прогнозування НАН України», (м. Київ, 18 січня 2024р.); Перший Міжнародний фінансовий форум «Модерні фінанси: глобальні виклики і сучасні тренди». (м. Тернопіль, 19-23 червня 2024р.); ІІ Науково-практична конференція аспірантів та докторантів «Забезпечення резилієнтності економіки України в умовах військової агресії та повоєнного відновлення» (м. Київ, 17 липня 2024 р.); Х Міжнародна науково-практична конференція «Актуальні проблеми управління соціально-економічними системами» (м. Луцьк, 6 грудня 2024 р.); ІІ Міжнародна науково-практична конференція «Економічна аналітика: сучасні реалії та прогностичні можливості» (м. Київ, 24 січня 2025р.); Міжнародна

науково-практична конференція «Наукова спадщина Михайла Туган-Барановського як концептуальне підґрунтя суспільного розвитку» (м. Київ, 29 січня 2025р.).

Публікації. Основні положення та результати дисертації опубліковано в **33** працях, серед яких: **20** статей у періодичних фахових наукових виданнях, включених до міжнародних наукометричних баз, з яких 3 статті у наукових виданнях, що включені до наукометричних баз даних Scopus / Web of Science, 1 стаття з яких в іноземному виданні, та **13** публікацій апробаційного характеру. Загальний обсяг публікацій, що належить автору, – **15** друк. арк.

Структура роботи обумовлена метою та завданнями дослідження, його об'єктом та предметом, складається із вступу, чотирьох розділів, які містять тринадцять підрозділів, висновків, списку використаних джерел (**515** найменувань) і додатків (2,83 друк. арк.). Робота містить **37** таблиці, **32** рисунки, **27** формул. Обсяг основного тексту дисертації складає **18,08** друк. арк., повний обсяг – **26** друк. арк.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В СФЕРІ ПВК/ФТ ДО РЕГУЛЮВАННЯ ОБОРОТУ ЦИФРОВИХ АКТИВІВ

1.1. Ризик-орієнтований підхід як модель ефективного регулювання

Поняття ризику є відносно новим для української економічної науки. Інтерес до питання ризику в економічній діяльності зріс у 90-х роках XX ст., коли трансформаційні процеси зумовили усвідомлення ризику як чинника, що може зменшити прибуток або призвести до його втрати. У цей період теорія ризику почала активно розвиватися та набувати застосування на практиці в умовах становлення ринкових відносин. Хоча ризик завжди супроводжував будь-яку людську діяльність, зокрема економічну, акценти на його різних аспектах змінювалися залежно від економічних умов і особливостей системи.

Поняття ризику відоме з давніх часів, і можна сказати, що воно виникло одночасно з появою людини. Однак як самостійна наука теорія ризику сформувалася відносно нещодавно. Раніше вона існувала як складова інших теорій. Серед науковців нині тривають дискусії щодо того, до якої саме галузі належить теорія ризику.

Наприклад, на думку польського професора Вітольда Варкалло, термін «ризик» спочатку став науковим у межах теорії страхування, і лише пізніше, у XIX–XX ст., його почали використовувати в економічній теорії [1]. Чеський теоретик Ярослав Данґель вважає, що поняття «ризик» походить із загальнонаукових дисциплін, таких як філософія та економіка [2, с. 16]. Варто

зазначити, що хоча термін «ризик» має тривалу історію, активне дослідження різних його аспектів почалося наприкінці XIX — на початку XX ст.

Представники німецької школи теорії ризику, спираючись на розроблену американськими математиками Дж. фон Нейманом і О. Моргенштерном теорію корисності й використовуючи теорію розпливчастих множин, досягли значних результатів стосовно оцінки ризику з використанням теорії нечітких множин [3, с. 115].

Американські економісти-теоретики Вільям Меклінг та Майкл Дженсен – представники сучасного неоінституціоналізму – вдаються до теорії ризику, розглядаючи розподіл прав контролю між нейтральними, схильними і не схильними до ризику індивідами [4]. Професор Дартмутського коледжу (США) Кеннет Френч вивчає проблематику практичної оцінки очікуваної вартості дохідності цінних паперів, вартості капіталу, питання дивідендної політики і структури капіталу [5, с. 48].

Центральна концепція теорії очікуваної корисності фон Неймана – Моргенштерна пропонує, що раціональний суб'єкт за невизначеності обирає альтернативу з найбільшою очікуваною корисністю [3]. Це означає зважування вигоди кожного можливого результату на ймовірність його настання. Класична економічна інтерпретація припускає, що люди або компанії приймають рішення, максимізуючи очікувану віддачу з урахуванням свого ставлення до ризику. В контексті ризик-орієнтованого підходу ПВК/ФТ ця теорія надає корисну рамку для аналізу того, як різні учасники діяльності – і легальні, і нелегальні – пристосовують свою поведінку, реагуючи на стимули й загрози.

З точки зору злочинця, що займається ВК, застосування теорії очікуваної корисності допомагає змоделювати рішення доцільності здійснювати цю фінансову операцію, якщо є ризик бути викритим. Раціональний підхід означає зіставлення очікуваного прибутку від успішного відмивання з імовірністю викриття та очікуваним покаранням (штрафи, конфіскація, ув'язнення). Класична модель економіки злочинів, розвинена Г. Беккером [15], саме й трактує

злочинця як раціонального агента, що вчиняє злочин, якщо очікувана вигода перевищує очікувані витрати. У випадку появи нових технологій, таких як блокчейн, цей розрахунок суттєво змінюється. Децентралізовані технології можуть збільшувати очікувану корисність злочину, знижуючи ризик бути спійманим або витрати на маскування слідів.

Дослідження, проведене Мюллером та ін. (2020) [18], побудувало функцію очікуваної корисності відмивання коштів з урахуванням специфіки блокчейну. Висновки показали, що блокчейн-технології загалом підвищують очікувану корисність ВК для злочинців, тобто роблять таку діяльність привабливішою з точки зору раціонального вибору. Причини – анонімність або псевдоанонімність трансакцій, можливість швидко переміщати великі суми за межі національних юрисдикцій, відсутність посередників, які могли б виявити підозрілу активність. Наприклад, якщо раніше злочинець міг оцінювати ймовірність замороження коштів у банку як досить високу, то переведення цих коштів у криптовалюту та використання міксерів знижує цю ймовірність, тим самим підвищуючи очікуваний виграш.

Така раціональна модель поведінки має дві важливі імплікації. По-перше, регуляторам слід впливати на компоненти цього розрахунку, знижуючи очікувану корисність злочину. Це досягається як підвищенням шансів викриття (наприклад, упровадження потужної аналітики блокчейну і вимог прозорості для бірж), так і збільшенням потенційних втрат для злочинця (суворіші санкції, конфіскація криптоактивів, санкційні списки криптогаманців). Необхідно змістити «систему рівнянь» так, щоб ризики перевищили вигоди, роблячи відмивання через цифрові активи менш раціонально вигідним. Фактично це і є втіленням ризик-орієнтованого підходу: скеровувати ресурси в ті сфери, де можна найсуттєвіше зменшити очікувану корисність фінансового злочину.

По-друге, модель очікуваної корисності дає лише нормативний погляд – тобто як повинні діяти раціональні особи. У реальності поведінка може відхилятися від раціональної через обмежену інформацію, психологічні

упередження або інші фактори [1]. Тут у пригоді стають сучасні поведінкові теорії ризику. Наприклад, теорія перспектив Канемана та Тверскі показує, що люди схильні оцінювати виграші і втрати асиметрично й можуть приймати ірраціональні рішення під впливом ризику [16]. Застосування цього підходу до ПВК/ФТ означає, що і злочинці, і фінансові установи не завжди діятимуть як бездоганні «рахівники корисності». Злочинець може переоцінити свої шанси уникнути покарання (ефект надмірної самовпевненості) або бути мотивованим не лише матеріально (ідеологічні терористи можуть ігнорувати низьку очікувану корисність через фанатичну відданість справі). У свою чергу, банк може недооцінити ризик, спокушений великим прибутком від обслуговування сумнівного клієнта, або, навпаки, через надмірний страх втрат відмовитися від вигідного бізнесу (ефект неприйняття ризику) [16].

Отже, для розвитку теорії очікуваної корисності в контексті ПВК/ФТ варто поєднувати класичні раціональні моделі з напрацюваннями поведінкової економіки. Раціональна основа максимізації очікуваної корисності залишається корисною, але її слід коригувати з урахуванням сприйняття ризику та поведінкових реакцій на регуляторні заходи. Це міждисциплінарне завдання на перетині економіки, психології і кримінології: створити реалістичніші моделі, що прогнозують, як учасники фінансової системи – і легальні, і кримінальні – насправді реагують на зміни в ризик-орієнтованому регулюванні.

Однозначного трактування сутності категорії «ризик» не сформувалося, оскільки це складне явище, що має багатоаспектні, а інколи протилежні реальні основи. В економічній літературі відомі численні спроби сформулювати теоретичні визначення поняття ризику.

Уперше наукове, математичне визначення поняття «ризик» сформулював більш як двісті років тому німецький математик Йоганн Ніколаус Тетенс (1736—1807) у праці «Вступ до розрахунку життєвої ренти і право на її отримання» [6, с. 9], виданій у 1786 р. в Лейпцигу. Тим самим він започаткував основи нового наукового напряму — ризикології, яка набула практичного застосування у

страхуванні життя. Дослідники його творчості наголошують, що навіть за відсутності на той час необхідного емпіричного матеріалу, він дуже часто інтуїтивно робив правильні висновки. Йому приписують каламбурний вислів: «...навіть коли відсутня теорія, то все ж добре видно, як вона повинна бути застосована».

Й. Тетенс запропонував прийняти мірою ризику половину величини стандартного відхилення, вважаючи його обсягом очікуваного збитку страхового закладу, що виникає за умовами договору страхування. Контраргументом такого твердження стала поширена теза, згідно з якою ймовірність є лише мірою величини ризику, але не може бути ним самим [6, с. 16]

Очевидно, такий підхід пояснюється бажанням побачити давнє походження цього терміна, тобто набагато раніше від початку розвитку комерційного страхування. На погляд фахівців, підставу вважати ризик предметом турботи ще античного світу надає М. І. Фінлей, автор книги «Античне господарство» [7, с. 14].

Найпоширенішим, але й найсуперечливішим у теорії ризику є погляд, згідно з яким ризик є невизначеністю (або непевністю). Відомий польський учений професор Оскар Ланге підкреслює, ще економісти неокласичної школи (кінець XIX — початок XX ст.) протягом тривалого часу переважно вживали замість терміна «ризик» термін «невизначеність» [8]. Наукова дискусія стосовно обґрунтованості такого визначення відбувається понад століття. Уперше розглянути економічний аспект ризику в такому контексті намагався американський учений Алан Віллетт у роботі «Економічна теорія ризику і страхування» (1901 р.) [9]. На його погляд, попри вживання поняття «ризик» у різних значеннях, поширена загальна думка, що він певним чином пов’язується з поняттям невизначеності. Останнє стосується кожної ситуації, коли неможливо уявити процес діяльності та його наслідки, неможливо виявити причинно-наслідковий (детерміністичний) зв’язок між елементами цього процесу. Тому

позиція стосовно співвідношення ризику і невизначеності А. Віллетта сформована на підставі виключно принципу загального детермінізму, тобто того, що всі очевидні явища, зокрема й випадкові, завжди мають причинно-наслідковий характер і тому постають наслідками інших явищ — причин. Тому окремі явища видаються випадковими через неповне знання причин їх походження. У зв'язку з цим в індивідів виникає суб'єктивний стан невизначеності.

Отже, на думку А. Віллетта, ризик є чимось об'єктивним, але корельованим із суб'єктивною невизначеністю, або інакше — об'єктивним корелянтом останньої [9, с. 5]. Однак така орієнтація на невизначеність не отримала належного теоретичного підтвердження, бо невизначеність теж сприймалася мінімум у трьох значеннях, а саме як: об'єктивна; психологічна, або суб'єктивна; як така, що виникає у процесі прийняття рішень.

Сформоване на такій основі поняття ризику теж сприймається трояко:

1. Ризик як об'єктивне відображення суб'єктивної невизначеності. Остання постає як свідома інтерпретація об'єктизованої невизначеності. Так, представлена непевність існує навіть тоді, коли вважається, що «дещо» може, але не повинне настати.

2. Ризик як невизначеність через її психологічне сприйняття. У такому значенні ризик становить комбінацію азарту та інших цілеспрямованих дій і вимірюється за допомогою показника ймовірності ступеня переконання особи. Водночас ризик вважається станом реального світу, а невизначеність — станом свідомості.

3. Третє трактування зв'язку «ризик — невизначеність» — сприйняття ризику як суто психологічного явища, що проявляється лише в розумінні людських відчуттів та досвіду (поведінки). Прихильники психологічного підходу спираються на тісний зв'язок між суб'єктивними переживаннями індивіда й об'єктивною реальністю. За такою позицією величина ризику має

змінюватися відповідно до стану психіки, свідомості особи, котра наражається на «дещо».

Отже, ризик на основі невизначеності описується в широкому діапазоні – від об'єктивізації невизначеності (ризику) до її суб'єктивного сприйняття. Однак, на думку фахівців, у міру відходу від об'єктивізації невизначеності й переходу до її суб'єктивного сприйняття з метою визначення на її основі обсягу ризику, теоретична цінність таких спроб і отриманих результатів стає дедалі меншою, оскільки скорочуються можливості квантифікації невизначеності й ризику [10, с. 44].

Поширена думка про те, що правильно пояснити джерел походження ризиків різних видів, які детермінують діяльність сучасних організацій, суб'єктів господарювання, можна на основі «теорію катастроф», сформульованої Р. Томою та Е. С. Зееманом. Ця теорія ґрунтується на тезі про стрибкоподібний, раптовий характер будь-якої організації. Однією з ознак такого розвитку є так звана дисконтинація. Про неї йдеться, коли відбувається стрімка, неочікувана зміна величини або ознак об'єкта, попри те, що чинники, які безпосередньо впливають на це явище, не піддаються таким самим стрімким змінам. Однак приписувати ризикам абсолютну випадковість, на погляд представників Лондонського страхового інституту, для визначення кількісної оцінки ризику з метою його передбачення та практичного управління, неправильно [10, с.52].

Цю ідею розвиває і «теорія звільнення енергії», розроблена Вільямом Халдоном. За нею всі нещасні випадки є наслідком неконтрольованого вивільнення енергії, що виявляється більшим, ніж певний об'єкт (структура) може витримати [11]. Аналогічне також твердження Фрідріха Ніцше про те, що кожне людське серце, переповнене сміливістю і радістю, час від часу потребує відчуття деякої небезпеки [12, с. 133].

Уперше наукову спробу розмежувати поняття ризику і невизначеності здійснив представник неокласичної школи, американський економіст Френк Найт у праці «Ризик, невизначеність, прибуток» (1921 р.). У ній він, зокрема,

стверджує, що ризик — це лише така невизначеність, яку можна технічно оцінити й виміряти. Як методом вимірювання він запропонував пробабілістичний розрахунок (визначення ймовірності) [13]. Залежно від точності розрахунку він поділив імовірність на три види: математичну (апріорну); статистичну (апостеріорну); експертної оцінки (естиматичну). Третій із запропонованих методів розрахунку ймовірності — естиматичний, на відміну від попередніх, має здебільшого вимушений характер застосування. Тільки через обмеженість математико-статистичної інформації експертна оцінка здійснюється на підставі як об'єктивних, так і суб'єктивних знань, тобто на основі загальної досвідченості, а також інтелігентності та інтуїції особи, котра проводить оцінку ймовірності.

В умовах цифрової економіки та криптовалютної революції найтівське розрізнення набуло ще більшої актуальності. Ринок цифрових активів характеризується екстремальною волатильністю та непередбачуваністю. Наприклад, для біткоїна та інших криптовалют історичних даних бракує, тому оцінити ризик стандартними методами складно – розподіли дохідностей можуть змінюватися, «хвости» важко передбачити. Дослідження крипторинку підтверджують, що інвестори стикаються як з вимірюваним ризиком, так і з істотною невизначеністю. Зокрема, було запропоновано оцінювати невизначеність криптовалют через ентропію Шеннона , а ризик – через вартість у зоні ризику (англ. Value-at-Risk (VaR)) і умовну вартість під ризиком (англ. Conditional VaR) для врахування екстремальних втрат [17]. Виявилося, що у періоди бурхливих спекуляцій ентропія (невизначеність) зростає, відображаючи непередбачувані зміни на ринку, тоді як оцінки VaR сигналізують про високий ризик потенційних збитків.

У сфері ПВК/ФТ проблема невизначеності проявляється в постійному виникненні нових схем відмивання коштів. Регулятори часто не мають статистики або моделей для абсолютно нових феноменів – таких як відмивання через децентралізовані платформи чи використання невзаємозамінних

криптотокенів для переказу цінностей. Це найтівська невизначеність у чистому вигляді, тому що неможливо наперед імовірнісно оцінити ризик коли прецедентів мало або взагалі немає. Наприклад, поява нових анонімізуючих сервісів (міксерів) створює ситуацію, коли невідомо, як часто та з яким успіхом злочинці їх використовуватимуть – отже, важко призначити ймовірності виявлення чи збитків.

Адаптація найтівської теорії ризику в сучасних умовах означає визнання і врахування високої невизначеності цифрових фінансів. Регуляторам варто застосовувати підходи управління, націлені не лише на ймовірні, а й на «невідомі» ризики. Це може включати стрес-тестування фінансових систем на гіпотетичні сценарії, наприклад, масове ВК через нову платформу, а також постійний моніторинг технологічних трендів [89]. Міжнародна практика вже рухається в цьому напрямі: FATF підкреслює, що сектор віртуальних активів розвивається надзвичайно динамічно і потребує безперервного нагляду та взаємодії між державою і приватними гравцями [89]. Іншими словами, щоб боротися з невизначеністю, регулятори мають бути проактивними, обмінюватися даними з індустрією та швидко оновлювати оцінки ризиків у відповідь на нові загрози. Такий гнучкий, адаптивний підхід цілком у дусі Найта, тобто приймати невизначеність як даність і бути готовим до несподіваного.

На думку автора, попри певну обмеженість можливостей експертно-оціночного методу, його застосування в економічній сфері зростатиме, зокрема, у сфері ризиків фінансово-кредитної діяльності. Невизначеність, оцінену таким методом, лише умовно можна прийняти за кількісне значення ризику. Тому, за теорією Найта, про ризик можна говорити лише тоді, коли результат будь-якої діяльності вимірюється з допомогою хоча б одного з трьох наведених методів розрахунку ймовірності. Якщо зробити це неможливо, результат залишається на рівні невизначеності.

Варто підкреслити, що таке пояснення головного питання ризикології мало також велике загальноекономічне значення, адже надавало нове пояснення

походженню прибутку з ризику. Відзначаючи цю заслугу Найта в галузі економічної теорії, Джон Гелбрайт підкреслив: відсутність протягом усього XIX ст. теоретичного обґрунтування походження доходу з капіталу надихнула Карла Маркса на створення революційного вчення про походження прибутку з додаткової вартості. Найімовірніше, на думку Гелбрайта, пояснення цього явища остаточно сформувалося тільки на початку XX ст. у зв'язку з дослідженнями у сфері теорії ризику. Прибуток, який тепер почали відрізняти від процента, не без певної логіки вважають винагородою за новаторство [14, с. 104].

На потребу в розмежуванні невизначеності й ризику наголошують, коли аналізується ефективність інноваційного проєкту. Причому така невизначеність тлумачиться як результат змін вартості змінної випадковості у формі її сподіваної вартості. Ризик виникає в можливості набуття змінною випадковою такого значення, яке відносно її середньої величини означає зменшення (втрату) майна. Вживається також вираз «невизначеність ризику», що свідчить про однорідність ризику і невизначеності, а водночас і відмінність між ними.

У концепції професора Оскара Ланге проблеми співвідношення невизначеності й ризику розглядаються саме під таким кутом зору. За приклад береться підприємство, що діє в умовах невизначеності й чий прибуток є змінною випадковою, як і трапляється на практиці. З метою отримання точніших значень Оскар Ланге вводить кількісний показник — коефіцієнт невизначеності, що розраховується як змінна випадкова при відомому розкладі ймовірності, і таким чином уже застерігається вимірність цієї невизначеності. Невимірна невизначеність, за Оскаром Ланге, набуває характеру абсолютної [8, с. 148].

За неокласичною теорією ризику, економічна поведінка людей ґрунтується на концепції граничної корисності, згідно з якою гарантований прибуток є цінішим, ніж очікуваний прибуток того самого розміру, але з потенційними коливаннями.

Гаррі Марковіц у 1952 р. розробив модель оптимального інвестування, відому як «Сучасна теорія портфеля», що базується на принципі балансування

ризику та дохідності за допомогою диверсифікації інвестиційних активів. Центральною ідеєю цієї теорії є те, що інвестори повинні раціонально розподіляти свої ресурси між різними активами, аби зменшити загальний ризик портфеля за заданого рівня очікуваної дохідності. У цій моделі ризик вимірюється дисперсією дохідностей активів, а його зменшення досягається завдяки низькій кореляції між різними інструментами. При цьому Марковіц підкреслював, що важливими є не стільки індивідуальні характеристики окремих активів, скільки їхній взаємний вплив на загальний ризик та прибутковість портфеля. Ця концепція покладена в основу сучасного фінансового ризик-менеджменту та таких важливих фінансових метрик, як ефективна межа портфеля та коефіцієнт Шарпа.

Застосування портфельної теорії Марковіца до цифрових активів і ризик-орієнтованого підходу в контексті ПВК/ФТ відкриває нові перспективи. Для фінансових інститутів включення криптовалют до портфеля традиційних інвестиційних активів ставить питання про вплив цього високоризикового елемента на загальний ризик портфеля [19; 433]. Навіть невелика частка криптоактивів може покращити диверсифікацію, проте значна волатильність криптовалют створює суттєві ризики екстремальних втрат, що недостатньо точно відображається класичними моделями, які базуються на дисперсії [28]. Тому з'являються нові підходи, наприклад, оптимізація портфеля за допомогою умовної вартості під ризиком (CVaR), що мінімізує потенційні максимальні втрати замість класичної дисперсії [28]. Це ілюструє адаптацію класичної портфельної теорії до специфічних умов цифрового ринку.

Для банків та регуляторних органів принцип диверсифікації також можна ефективно використовувати в управлінні ризиками фінансових злочинів. Фінансові установи фактично формують портфелі ризиків, які охоплюють клієнтів, продукти, ринки та канали платежів. Ризик-орієнтований підхід вимагає досягнення оптимального балансу, коли загальний ризик залишається керованим, а бізнесові цілі реалізуються. У цьому контексті можна провести

аналогію з ефективною межею портфеля Марковіца, де існує оптимальна межа між прибутковістю та ризиком, яку прагнуть знайти банки у своїй комплаєнс-політиці. Таким чином, менеджмент банківських установ розв’язує задачу, аналогічну марковіцівській, але вже в площині комплаєнс-ризиків.

Цікавою є й можливість застосування підходів класичної теорії портфеля для аналізу поведінки злочинних груп. Професійні відмивачі коштів зазвичай не покладаються на єдиний механізм відмивання, а диверсифікують ризики шляхом розподілу нелегальних фінансових потоків між різними каналами та юрисдикціями. Це дає їм змогу знизити ризик викриття та конфіскації активів. Стратегії на взірець дроблення сум трансакцій (smurfing) демонструють, як злочинці використовують принцип некорельованих активів, аналогічний до марковіцівської диверсифікації, для досягнення своїх незаконних цілей. Розуміння таких стратегій надає правоохоронним органам і регуляторам важливі інсайти для розроблення комплексних заходів із ПВК.

Подальший розвиток портфельної теорії в цифрову епоху передбачає інтеграцію багатовимірних моделей ризику, що враховують взаємозв'язок різних типів ризиків: операційних, ринкових, кібернетичних та регуляторних. Це передбачає створення міждисциплінарних команд експертів, котрі зможуть формувати складні моделі, здатні адекватніше оцінювати сукупний ризик сучасних фінансових установ, ураховуючи ефекти взаємодії різних ризиків та прогнозуючи потенційні системні збої.

Теорія регулювання ризиків, сформульована Джорджем Стіглером та Семом Пельцманом, акцентує увагу на тому, що державне регулювання має бути гнучким і адаптивним, а не жорстким та обмежувальним [527]. Суть цього підходу полягає в оптимізації витрат і вигід від регуляторних рішень. Теорія описує взаємодію між державними органами, компаніями та суспільством, наголошуючи, що регуляторні механізми можуть бути використані на користь великих корпорацій, а не суспільних інтересів. Стіглер та Пельцман продемонстрували, що регулятори часто можуть бути захоплені тими, кого

повинні контролювати, що призводить до формування регуляцій, які підтримують великі бізнес-структури за рахунок менш потужних конкурентів та споживачів. Ця теорія пояснює, як економічна політика формується під впливом зацікавлених сторін та може викликати зниження рівня конкуренції на ринку [527; 528].

Сучасні дослідники розширили ідеї Стіглера та Пельцмана, запровадивши нові моделі, такі як теорія поведінкових фінансів Річарда Тайлера [529], що досліджує вплив психологічних факторів на регуляторні рішення. Економічна теорія регулювання ризиків Стіглера та Пельцмана стала основою сучасного аналізу державної політики та ролі регуляторів у ринковій економіці.

Сучасні виклики, такі як цифровізація економіки та фінансові кризи, вимагають подальшого розвитку економічної теорії регулювання ризиків. Інновації у сфері цифрових активів та нові моделі поведінкових фінансів змушують науковців шукати ефективніші регуляторні механізми, здатні протидіяти сучасним загрозам та забезпечити стабільність і конкурентність фінансових ринків у XXI ст.

Попри те, що ризик є невід'ємною частиною економічної діяльності підприємства, його дослідження залишається недостатньо розвиненим. Дотепер немає загальновизнаного визначення поняття «ризик», єдиної класифікації його видів, бракує фундаментальних досліджень, які би цілком розкривали сутність і зміст цієї економічної категорії. У табл. 1.1 наведено погляди науковців відповідно до теорій, у рамках яких вони проводили дослідження.

Таблиця 1.1

Погляди економістів на проблему ризику

Автор	Теорія, у рамках якої розглядалась проблема ризику	Внесок у розвиток теорії ризику
Йоганн- Ніколаус Тетенс	Сучасні теорії актуарних розрахунків	- вперше сформулював наукове визначення поняття «ризик»; - дослідження щодо вимірювання величини ризику

Продовження таблиці 1.1

Дж. Мілль, Н. І. Сеніор	Класична теорія ризику	Ризик визначається як збиток унаслідок реалізації обраного рішення
Кантоністи	Теорія відсотка	Перше згадування про ризик економічної діяльності
Дж. М. Кейнс	Теорія відсотка	Обґрунтував ідею, що до вартості товару повинні входити можливі витрати, викликані непередбачуваними обставинами. На його думку, в економічному житті доцільно враховувати три основних види ризику - ризик підприємця (позичальника); ризик кредитора (ухилення боржника від сплати боргу); зменшення вартості грошової одиниці.
Адам Сміт	Теорії заробітної плати, прибутку, відсотку	- Розгляд ризику як фактора розміру заробітної плати; - дослідження зв'язку ризику і прибутку, виокремлення психологічної природи ризику
Альфред Маршалл	Теорія прибутку	Закладено основу неокласичної теорії ризику, яка, на відміну від класичної теорії, припускає позитивні наслідки настання ризику
Ганс фон Мангольдт	Теорія прибутку	Розгляд існування нестрахового ризику; введення в систему оцінювання величини ризику фактора часу; розгляд можливості управління і зменшення ризику
Йоганн-Генріх фон Тюнен	Теорія прибутку	Поділ ризику на такий, від якого можна застрахуватися, і такий, що не може бути застрахованим
Карл Маркс	Теорія наукового соціалізму	Припущення про можливість повністю позбутися економічного ризику в умовах планової економіки
Йозеф Шумпетер	Теорії підприємництва, прибутку і відсотка	- Спростовано уявлення про підприємця як про носія ризику; - висловлено думку про залежність між рівнем ризику та рівнем ділової активності в окремих галузях виробництва; - започатковано класифікацію ризиків
Джон-Гейтс Кларк	Теорія прибутку	Визначення природи ризику в динамічних змінах
Даниїл Бернуллі	Використання математичних методів як інструменту теорії ризику	Наголошення на тому, що в ризикованих операціях слід ураховувати не суму виграшу, а корисність виграшу
Вернер Зомбарт	Теорія підприємництва	Визначення ризику як невід'ємного атрибуту підприємця-«завойовника»
Джон Аткінсон Гобсон	Інституціональна економічна теорія	Включення ризику до складу причин класової нерівності

Продовження таблиці 1.1

Мілтон Фрідмен	Проблеми корисності та вибору	Розгляд особливостей реакції різних людей на ризик та схильності людини до ризику залежно від рівня їхнього доходу
Джон Хікс	Інвестування на ринку цінних паперів	Пояснення відсотка, принесеного цінними паперами, премією за очікування і винагородою за ризик при довгостроковому інвестуванні
Алан Віллетт	Теорія страхування	Перша спроба висвітлити економічний аспект ризику з точки зору невизначеності
Френк Найт	Теорія прибутку	- Перше обґрунтування необхідності відокремлення поняття ризику від невизначеності; - виокремлення зв'язку прибутку з елементом невизначеності; - започаткування сучасної теорії фінансового ризику, головною метою якої є оптимізація величини ризику.
Гаррі Марковіц, Вільям Шарп, Джеймс Тобін	Теорія фінансів (математичне обґрунтування стратегії диверсифікації інвестиційного портфеля)	Визначення оптимальної структури портфеля, що включає безризикові цінні папери (короткострокові державні векселі) і не залежить від схильності інвестора до ризику
Вільям Шарп	Теорія фінансів	- Створення моделі ціноутворення на ринку капіталів і цінних паперів; - поділ загального ризику на систематичний і специфічний ризик

Джерело: складено автором за матеріалами [3–22].

Доповнення неокласичної теорії фактором задоволення зумовило висновок, що підприємець може йти на великий ризик заради можливого високого прибутку.

Варто зазначити, що стан ризику суттєво відрізняється від стану невизначеності. Невизначеність характеризується тим, що ймовірність настання результатів рішень або подій взагалі не може бути встановлена.

Отже, стан ризику є різновидом невизначеності, коли деякі події можуть статися з певною ймовірністю, яку можна оцінити. У такій ситуації існує реальна можливість визначити ймовірність подій, що можуть виникнути через співпрацю з партнерами, дії конкурентів, вплив природних умов, науково-технічний прогрес. Серед дослідників немає єдиної думки щодо визначення ризику. Його

трактують як шкоду, недоотримання прибутку або діяльність, спрямовану на усунення невизначеності. Френк Найт розрізняв ризик шкоди (небезпеки) як імовірні події, які можна оцінити, і невизначеність як події, ймовірність яких неможливо визначити. Дуглас Бернштейн розглядав ризик як можливу загрозу для економічних систем, що призводить до втрат. Стосовно недоотримання прибутку Гаррі Марковіц у межах теорії портфеля інвестора визначав ризик як волатильність дохідності, що впливає на очікуваний прибуток, а Вільям Шарп у моделі оцінювання капітальних активів (CAPM) трактував ризик як відхилення фактичного прибутку від очікуваного. Ризик як діяльність для усунення невизначеності Герберт Саймон у рамках теорії обмеженої раціональності описував як процес прийняття рішень у ситуаціях невизначеності, а Насім Талеб у теорії «чорного лебедя» пояснював, що ризик — це процес адаптації до непередбачуваних подій.

Під ризиком зазвичай розуміють імовірність втрат ресурсів підприємства, недоотримання доходів чи виникнення додаткових витрат у процесі ведення певної виробничої або фінансової діяльності. Ризик тлумачиться як невизначеність, пов'язана з певною подією або її наслідками. Також ризик – це ситуативна характеристика діяльності виробника, що відображає невизначеність результату і можливі несприятливі наслідки в разі невдачі. Ризик можна розглядати як постійну необхідність долати перешкоди на шляху до досягнення мети. У підприємницькій діяльності ризик становить поведінку в умовах невизначеності. Також його можна описати як подію, що може відбутися або не відбутися, дії зі сподіванням на позитивний результат [17]. Розглянемо підходи до трактування поняття «ризик».

Аналізуючи це поняття, варто відзначити його комплексність і полінауковість, оскільки теоретичні засади ризику розроблялися в таких дисциплінах, як соціологія, економіка, прикладна математика, психологія прийняття рішень і когнітивна психологія.

Аналіз еволюції поняття «ризик» показує, що його значення поступово розширюється та конкретизується на двох рівнях. На рівні окремої особи ризик розглядається як суб'єктивна невизначеність, потенційна загроза або вибір серед імовірних варіантів дій, зокрема потенційно небезпечних. Оцінка ризику залежить від сприйняття ситуації та ставлення суб'єкта до оточення і себе. На рівні соціальних груп, організацій та суспільства ризик розуміється як посилення соціальної активності й інформаційних процесів, що збільшує ризики в соціальному середовищі та сприяє виникненню несприятливих подій або негативних наслідків.

Основне визначення ризику – це «ймовірність виникнення небезпеки». У цьому визначенні ключовими є два поняття: «ймовірність», яка відображає певний рівень невизначеності, та «небезпека», що вказує на потенційно негативний вплив або ризик негативного результату. Таким чином, ризик – це можливість того, що під час виконання процесів і операцій, спрямованих на досягнення певної мети, можуть виникнути обставини, що призведуть до втрат, небезпеки або негативного результату в майбутньому.

Однак існує й інший підхід до розуміння ризику, який акцентує увагу на тому, що ризик здатний створювати нові можливості для досягнення цілей. Причому класифікувати їх як «позитивні ризики» не варто. Ризик завжди залишається небезпекою, тоді як можливість – це позитивний шанс. Тобто ризик не лише створює загрози, а й може відкривати нові перспективи.

Невизначеність у понятті «ризик» вплинула і на прагнення його класифікувати. Дотепер дослідники, котрі працюють над проблемою ризику, не дійшли спільної думки щодо того, якою має бути класифікація систем ризиків. Як наслідок, у працях різних науковців нараховується понад 200 різних видів ризиків, представлених у різноманітних класифікаційних комбінаціях. Аналіз зростаючої кількості робіт, присвячених створенню єдиної структури ризиків, свідчить про те, що дослідники не лише не досягли універсального підходу, а й

не наближаються до його формування. Розподіл за критеріями класифікації ризиків наведено в табл. 1.2.

Таблиця 1.2

Класифікація ризиків за певними ознаками

За сферою виникнення	Зовнішні
	Внутрішні (управлінські)
За сферою походження	Загальні (інформаційні)
	Специфічні (банківські, виробничі)
За рівнем прийняття рішень	Макроекономічні (глобальні)
	Мікроекономічні (локальні)
За тривалістю дії	Короткочасні (транспортні, неплатіж по конкретній угоді)
	Постійні (ризики стихійних лих у певному районі)
За рівнем втрат	Мінімальні, середні, максимальні або припустимі
	Критичні
	Катастрофічні
За ступенем правомірності	Правомірні (виправдані)
	Неправомірні (невиправдані)
За можливістю страхування	Що страхуються
	Що не страхуються
За об'єктивністю	З об'єктивною ймовірністю
	Із суб'єктивною ймовірністю
	Із суб'єктивно-об'єктивною ймовірністю
За часом прийняття рішень	Випереджальний
	Своєчасні
	Запізнілі
За типами	Раціональні (обґрунтовані)
	Нераціональні (необґрунтовані)
	Авантюрні (азартні)
За кількістю осіб, що приймають рішення	Індивідуальні
	Групові
За загрозою сталості втрат	Статичні (прості)
	Динамічні (спекулятивні)

Джерело: складено автором за матеріалами [3–22].

На думку автора, запропонована класифікація не є вичерпною, оскільки принцип її формування залежить від конкретного завдання, характеристик суб'єкта, що виконує це завдання, і конкретної ситуації, в якій він перебуває. Для кожного окремого завдання класифікація ризиків може мати унікальне рішення, оскільки природа ризику, притаманна певному виду діяльності, має специфіку, що визначає доцільність використання тих чи інших ознак у класифікації. Тому створення універсальної класифікації видається майже неможливим, і спроба

застосувати стандартну класифікацію ризиків для управління підприємством може бути неправильною. Однак запропонована класифікація може бути корисною для організацій і моделлю для розроблення власної класифікаційної системи.

У юридичному контексті ризик відображає наявність факторів невизначеності в рішеннях особи, котра їх ухвалює. Тому в юридичній літературі ризик зазвичай має негативне забарвлення, хоча йому приділяється значна увага. Термінологія, що стосується ризику, у правових документах є чіткішою порівняно з економічною. З точки зору права ризик починається там, де закінчується відповідальність і можливість відшкодування збитків за договором або іншими підставами. Виникає запитання, хто несе відповідальність за збитки, за які неможливо притягти когось до відповідальності та немає законних підстав вимагати відшкодування.

Останнім часом у юридичній літературі збитки у вигляді неотриманого прибутку або прибутку, меншого за очікуваний, набувають чіткішого визначення. Хоча межу між ризиком, недбалістю та злочинними діями важко встановити, це не означає, що немає підстав для притягнення до відповідальності за результати господарської діяльності згідно зі статтями трудового або кримінального права. З правової точки зору караними є недбалість, некомпетентність керівників і недостатність знань, якщо вони призводять до серйозних наслідків.

Аналіз напрямів адаптації класичних економічних теорій ризику свідчить про їхню стійкість і гнучкість у контексті цифрових трансформацій. Хоча фундаментальні праці таких науковців, як Френк Найт, фон Нейман – Моргенштерн, Гаррі Марковіц та Стіглер – Пельцман створювалися в іншій історичній та економічній реальності, базові принципи цих теорій успішно інтегруються в сучасні підходи до ризик-менеджменту. Зокрема, у сфері ПВК/ФТ в умовах функціонування криптовалют та цифрової економіки відбувається суттєва еволюція зазначених теорій.

Сучасний тренд у науковому дискурсі характеризується активною міждисциплінарною взаємодією. Економічні моделі ризику сьогодні інтегрують експертизу у сферах штучного інтелекту, кібербезпеки та міжнародного права. Наприклад, ризик-орієнтований підхід у сфері ПВК/ФТ базується на ідеях оптимального розподілу ресурсів (Марковіц), оцінці ймовірностей та очікуваної корисності (фон Нейман – Моргенштерн), розрізненні вимірюваних і невимірюваних ризиків (Найт), а також ефективності регулювання за наявності поведінкових реакцій учасників (Стіглер – Пельцман) [53, 115].

Отже, класичні економічні теорії ризику не втрачають актуальності, а навпаки, – набувають нового звучання завдяки інтеграції сучасних технологічних інновацій. Актуальні виклики, такі як криптовалюти та децентралізовані фінансові системи (DeFi), сприяють формуванню нових міждисциплінарних теоретичних конструкцій, зокрема поведінкових теорій регулювання або моделей ризику, що використовують штучний інтелект. Подальший успіх у ПВК/ФТ багато в чому буде залежати від ефективної інтеграції класичних економічних підходів із науково-технічними досягненнями сьогодення. Наприклад, оновлення настанов FATF щодо ВА для науки означає появу нового поля досліджень – «RegTech» (регуляторні технології) та «SupTech» (технології нагляду): моделювання ефективності різних регуляторних інструментів, оцінка глобального і локального впливу правил, оптимізація співпраці між країнами. Економісти спільно з фахівцями права і комп’ютерних наук можуть розробляти моделі, що підкажуть, як найкраще структурувати міжнародні угоди, аби мінімізувати можливості арбітражу для фінансових злочинців. Перелічені виклики вимагають міждисциплінарного синтезу економічної теорії, регуляторної політики та новітніх технологій, що відкриває широкі перспективи для академічних досліджень і практичного застосування.

З позиції сучасного науковця, вважаю, що окреслені теорії потребують адаптації до нових реалій цифрової економіки, особливо у сфері обігу цифрових

активів та ПВК/ФТ. Сучасний крипторинок сформував унікальні виклики, які не враховувались у класичних теоріях ризику.

По-перше, теорія ризику та невизначеності повинна розширити свій фокус з акцентом на алгоритмічній невизначеності, що характерна для смарт-контрактів, децентралізованих фінансів (DeFi) та децентралізованих організацій (DAO). Невизначеність у блокчейн-екосистемах має не лише стохастичний, а й програмний характер, що вимагає нових математичних моделей.

По-друге, модель очікуваної корисності має бути переосмислена в контексті поведінкової економіки в криптосередовищі. Користувачі цифрових активів часто діють нераціонально, під впливом ажіотажу, соціальних сигналів або маніпуляцій, що знижує релевантність класичних моделей.

По-третє, портфельна теорія Марковіца повинна враховувати ризики, властиві криптоактивам: високу волатильність, непрозору ліквідність, регуляторну невизначеність. Вона має бути доповнена моделями з урахуванням ризиків технічних вразливостей (експлойти, хакерські атаки), поведінкових ризиків користувачів і навіть меметичних ефектів.

Нарешті, теорія регуляторного ризику Стіглера – Пельцмана повинна еволюціонувати в напрямі гнучкого, децентралізованого регулювання з використанням супервізійних технологій. В умовах цифрових активів класичні інструменти іноді втрачають ефективність. Необхідно формувати ризик-орієнтовану модель, що враховує ризики на рівні й інституцій, і інфраструктур.

Таким чином, подальший розвиток економічних теорій має бути міждисциплінарним і технологічно чутливим. У ньому доцільно поєднувати класичні підходи із сучасними інструментами аналізу даних, штучного інтелекту, поведінкової економіки та криптографії. Лише в такому разі ризик-орієнтований підхід залишатиметься релевантним та ефективним у цифрову епоху.

Проте у XXI ст. виникають нові виклики, такі як цифровізація економіки, фінансові кризи та проблеми монополізації ринків, що вимагають подальшого розвитку цієї теорії та пошуку ефективніших механізмів регулювання.

Ризик-орієнтований підхід є ключовим інструментом сучасної економічної науки, який дає змогу аналізувати, мінімізувати й управляти ризиками в різних сферах: від фінансів і державного регулювання до корпоративного управління та економічної політики. Основою цього підходу є економічні теорії, що пояснюють природу ризику, його оцінку та шляхи його зменшення.

У сфері цифрових активів невизначеність відповідно до теорії ризику та невизначеності Френка Найта проявляється через відсутність єдиної нормативно-правової бази для їх регулювання, тоді як ризик може бути кількісно оцінений через аналіз волатильності криптовалютних активів і рівня їхньої ліквідності.

Інвестори, котрі вкладають кошти в цифрові активи, часто керуються власною оцінкою ризиків і вигід, зокрема співвідношенням можливих прибутків від володіння криптоактивами та ймовірністю їхньої втрати через регуляторні обмеження або шахрайство. Теорія очікуваної корисності Неймана – Моргенштерна, яку використовують для аналізу поведінки інвесторів, банківських установ та державних регуляторів може бути застосована для розроблення політики ПВК/ФТ.

Державні регулятори можуть застосовувати методи диверсифікації ризиків, обмежуючи вплив волатильних цифрових активів на фінансову систему шляхом впровадження механізмів контролю та страхування ризиків у банківському секторі та ринку віртуальних активів. Ефективне управління ризиками завдяки диверсифікації активів відповідно до портфельної теорії ризику Гаррі Марковіца є основою для сучасних методів оцінки ризиків у фінансовому секторі.

У сфері цифрових активів жорсткі заборони на користування ВА в окремих країнах, наприклад, Китаї, призводять до відпливу капіталу на нерегульовані

ринки, тоді як адаптивні підходи, наприклад, у Швейцарії чи ЄС, дають змогу контролювати цей ринок через механізми ліцензування постачальників послуг, пов'язаних з оборотом віртуальних активів.

На думку автора, державне втручання в ринок має бути гнучким і адаптивним. Головна ідея полягає в тому, що регулювання повинне базуватися на співвідношенні витрат і вигід, а не на жорстких обмеженнях. Це допоможе ефективніше розподіляти ресурси й мінімізувати негативні наслідки регуляторних рішень, що відповідає засадам ризик-орієнтованого підходу та економічній теорії регулювання ризиків Стіглера – Пельцмана. З огляду на випереджальні темпи розвитку цифрової економіки і системно-сповільнені темпи розроблення та впровадження відповідного державного регулювання через виявлення сутності цифрових інновацій доцільно сконцентрувати державне регулювання на сфері запобігання та реагування на злочинну діяльність із використанням цифрових активів та у віртуальному просторі. Другим за важливістю напрямом державного регулювання повинне стати дослідження цифрових інновацій із використання сучасних управлінських рішень, таких як «регуляторні пісочниці».

Регуляторна пісочниця — це спеціально створене регулятором середовище, яке дає змогу фінансовим технологічним компаніям та іншим новаторам тестувати інноваційні продукти, послуги чи бізнес-моделі в реальних умовах ринку під наглядом регулятора. Такий підхід сприяє безпечному впровадженню новацій, забезпечуючи дотримання необхідних нормативних вимог та захист прав споживачів [23].

Попри очевидні переваги ризик-орієнтованого підходу, існує низка викликів щодо його застосування в регулюванні цифрових активів. Деякі експерти вважають, що традиційні моделі оцінки ризиків не здатні ефективно відображати динамічні та швидкозмінні ризики криптовалютного ринку. Наприклад, ризикова премія в теорії Марковіца не враховує раптових змін у регуляторному середовищі, що може спричиняти різку зміну вартості активів.

Також очікувана корисність не завжди відображає поведінку інвесторів на криптовалютному ринку, адже значна частина угод здійснюється на підставі спекулятивних мотивів, а не реальної оцінки ризику.

Гнучке регулювання за теорією Стіглера – Пельцмана не завжди є ефективним у боротьбі з фінансуванням тероризму через криптоактиви, оскільки відсутність жорстких обмежень може сприяти використанню цифрових активів у нелегальних схемах.

З урахуванням цих аспектів подальше дослідження ризик-орієнтованого підходу у сфері цифрових активів має включати розроблення нових моделей методики оцінки ризиків, адаптованих до технологічних особливостей цього ринку, зокрема:

– аналіз поведінкових аномалій у блокчейні – використання алгоритмів машинного навчання для виявлення нетипових трансакцій і підозрілих шаблонів поведінки;

– моніторинг санкційних списків цифрових гаманців у реальному часі – застосування блокчейн-аналітики та AI-інструментів для автоматичного відстеження санкційних адрес і підозрілих контрагентів;

– оцінку рівня вразливості DeFi-протоколів на основі кібербезпекових аудитів та історії зламаних контрактів через ризик-аналіз DeFi-платформ і смарт-контрактів;

– аналіз ризику на основі глибини ринку, розподілу активів і рівня централізації в управлінні токенами для оцінки ліквідності та волатильності токенів;

– використання аналітики блокчейну для відстеження походження активів та виявлення ризикових потоків, шляхом інтеграції процедур комплаєнсу та ПВК/ФТ.

У цифровій економіці ризики змінюються через децентралізацію, відсутність єдиного регулятора та анонімність. Необхідно вдосконалити теорію, включивши до неї невизначеність щодо правового статусу криптоактивів і зміни

регуляторного середовища та вплив алгоритмічного трейдингу, автоматизованих смарт-контрактів на зміну ризик-профілю інвесторів. Такі підходи сприяють розширенню теорії ризику та невизначеності (Ф. Найт, 1921).

У функціонуванні крипторинку учасниками ринку рішення приймаються не лише на основі раціонального очікування, а й під впливом волатильності та ажіотажу. Тому теорію очікуваної корисності (Нейман – Моргенштерн, 1944) слід доповнити оцінкою психологічних аспектів інвесторів (ефект FOMO (англ. Fear Of Missing Out) – страх втратити можливість) і визначенням корисності через довгострокову стабільність проєкту (аналіз реального використання токенів).

Переосмисленням портфельної теорії ризику (Г. Марковіц, 1952) має стати диверсифікація на крипторинку, що відрізняється від традиційних фінансових ринків, оскільки криптоактиви мають нестабільні кореляції між собою та з традиційними активами. Ліквідність багатьох цифрових активів є низькою, що ускладнює управління портфелем. Новим підходом може бути створення «динамічного криптопортфеля», де активи адаптуються в режимі реального часу через AI-аналіз ринку.

У світі цифрових активів регуляторні моделі потребують гнучкості, зокрема через запровадження механізму адаптивного регулювання, де вимоги змінюються залежно від обсягу ризиків у певній юрисдикції, використання смарт-контрактів для автоматичного виконання вимог ПВК/ФТ. Такі підходи модернізують економічну теорію регулювання ризиків (Стіглера – Пельцмана, 1971–1976).

У сфері ПВК/ФТ ризик-орієнтований підхід (РОП) дає змогу визначати категорії ризику та застосовувати відповідні заходи контролю. Міжнародні регулюючі органи, такі як FATF, рекомендують використовувати його для ефективного аналізу фінансових потоків і розроблення заходів боротьби з фінансовими злочинами. РОП широко застосовується в економіці для забезпечення стабільності та ефективності фінансових систем, а саме через

оцінку ризиків банківських установ та інвестиційних фондів, державне регулювання фінансових ринків для запобігання кризовим явищам і моніторинг трансакцій для виявлення нелегальних фінансових потоків та попередження ВК.

РОП є ефективним інструментом в економічній теорії та практиці. Він допомагає оптимізувати використання ресурсів, підвищити ефективність державного регулювання та забезпечити стабільність фінансової системи. Використання цього підходу в управлінні ризиками сприяє зменшенню економічних загроз і створенню безпечного фінансового середовища.

1.2. Міжнародні та європейські стандарти ПВК/ФТ в операціях з цифровими активами та діяльності постачальників послуг, пов’язаних з оборотом віртуальних активів

Нові технології, продукти та пов’язані з ними послуги можуть стимулювати фінансові інновації, підвищувати ефективність і покращувати доступ до фінансових ресурсів. Проте вони також відкривають нові можливості для злочинців, котрі використовують ці інструменти для відмивання грошей або фінансування незаконної діяльності. Сучасні транснаціональні організовані злочинні групи активно застосовують інтернет-технології для вчинення злочинів, передачі та приховування доходів. Завдяки глобальній доступності через комп’ютерні мережі ринок віртуальних активів має міжнародний характер, і злочинні організації, пов'язані з наркотиками та іншими правопорушеннями, використовують його можливості.

З моменту запуску в оборот першого біткоїна новітніми інструментами цікавились не тільки інвестори та розробники нової цифрової економіки, а й злочинці, особливо ті, що займаються економічними злочинами. Через відсутність державного регулювання, необізнаність правоохоронців та суддів,

такий інструмент стає цікавим для організації злочинних схем. Тому через короткий час після початку розвитку крипторинку стала проявлятись злочинна діяльність із використанням віртуальних активів. Звісно, незабаром з'явилася реакція на злочини. До 2018 р. відомими стали організація розрахунків в біткоїнах за поставку наркотиків SilkRoad, організована Ульбрехом Россом (Додаток А. Типологічне дослідження А.1), «фінансова піраміда» OneCoin, організована німкенею болгарського походження Ружою Ігнатової (Додаток А. Типологічне дослідження А.2), викрадення активів канадської криптобіржі Quadriga CX з дивними обставинами смерті її співзасновника Джеральда Коттона в Індії, котрий єдиний знав приватні ключі від криптогаманців біржі (Додаток А. Типологічне дослідження А.3), цілий потік банкрутств випусків нових криптотокенів (ICO, англ. Initial coin offering) у 2016–2018 рр.

Відповіддю на згадані злочини були не тільки започатковані переслідування з боку правоохоронних органів, а й робота над побудовою регулювання нової галузі.

Такі виклики потребують відповідної реакції з боку держави та приватного сектору, яка повинна базуватися на розумінні ризиків і реалізації узгоджених заходів. Останні мають охоплювати ефективне регулювання ринку віртуальних активів, упровадження заходів щодо ПВК/ФТ відповідно до актуальних рекомендацій FATF, Директиви ЄС щодо боротьби з відмиванням грошей (AMLD5, англ. 5th EU Anti-Money Laundering Directive [24]), а також керівних настанов FATF, Європейської комісії та міжнародної практики.

Проблема регулювання обігу нових фінансових інструментів привертає увагу як вітчизняних, так і міжнародних експертів. Однією з головних труднощів є відсутність єдиного розуміння ключових термінів: поняття «цифрові активи», «віртуальні активи», «валюти», «криптовалюти» та «цифрові гроші» часто використовуються як синоніми. Це ускладнює регулювання операцій із ВА, взаємодію з правоохоронними органами та приватним сектором, а також виконання вимог ПВК/ФТ.

З регуляторної точки зору багато ризиків, пов'язаних із віртуальними валютами, схожі на ті, що виникають при впровадженні нових технологій у фінансовій сфері. До них належать неперевірені бізнес-моделі, можливості для шахрайства та зловживань, а також недостатнє розуміння того, як відбуваються криптовалютні трансакції за допомогою технологій розподіленого реєстру (DLT). Окрім того, регуляторне середовище швидко розвивається і залишається великою мірою невизначеним.

Ключові елементи криптовалютної екосистеми істотно відрізняються від традиційних фінансових інструментів і платформ. Аутентифікація трансакцій між учасниками без посередників (peer-to-peer) спочатку була розроблена для того, щоб користувачі могли обходити інституційних посередників, котрі відіграють роль захисників у глобальних заходах із протидії відмиванню коштів. Передбачувана анонімність користувачів криптовалют може перешкоджати процедурам ідентифікації клієнтів за правилом ЗСК, що є важливою частиною політики боротьби з відмиванням грошей. Додатково онлайн-екосистема, яка підтримує обіг цифрових активів, створює нові загрози для кібербезпеки та захисту інформації. Крім того, ітеративний характер технології DLT ускладнює відкликання шахрайських або неправомірних трансакцій після їхнього здійснення. Нарешті, відсутність вбудованих географічних обмежень ускладнює вирішення питання, яка юрисдикція чи юрисдикції потенційно можуть регулювати певну послугу або трансакцію.

У такому середовищі фінансові установи та регулятори стикаються з технічно складними проблемами, що виникають у короткі терміни та часто сприймаються як непередбачувані ризики. Після початкового періоду відносної терпимості фінансові регулятори тепер активніше реагують на нові ризики та потенційні вигоди, пов'язані з криптоактивами, первинними пропозиціями токенів (англ. Initial Coin Offering, ICO) і розвитком блокчейн-платформ. Невизначений правовий статус багатьох компаній, що займаються випуском або обігом ВА, додатково посилює ризики для фінансових організацій, які

співпрацюють з такими установами, де культура управління ризиками скоріше нагадує «дикий Захід» технологічних стартапів, ніж традиційних постачальників фінансових послуг.

До 2018 р., незважаючи на заклики до впровадження глобальних стандартів ПВК/ФТ для торгівлі криптовалютами [25], таких універсальних правил не існувало. Оскільки міжнародні стандарти FATF є одним із ключових чинників протидії легалізації віртуальних активів, варто згадати міжнародні документи, розроблені Групою протягом останніх років, що сприяли формуванню правової бази і термінології.

З моменту впровадження розробленої у 2012 р. FATF методології щодо РОП до ПВК ця міжнародна організація активно відстежує ризики, пов’язані з новітніми технологіями. Особливу увагу вона приділяє загрозам, які можуть виникати через використання нових платіжних інструментів. Хоч інновації та послуги значно сприяють фінансовим інноваціям і розширенню доступу до фінансових послуг, вони також відкривають нові можливості для злочинців і терористів, надаючи їм змогу відмивати кошти або фінансувати незаконну діяльність.

У 2014 р. у відповідь на появу криптовалют і пов'язаних із ними способів передачі вартості через інтернет FATF опублікувала «Віртуальні валюти: ключові визначення та потенційні ризики ПВК/ФТ» [26]. У червні 2015 р. FATF випустила Керівництво стосовно ризик-орієнтованого підходу щодо віртуальних валют [27] у рамках поетапного підходу до визначення та управління ризиками ВК/ФТ, пов'язаними з платіжними інструментами й послугами у віртуальних валютах.

Керівництво 2015 р. акцентувало увагу на взаємодії між операціями з віртуальними валютами і традиційною регульованою фінансовою системою, зокрема через обмінні платформи для конвертації віртуальних валют, щоб забезпечити прозорість таких взаємодій. Проте цифровий простір активно розвивається, з'являються нові продукти, послуги, бізнес-моделі та способи

взаємодії, включно з обміном віртуальних активів на інші віртуальні активи. В екосистемі віртуальних активів спостерігається зростання анонімних криптовалют, використання міксерів, тумблерів, децентралізованих платформ і бірж, а також інших продуктів і послуг, які знижують прозорість операцій та ускладнюють їх відстеження.

Також з'являються нові бізнес-моделі, такі як первинні пропозиції монет (ICO), які створюють ризики ВК/ФТ, зокрема шахрайства, залучення коштів сумнівного походження та ринкових маніпуляцій. Окрім того, виникають нові незаконні схеми фінансування, що використовують цифрові середовища для подальшого ускладнення відстеження трансакцій, які здійснюються швидко і з невеликими витратами. З огляду на розроблення нових інструментів та послуг і впровадження нових типів їх постачальників у криптопросторі FATF визнала необхідність подальших роз'яснень щодо застосування її стандартів до нових технологій та їх постачальників.

У жовтні 2018 р. FATF внесла зміни до своїх Рекомендацій. Оновлена Рекомендація 15 «Новітні технології» вимагає регулювання операцій із ВА та діяльності ППВА, з метою забезпечення ПВК/ФТ [231]. Уперше в оновленій Рекомендації введено терміни «віртуальні активи» та «постачальники послуг, пов’язаних з оборотом віртуальних активів».

Віртуальний актив (ВА) – цифрове представлення вартості, яким можна торгувати в цифровому форматі або переказувати і яке може використовуватись для платіжних чи інвестиційних цілей. Віртуальні активи не включають цифрове представлення фіатних валют, цінних паперів та інших фінансових активів, які вже охоплені в інших Рекомендаціях FATF.

Постачальник послуг, пов’язаних з віртуальних активів (ППВА), характеризується як будь-яка фізична чи юридична особа, визначена як суб’єкт господарювання і провадить один або кілька таких видів діяльності чи операцій для або від імені іншої фізичної чи юридичної особи:

- обмін між віртуальними активами та фіатними валютами;

- обмін між однією або кількома формами віртуальних активів;
- переказ віртуальних активів:
- зберігання та/або управління віртуальними активами або інструментами, що забезпечують контроль над віртуальними активами;
- участь і надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажом віртуального активу.

Зокрема, визначення FATF включає як операції чи фінансову діяльність між різними видами віртуальних активів, так і операції між віртуальними та фіатними активами.

У лютому 2019 р. FATF прийняла Пояснювальну записку до Рекомендації 15 [231], що уточнює, які саме вимоги FATF мають застосовуватися до ВА та ППВА, зокрема щодо впровадження РОП до таких операцій. У Пояснювальній записці (п. 7 (b)) передбачено, що ППВА повинні отримувати від ініціатора операції та зберігати необхідну та точну інформацію про джерела і необхідну інформацію про вигодоотримувача (бенефіціара) ініціатора щодо передачі ВА, подавати зазначену інформацію до бенефіціара ППВА або фінансової установи, якщо така є, і негайно та надійним способом на запит відповідним органам влади передавати запитувану інформацію. Подібним чином бенефіціари ППВА мають «отримувати та зберігати необхідну інформацію про ініціатора операції з ВА і також надавати її за запитом відповідних органів влади негайно й надійним способом».

У контексті діяльності ППВА необхідна інформація стосується:

- ім'я автора (тобто клієнт-відправник);
- номера рахунку ініціатора, коли такий рахунок використовується для обробки трансакції (наприклад, гаманець ВА);
- фізичної (географічної) адреси ініціатора – національного ідентифікаційного номера або ідентифікаційного номера клієнта (тобто не номер трансакції), який однозначно ідентифікує особу, котра розпочала процедуру замовлення, або дату та місце народження;

- ім'я бенефіціара;
- номера рахунку бенефіціара, коли такий рахунок використовується для обробки трансакції (наприклад, гаманець ВА) [30].

Варто зауважити, що зазначені вимоги застосовуються не вперше. Вони продовжують вироблені міжнародними компаніями підходи до регулювання грошових переказів фінансовими установами, а саме: країни повинні забезпечити, щоб у контексті обробки грошових переказів ці установи вживали заходи щодо замороження, а також заборонити здійснення операцій з включеними до списку фізичними та юридичними особами відповідно до зобов'язань, визначених у відповідних Резолюціях Ради Безпеки ООН, таких як 1267 (1999) [28] та наступні пов'язані з нею резолюції, а також Резолюції 1373 (2001) [29], які стосуються запобігання та протидії тероризму і фінансуванню тероризму.

Для цього було встановлено такі вимоги до фінансових установ:

- включати необхідну та точну інформацію про джерела походження коштів клієнта, відповідні повідомлення про банківські перекази та інформацію, що супроводжує такий банківський переказ або повідомлення по всьому платіжному ланцюжку;
- відстежувати ланцюгові перекази з метою виявлення тих, кому бракує необхідної інформації про ініціатора та/або отримувача і вживати відповідних заходів;
- вживати заходів щодо заморожування та заборони проведення операцій із зазначеними фізичними і юридичними особами в контексті обробки банківських переказів [29].

Після ухвалення в червні 2019 р. Керівництва щодо впровадження РОП до операцій з ВА та діяльності ППВА [30] (далі – Керівництво), а також перегляду стандартів FATF продовжила вдосконалювати моніторинг ринку ВА та підтримувати впровадження оновлених стандартів у різних країнах.

Щодо механізму передачі інформації стосовно операції з ВА та діяльності ППВА Керівництво детально описує настанови щодо необхідної для переказу інформації:

1) Не обов'язково, щоб інформація додавалася безпосередньо до переказу ВА. Інформація може бути подана як прямо, так і опосередковано. Передбачено, що «необхідна інформація не повинна передаватися як частина або включення в переказ, що здійснюється в певному блокчейні або іншій DLT-платформі. Надання інформації до бенефіціара ППВА може бути абсолютно окремим від операції з ВА» [30]. Будь-яке технологічне або програмне рішення є прийнятним за умови, що воно дозволяє установам-бенефіціарам дотримуватися вимог Рекомендації 16 «Грошові перекази» [31].

2) FATF підкреслює, що механізм передачі інформації може бути написаним кодом в основному протоколі трансакції блокчейну переказу ВА або таким, що працює як надбудова до платформи блокчейну (наприклад, за допомогою смарт-контракту, багаторазового підпису чи будь-якої іншої технології – незалежна (тобто не обов'язково DLT-технологія) платформа обміну повідомленнями, або програма, інтерфейс програми (API), або будь-який інший ефективний (негайний та надійний) засіб для дотримання Рекомендація 16 FATF).

3) Керівництво вимагає необхідної (негайної та надійної) процедури передачі інформації, пов'язаної з ВА для обміну між ППВА-постачальником та ППВА-отримувачем. З огляду на транскордонний характер, глобальний характер охоплення та швидкість трансакції переказу ВА «негайно» означає, що ППВА повинні подати необхідну інформацію разом або одночасно із самим переказом; «надійно» означає, що ППВА повинні захистити цілісність і доступність необхідної інформації для полегшення ведення діловодства (серед інших вимог) та використання такої інформації, отриманої від ППВА або інших зобов'язаних осіб, захистити від несанкціонованого розголошення.

Керівництво також містить перелік інформації щодо оцінки ППВА з метою впровадження ризик-орієнтованого підходу для ідентифікації бенефіціарів ВА переказів, а також передачі джерела походження активів бенефіціара для подальшого переказу ВА на платформі DLT. Цей список охоплює: відкриті й приватні ключі; транспортний рівень безпеки / рівень захищених сокетів (TLS/SSL) з'єднання; сертифікати X.509; сертифікати атрибутів X.509; технологію API; іншу комерційну технологію чи програмне забезпечення або рішення для обміну даними [30].

Офіційно прийняте FATF в 2019 році у рамках Керівництва Правило подорожей FATF – це зобов'язання щодо дотримання міжнародних стандартів про боротьбу з відмиванням коштів та фінансуванням тероризму, які повинні застосовувати фінансові установи в 37 країнах – членах FATF. Його також називають Правилом криптоподорожей, оскільки вони імітують Правило подорожей Закону США про конфіденційність банківської діяльності (англ. BSA recordkeeping rules [31 CRF 103.33(e) and (f)) for funds transfers and transmittals of funds]). Крім того, вважається, що це правило зміцнює зусилля, спрямовані на боротьбу з відмиванням коштів, та політику ЗСК.

Правило подорожей прийнято в червні 2019 р. в ході проведення FATF обговорень щодо нещодавно оновлених вимог до банківських переказів.

Відповідно до Рекомендації 16 усі ініціатори та бенефіціари переказів цифрових фондів повинні обмінюватися описовою інформацією безпечно і негайно. Правило застосовуватиметься до всіх ППВА, фінансових установ та залучених до операцій організацій. До того криптоіндустрія намагалася дотримуватися політики боротьби з ВК/ФТ шляхом виконання політики «Знай свого клієнта» [191] та «Знай свою трансакцію» (англ. know your transaction, KYT; далі – ЗСТ) [33], що розкриває справжню ідентичність зареєстрованих облікових записів користувачів та підозрілих переказів криптоактивів відповідно.

Під час відкриття банківського рахунку, страхового поліса чи інвестиційної програми компанії часто застосовують політику ЗСК. Цей процес спрямований на детальне вивчення клієнта, підтвердження його особи та оцінку можливих ризиків співпраці. ЗСТ є ключовим інструментом у запобіганні ВК, шахрайству та захисті фінансових установ від загроз.

Політика ЗСТ передбачає детальний аналіз трансакцій клієнта, базований на даних. Вона охоплює контроль за ключовими фінансовими операціями на рахунку, такими як готівкові трансакції, міжнародні платежі, грошові перекази та торгові операції. Ця політика дає змогу банкам і фінансовим установам ідентифікувати, відстежувати та повідомляти про підозрілі трансакції, забезпечуючи виконання вимог законодавства. Глибокий аналіз даних трансакцій допомагає виявляти й запобігати фінансовим злочинам, підтримуючи безпеку фінансової системи.

За Рекомендацією 16 FATF передача віртуальних активів повинна містити таку інформацію, як ім’я, номер рахунку, фізична адреса, національний ідентифікаційний номер, ідентифікаційний номер клієнта, дата та місцезнаходження ініціаторів та бенефіціарів переказу, а також номери банківських рахунків, належних ініціаторам трансакції. Підприємства або фізичні особи, визначені у класифікації бізнесу як ППВА, повинні виконувати дії, пов'язані з обміном інформацією та ВА, а саме обміном, передачею, випуском, захистом та виконанням зобов'язань щодо віртуальних активів відповідно до Правила подорожей. ППВА збирають і зберігають необхідну та достовірну інформацію про активи, належну інформацію про бенефіціарів і передають її до установ-бенефіціарів, якщо такі є. Установи-бенефіціари отримують та зберігають необхідну інформацію про активи та необхідну та достовірну інформацію про бенефіціарів.

Якщо локальні ППВА не відповідають стандартам FATF, Група залишає за собою можливість накладати санкції на країни таких ППВА, додаючи їх до списку спостереження щодо високого ризику імплементації міжнародних

стандартів (сірий список) або до списку несумісності з міжнародними стандартами FATF (чорний список).

Країни ставлять дотримання положень FATF щодо ПВК/ФТ пріоритетом діяльності ППВА в усіх юрисдикціях. У березні 2019 р. було менше 20 країн, де володіння біткоїнами вважалося незаконним або обмеженим, і якщо немає відповідного рішення щодо процедур упровадження Правила подорожей не відбулося, збільшення цієї кількості може стати реальним ризиком. Коли країни стикаються з ВК/ФТ через криптоактиви найпростішим способом позбутися небезпеки є повністю заборонити них.

Але ППВА були зобов'язані забезпечити конструктивну та об'єктивну дискусію з регуляторами, щоб полегшити ситуацію не лише на теперішній момент, а й у наступному десятилітті. На додаток до численних різноманітних викликів питання процесу передачі необхідних даних для дотримання Правила подорожей щодо ППВА та подібних норм ще перебуває в процесі вирішення.

Державний сектор також почав демонструвати чітке спрямування на прийняття та впровадження переглянутих стандартів FATF. У 2021 р., коли були остаточно сформовані міжнародні стандарти ПВК/ФТ до ВА та діяльності ППВА, з 54 юрисдикцій FATF та 32 регіональних, побудованих за типом FATF юрисдикцій 13 юрисдикцій повідомили, що мали правила, які перебували у стані розроблення, і 5 юрисдикцій вказали на заборону або потенційну в майбутньому заборону діяльності ППВА [36] (рис. 1.1).

У червні 2020 року FATF завершила свій 12-місячний огляд стандартів FATF щодо ВА та ППВА [82] та оприлюднила свої висновки у своєму звіті. Цей звіт виявив, що в цілому обидва - державний та приватний сектори - досягли прогресу у впровадженні переглянутих FATF стандартів. Однак у звіті зазначено, що проблеми залишаються, оскільки режими ПВК/ФТ в деяких юрисдикціях для ППВА ще не створені або ще не функціонують. У звіті також було визначено сфери, де необхідно розширити рекомендації FATF щодо роз'яснення застосування переглянутих стандартів FATF. Одночасно з цим

звітом FATF також опублікувала свій звіт до G20 про так звані стабільні монети (стейблкоіни) [83]. У цьому звіті викладається, як переглянуті стандарти FATF застосовуються до так званих стабільних монет, та яким чином впроваджуються до них процедури ПВК/ФТ. У вересні 2020 року FATF опублікував Звіт про показники Червоних прапорців ВА щодо показників ВК/ФТ [84] для використання державним та приватним секторами.

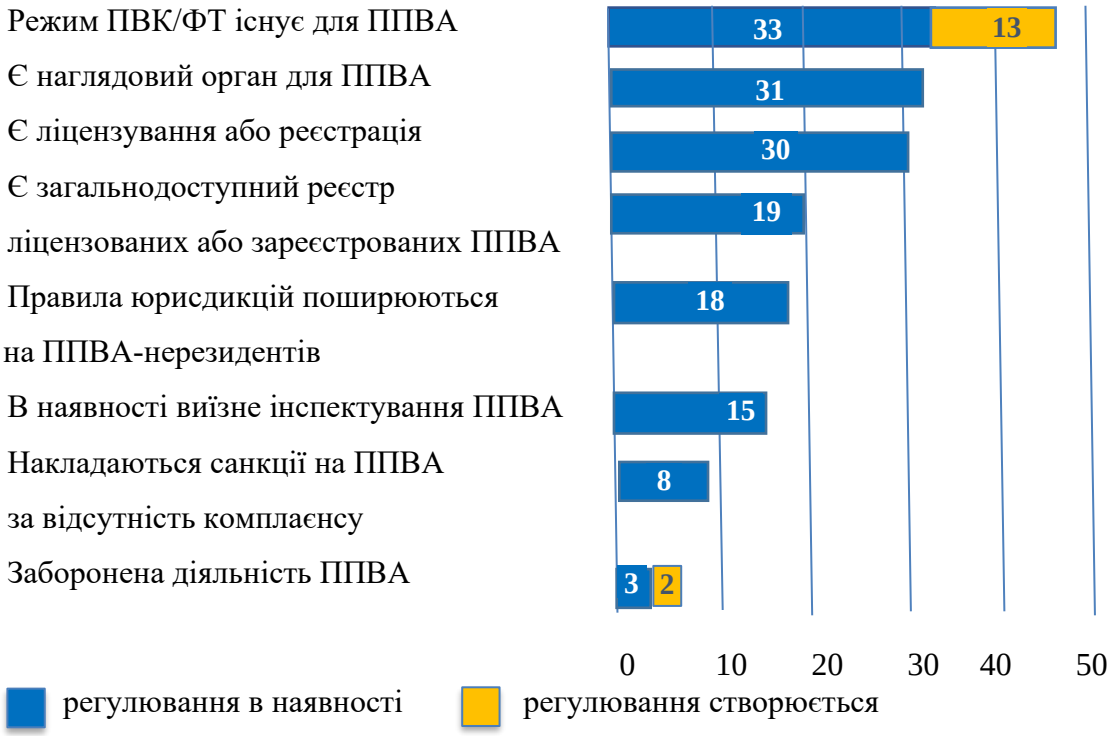


Рис. 1.1. Впровадження урядами крипто-регулятивних норм ПВК/ФТ

Джерело: складено на основі [34]

В 2020 році відбувся потік нових криптографічних норм, а також масштабні заходи правозастосування проти ППВА та їхніх керівників через відсутність відповідності нормативним актам. Прогалини в цих правилах є тими можливостями, якими користуються відмивачі грошей та терористичні організації. Зокрема, потенціал відмивання грошей крипто-валютних бірж, наявність міксерів, що змішують великі обсяги трансакцій для неможливості відслідковування ланцюга операцій, та анонімних віртуальних валют (Monero)

розглядаються законодавцями як виклик спробі регулювати цифрові активи через регулювання фіатних валют, враховуючи їхню природу.

Водночас Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN, англ. Financial Crimes Enforcement Network) оприлюднила перший набір пріоритетів щодо боротьби з відмиванням грошей та фінансуванням тероризму. Згідно із заявою FinCEN від 30.06.2021, пріоритети спрямовані на найсерйозніші загрози відмивання грошей і фінансування тероризму, з якими стикаються США [38].

Треба розуміти, що фінансові установи не зобов'язані коригувати свої комплаєнс-програми, допоки остаточні положення не набудуть чинності. Однак їм настійно рекомендується розпочати процес розгляду цих пріоритетів, таким чином визначаючи необхідні коригування на основі ризиків.

Крім того, вказані пріоритети переглядатимуться принаймні раз на чотири роки й узгоджуватимуться з появою нових та поточних загроз для критично важливої фінансової інфраструктури. Оскільки фінансові організації застосовують ці пріоритети до своїх бізнес-моделей, клієнтів, продуктів, послуг, включно з іншими банківськими каналами та платформами, географічними регіонами, вони помітять, що істотно розширені типології покриватимуть кілька пріоритетів.

"Червоні прапорці" (англ. Red flag indicators) – індикатори високого ризику ПВК/ФТ – тривожні ознаки використання інструментів ринку віртуальних активів у діяльності фінансових установ та учасників ринку віртуальних активів з метою відмивання доходів, отриманих злочинним шляхом, фінансування тероризму та розповсюдження зброї масового знищення, шахрайства й кіберзлочинності. Деякі з "червоних прапорців" і прийомів, що часто використовуються злочинними організаціями, можуть бути застосовані до багатьох пріоритетів. Виявлення їх стає простішим і очевиднішим, коли ці прийоми та тригери повторюються в серії ризиків. Поширене питання, яке ставлять фінансові організації, має на увазі визначення і розуміння сутності

злочинів та того, як вони впливають на фінансові операції й операції з віртуальними активами [39].

Найбільш масштабним та впливовим злочином є корупція. Згідно з національним законодавством, “корупція – використання особою, зазначеною у частині першій статті 3 цього Закону [40], наданих їй службових повноважень чи пов’язаних з ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди особі, зазначеній у частині першій статті 3 цього Закону, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов’язаних з ними можливостей”. Інакше кажучи, корупція – це зловживання довіреною владою для отримання особистої вигоди, зазвичай пов’язане з розкраданням і хабарництвом. Відомо, що корупція спричиняє руйнівні соціальні, політичні та економічні наслідки. Політично значущі особи (PEP, англ. Politically exposed person) можуть мати вищий ризик, якщо оцінювати їх за цим пріоритетом [39].

При виявленні корупції варто звернути увагу на такі “червоні прапорці”:

- операції із залученням складних структур;
- операції між державними підприємствами та компаніями в юрисдикціях високого ризику;
- процеси, призначені для захисту кінцевого бенефіціарного власника;
- спрямування коштів через юрисдикції зі слабким регулятивним наглядом.

Наступними за обсягами завданої шкоди визначено кіберзлочинність та використання віртуальних валют у злочинних операціях. FinCEN характеризує кіберзлочинність як будь-яку незаконну діяльність із використанням комп’ютера, іншого цифрового пристрою чи комп’ютерної мережі. Доцільно групувати пов’язані з кіберзлочинами злочини у дві категорії: вчинені із залученням або атаками на мережі інформаційних технологій (IT) і ті, що є

злочинами, в яких кіберекосистему було застосовано для вчинення або підтримки злочину. Незважаючи на те, що ці дві категорії здаються дуже схожими, типології, методи та рівень кіберекспертизи надзвичайно відрізняються.

Третім за обсягами злочином визнано зовнішнє (іноземне) та внутрішнє фінансування тероризму. Визначення останнього може здатися простим на перший погляд. Тероризм, і внутрішній, і зовнішній, характеризується як насильницька злочинна діяльність, вчинена окремими особами та/або групами з метою примусу уряду чи його громадян до досягнення певних політичних чи соціальних цілей. Однак, коли до цього пріоритету застосовується так звана фінансова лінза, розслідування та збір доказової бази можуть стати доволі складними, як у випадку з використанням коштів із законним джерелом походження для підтримки актів насильства. Важливо пам'ятати, що до певних порушень у сфері фінансування тероризму висувають спеціальні вимоги до звітності, котрі можуть вимагати негайного вжиття заходів. Цей пріоритет є точкою перетину, де оцінюються дотримання санкцій та протидія відмиванню коштів. Варто підкреслити, що рейтинг ризику останнього і санкцій для клієнта може перебувати на різних рівнях, тобто низький ризик для відмивання коштів і високий – для санкцій [41].

Приклади поєднання подібних ризиків ми можемо бачити в уникненні з використанням криптоактивів міжнародних санкцій щодо збройної агресії з боку рф, коли з рахунків російських банків грошові кошти було виведено через крипто обмінники та криптобіржі за межі країни-агресора. Ці операції з грошовими (фіатними) та віртуальними активами для повернення в легальну економіку будуть потребувати подальшого їх відмивання.

Основні ознаки виявлення фінансування тероризму такі:

- трансакційна діяльність не відповідає профілю клієнта (наприклад, звичайні клієнти починають спрямовувати свої прибутки на підтримку терористичної мережі);

- грошові перекази певних осіб через АТМ-банкомати відбуваються в різних країнах одночасно;
- використання фінансування неприбуткових громадських організацій (НГО) не відповідає їхній заявленій меті;
- шахрайство.

Щодо ймовірної ролі НГО у фінансуванні тероризму, то до таких фінансових та криптотрансакцій необхідно застосовувати згадану нами «фінансову лінзу» [39]. Наразі слід дуже ретельно вивчати діяльність неприбуткових громадських організацій та благодійних фондів, не забуваючи про їхній великий внесок у протистояння російській збройній агресії, та швидко реагувати на використання діяльності таких організацій як прикриття злочинних цілей, часто саме шахрайства.

Загалом шахрайство характеризується навмисними діями, котрі мають оманливий характер і спрямовані на надання шахраю неправомірних переваг і фінансової вигоди. За даними FinCEN, злочини, пов’язані з шахрайством, генерують найбільшу кількість незаконних доходів у США. Фінансові установи повинні боротися з шахрайством двома способами: вживати заходів проти клієнта та проти самої установи, включно з її каналами надання банківських послуг. Ці два ризики відмінні, так само як кіберзлочинна діяльність клієнта та фінансування клієнтом кіберзлочинів, охоплюють різні методи, інструменти й рівні складності. Варто наголосити, що рейтинг клієнта стосовно відмивання коштів, шахрайства та санкцій може відрізнятися й вимагатиме відмінних рівнів моніторингу та належної обачності.

«Червоними прапорцями» для цього виду фінансових злочинів є:

- платежі кредитною карткою непов’язаними третіми особами;
- раптові великі обсяги трансакцій на малоактивний рахунок;
- отримання кредитів без законної мети;
- діяльність транснаціональної злочинної організації.

Транснаціональні злочинні організації – це злочинні групи або злочинні мережі, котрі діють на міжнародному рівні з метою отримання влади, впливу та/або фінансової вигоди незаконним шляхом [39]. Таким групам необхідно відмивати кошти та переміщувати доходи/вартість їхніх злочинів між країнами. Тому мірою зростання вони передають свої фінансові операції професійним відмивачам грошей. Про складність цього пріоритету свідчать окремі злочини, котрі охоплюють торгівлю дикою природою, екологічні злочини, торгівлю людьми, наркотиками.

До основних ознак діяльності транснаціональних злочинних організацій належать такі:

- суми трансакцій не відповідають діяльності підприємства;
- переказ коштів із рахунків підприємств відбувається на особисті рахунки;
- підприємства зі значним обсягом операцій з готівкою беруть участь у міжнародних торгових операціях або фінансують їх;
- послуги віртуального обміну іноземної валюти послідовно використовуються для приховування особи;
- провадиться організована діяльність із незаконного обігу наркотиків.

Стосовно злочинів, пов’язаних із продажем, транспортуванням або незаконним імпортом наркотиків / незаконних контрольованих речовин, організації можуть підпадати під пріоритет «Транснаціональна організована злочинність». Організації, котрі займаються торгівлею наркотиками, генерують великі суми готівки, що створює труднощі у викритті цих злочинних мереж. Незважаючи на те, що фінансові організації повинні детально вивчати (застосовувати згадувану “фінансову лінзу”) типології, а саме знати які фінансові й нефінансові інструменти використовуються, як вони комбінуються та за якою методикою для отримання найвищого ефекту, які витрати необхідні тощо, за цими злочинами та пов’язаною з ними діяльністю, існує низка рекомендацій,

котрі можуть допомогти полегшити цей тягар: визначити коригування власних програм, базованих на оцінці ризиків, і процесів оцінювання, включно з вказаними пріоритетами.

У червні 2021 року FATF розглянув прийняття вдосконалених галузевих настанов з оцінки ризику та майбутніх кроків для протидії злочинній діяльності на ринку ВА. Необхідно зауважити, що чим більш гармонізовані правила між усіма учасниками національних систем ПВК/ФТ, тим легше їх впроваджувати в діяльність галузі та застосовувати як на національному рівні, так і на глобальному ринку.

Нарешті, у жовтні 2021 року FATF оприлюднила свої оновлені Керівні принципи щодо підходу до контролю за ПВК/ФТ на основі оцінки ризику [36]. Незважаючи на те, що цей звіт стосується нагляду щодо ПВК/ФТ, він містить доволі значну інформацію щодо пруденційного нагляду за ППВА.

Звіт про огляд ринку ВА за дванадцять місяців [35] та Звіт FATF до Міністрів Фінансів та Керівників Центральних Банків G20 [43] зобов'язали FATF випустити для державного та приватного сектору оновлене Керівництво щодо переглянутих стандартів FATF та їх застосування до ВА та ППВА [42]. Зокрема, у двох доповідях викладені шість основних тез, в які були внесені зміни. Для вирішення нових викликів Керівництвом були поставлені такі цілі:

- пояснити визначення ВА та ППВА (визначення ВА та ППВА повинні бути експансивними і не було випадків, коли крипто актив чи традиційний фінансовий актив не охоплюється стандартами FATF);
- пояснити як стандарти FATF застосовуються до так званих стабільних монет (стейблкоінів);
- надати додаткові вказівки щодо ризиків та заходів з потенційного зниження ризику для однорангових трансакцій;
- надати оновлені вказівки з ліцензування та реєстрації ППВА;
- надати додаткові вказівки для державного та приватного секторів з впровадження «Правила подорожей»;

– включити Принципи обміну інформації та співпраці між керівниками ППВА.

Вимоги Правила подорожі спрямовані на запобігання використанню електронних переказів коштів терористами та іншими злочинцями, а також на виявлення таких зловживань у разі їх виникнення. Згідно з 16 Рекомендацією FATF, країни повинні зобов'язати фінансові установи отримувати та передавати точну інформацію про відправника та отримувача (бенефіціара) коштів. Ці дані мають супроводжувати платіжні транзакції на всіх етапах їх проходження [31].

Крім того, фінансові установи повинні контролювати грошові перекази, щоб виявляти ті, які не містять повної необхідної інформації про відправника або отримувача. У таких випадках вони мають застосовувати відповідні заходи для запобігання потенційному фінансовому зловживанню.

Незважаючи на те, що FATF зазначає, що деякі країни запровадили регуляторні режими для ВА та ППВА, багато юрисдикцій ще не мають ефективної системи у сфері ПВК/ФТ для пом'якшення ризиків ВК/ФТ, пов'язаних з обігом ВА, попри те, що діяльність ринку ВА стрімко розвивається по всьому світу та ППВА проводять дедалі більше операцій.

Швидкий розвиток, зростаюча функціональність, все більше визнання та глобальна, транскордонна природа ВА спричиняють застосування негайних дій, спрямованих на зменшення ризиків ВК/ФТ, і є ключовим пріоритетом FATF. Експерти Робочої групи FATF стверджують, що криптогалузь краще представити за допомогою простої структури та набору ресурсів, які всі ППВА можуть використовувати для створення шляху впровадження міжнародних стандартів ПВК/ФТ на основі власних потреб і вимог місцевої юрисдикції.

Як зазначено вище, Керівництво FATF щодо РОП до операцій з ВА та діяльності ППВА, оприлюднене ще у 2019 р., визначило, що цифрові валюти центральних банків (CBDC, англ. Central bank digital currency) не є ВА. Однак міжнародні стандарти FATF застосовуються до CBDC як до іншої форми фіатних валют, випущеної центральним банком. Цифрові валюти центральних

банків можуть мати унікальні ризики у сфері ВК/ФТ порівняно з фізичною фіатною валютою залежно від їхньої конструкції. Виключення їх огляду в Керівництві не означає, що FATF вважає їх неважливими – швидше, такий підхід вибудовано як результат того, що вони класифікуються як суверенні цифрові валюти, а не як ВА [42].

У розвитку цифрової економіки є місце і для криптоактивів, і для цифрових валют центральних банків, і для приватних валют комерційних банків та приватних фінансових груп. Головне – створити правову базу для їхньої діяльності та державного та приватного управління.

В розвитку цифрової економіки є місце і для криптоактивів, і для цифрових валют центральних банків, і для приватних валют комерційних банків та приватних фінансових груп. Головне – це створити правову базу для їхньої діяльності та державного та приватного управління.

На тлі розвитку цифрових фінансів змінюються підходи до публічно-приватного менеджменту. Розвиток законодавства потребує реагування на використання новітніх інструментів у злочинних схемах і забезпечення розвитку інновацій. Тому слід упровадити конкретні й суттєві заходи з реагування та превентивної діяльності, спрямованої проти модернізації злочинності, і сучасні підходи, такі як регуляторні пісочниці для подальшого інноваційного розвитку.

Державні регуляторні пісочниці – це спеціально створені зони або платформи, де інноваційні підприємства та стартапи можуть тестувати нові технології, бізнес-моделі та продукти в контрольованих умовах із зниженими нормативними обмеженнями. Такий підхід дозволяє експериментувати з інноваційними рішеннями, не порушуючи при цьому основних принципів захисту споживачів та фінансової безпеки [23].

Державні органи можуть спостерігати за результатами тестування нових технологій та бізнес-моделей, що дозволяє виявити недоліки існуючого законодавства і оперативно внести необхідні зміни для підтримки інновацій. Пісочниці дозволяють учасникам тестувати свої рішення, не зобов’язуючись

відразу дотримуватися всіх чинних законодавчих вимог, що стимулює інновації. Регуляторні пісочниці сприяють активній взаємодії між державними органами, підприємствами і технологічними стартапами, що дозволяє обмінюватися досвідом і розробляти спільні підходи до впровадження нових технологій. Коли інноваційні рішення проходять тестування у контрольованому середовищі, це сприяє підвищенню довіри з боку інвесторів, користувачів та інших зацікавлених сторін, що є важливим чинником для масштабування і подальшого розвитку технологій. Використання регуляторних пісочниць сприяє гармонізації національних нормативних актів із міжнародними стандартами, що дозволяє країні стати привабливішою для іноземних інвестицій і сприяє розвитку глобального ринку цифрових технологій.

Технологія блокчейн, що є основою для обороту цифрових активів, виступає каталізатором масштабних змін у сфері грошей і фінансів, які матимуть значний вплив на домогосподарства, корпорації, інвесторів, центральні банки та уряди. Завдяки можливості безпечного володіння виключно цифровими активами ця технологія сприяє розвитку нових фінансових інструментів, зокрема незамінних токенів (NFT).

Водночас центральні банки стурбовані наслідками як для фінансової, так і для економічної стабільності, якщо децентралізовані платіжні системи або приватні стейблкоїни витіснять як готівку, так і традиційні платіжні системи, якими керують регульовані фінансові установи. Платіжна інфраструктура, що повністю належить приватному сектору, може бути ефективною та економічно вигідною, проте окремі її компоненти можуть зазнати збою в разі втрати довіри під час фінансових потрясінь.

У відповідь на такі занепокоєння центральні банки розглядають можливість випуску цифрових форм грошей центрального банку для роздрібних платежів у вигляді CBDC. CBDC мають потенційні переваги. Вони перешкоджатимуть незаконній діяльності, такій як торгівля наркотиками, відмиванню грошей і фінансування тероризму, що покладаються на анонімні

грошові операції. Це б вивело більше економічної діяльності з тіні до легальної економіки і ускладнило б можливості ухилення від податків. Також малі підприємства виграли б від знижених трансакційних витрат і уникнули б труднощів і ризиків, пов'язаних з обслуговування готівки. Однак CBDC мають і недоліки.

Комерційні банки мають вирішальне значення для створення та розподілу кредитів, які забезпечують безперебійне функціонування економіки. Традиційні фінансові установи, особливо комерційні банки, стикаються з проблемами своїх бізнес-моделей, оскільки нові технології породжують онлайн-банки, що можуть охопити більше клієнтів і вебплатформи, такі як Prosper [44], здатні безпосередньо з'єднувати вкладників і позичальників. Ці нові установи та платформи загострюють конкуренцію, сприяють інноваціям і знижують витрати. Вкладники отримують доступ до ширшого набору заощаджень, кредитів і страхових продуктів, тоді як малі підприємці також можуть отримати фінансування з джерел, відмінних від банків, які зазвичай мають менш суворі вимоги до розміщення кредитів і вимог їхнього забезпечення. Внутрішні й міжнародні платежі стають дешевшими та швидшими, що приносить користь споживачам і компаніям.

Основні резервні валюти, особливо долар США, ймовірно, збережуть своє домінування як засоби збереження вартості, оскільки воно залежить не лише від економічного розміру країни-емітента та глибини фінансового ринку, а й від міцної інституційної основи, яка є важливою для підтримки довіри інвесторів. Цифрові гроші центрального банку настільки сильні та надійні, наскільки сильна і надійна установа, що їх випускає.

Станом на початок 2023 р. дев'ять із десяти центральних банків експериментують із цифровими версіями фіатних валют у секторах роздрібної та оптової торгівлі [45], причому більш як 50 % банків нині проводять конкретні експерименти або розробляють CBDC, поки політики готують нормативну базу для криптоактивів, CBDC відкриває абсолютно нову економічну модель за

допомогою програмованих гаманців і атомарних переказів (атомарна трансакція — це неподільна і незвідна серія операцій з базою даних, при якій або відбувається все, або нічого не відбувається), що допомагають стимулювати фінансову доступність. За підтримки регуляторів і центральних банків CBDC можуть спиратися на наявні дворівневі фінансові системи, одночасно використовуючи DLT для вивчення інноваційного потенціалу.

Фінансова стабільність опинилася на першому місці в переліку пріоритетів для центральних банків і регуляторів через пандемію коронавірусу та подальші геополітичні події. Крім того, загальне визнання криптовалют як альтернативної форми оплати проклало шлях для експериментів CBDC у більшості регіонів.

CBDC — цифрова валюта, випущена центральним банком і номінована в національній (фіатній) валюті. Вона є не просто «цифровими грошима», а безпосереднім зобов'язанням центрального банку. Існує два основних типи CBDC: роздрібні та оптові. Особливу увагу центральні банки приділяють роздрібним CBDC (згідно з опитуванням BIS 2021 р. щодо цифрових валют і токенів [46]). Близько 20 % центральних банків розробляють або тестують роздрібні CBDC, що вдвічі більше, ніж тих, хто працює над оптовими версіями. Роздрібні CBDC орієнтовані на широке використання споживачами як новий засіб для розрахунків і платежів. Вони здебільшого охоплюють невеликі трансакції зі значним обсягом між громадянами та бізнесом. Такі валюти можуть усунути посередників, що спрощує проведення платежів, знижує витрати й скорочує час на розрахунки. Роздрібні CBDC набирають обертів: останнім часом запустили свої цифрові валюти такі країни, як Багамські Острови (SendDolar), Нігерія (eNaira), Східні Кариби (DCash) і Китай (DCEP).

Китай є однією з найбільших економік, що досягла значних успіхів у впровадженні CBDC, започаткувавши пілотні програми в кількох регіонах країни. До кінця 2021 р. було відкрито понад 250 млн електронних гаманців, а обсяг трансакцій у e-CNY перевищив 85 млрд юанів [47]. Водночас США розглядають можливість заборони цифрового юаня через побоювання щодо

конфіденційності та безпеки [48]. У Сінгапурі Грошово-кредитне управління відібрало 15 інноваційних рішень для роздрібних CBDC, спрямованих на покращання платіжних систем [49]. Банк Японії перейшов до другої фази експериментів із CBDC [46].

Оптові CBDC призначені для використання в розрахунках між банками та центральним банком, охоплюючи високовартісні, але нечисленні трансакції між фінансовими установами. Вони можуть підвищити ефективність і покращити управління ризиками, особливо у сфері транскордонних платежів. Ключовим елементом успішної реалізації оптових CBDC стане забезпечення їх взаємодії між різними системами [50].

Грошово-кредитне управління Гонконгу у співпраці з Банком Таїланду розширило свою роботу над оптовою CBDC (спочатку названо проєктом Inthanon-LionRock) для подальших експериментів. Центральний банк Об’єднаних Арабських Еміратів, Інститут цифрової валюти Народного банку Китаю та Гонконгський центр BIS Innovation Hub долучилися до ініціативи, і тепер його перейменовано на mBridge [52]. Цей етап включатиме подальші експерименти та пошук джерел для підвищення ефективності транскордонних переказів.

Сьогодні центральні банки розглядають три моделі випуску, розподілу та розрахунків за CBDC – пряму, непряму та гібридну. У прямій моделі центральний банк надає послуги рахунку та гаманця безпосередньо кінцевим споживачам без жодних посередників. Непряма модель схожа на поточну систему роздрібного банківського обслуговування, де посередники відповідають за адаптацію клієнтів, політик ЗСК та ПВК/ФТ, керування рахунками та гаманцями. Також розглядається гібридна модель, яка поєднує в собі аспекти прямої та непрямої моделей.

Понад 70 % центральних банків, що вивчають CBDC, розглядають непряму модель, оскільки пряма модель збільшує накладні витрати центрального банку та може призвести до неефективності. Запропонована Банком Англії

модель платформи теж є непрямою, з державно-приватним партнерством, де банк запропонує основну книгу для CBDC, а постачальники платіжних інтерфейсів запропонують додаткові платіжні послуги та будуть взаємодіяти з кінцевими користувачами [46].

Хоча CBDC можуть підвищити операційну ефективність, рівень безпеки та зручність обміну валюти, окремі мережі CBDC, незалежні від міжнародної інфраструктури, здатні призвести до фрагментації та формування кількох паралельних систем.

Більшість центральних банків, які працюють над роздрібними CBDC, теж вивчають можливість взаємодії з наявними платіжними системами. Проєкт Dunbar, очолюваний Інноваційним центром BIS у партнерстві з Резервним банком Австралії, Центральним банком Малайзії, Валютним управлінням Сінгапуру та Резервним банком Південної Африки, розробив спільну платформу для міжнародних розрахунків за допомогою кількох CBDC [54].

Постачальники платіжних послуг відіграватимуть ключову роль у забезпеченні взаємодії та дедалі більшу роль у впровадженні CBDC. SWIFT у співпраці з Capgemini проводив нові експерименти з об’єднання внутрішніх CBDC для забезпечення безперебійних транскордонних платежів [55]. Visa також співпрацює з ConsenSys для з’єднання нещодавно розроблених мереж CBDC із традиційними фінансовими установами [56].

Упровадження та розвиток CBDC можуть значно підвищити ефективність валютних операцій як на регіональному, так і на глобальному рівні. У міру поширення роздрібних CBDC роздрібні банки зможуть запропонувати нові послуги, пов'язані з електронними гаманцями та зберіганням активів через непряму модель. Зі збільшенням доступності CBDC для населення через цифрові гаманці очікується також зростання фінансової інклюзії.

CBDC вже стали важливою складовою фінансової системи, і очікується, що ринки, які розвиваються, будуть лідерами у впровадженні цих валют, а зі

зміною правових і нормативних вимог глобальна система обміну на базі CBDC може скоро стати реальністю.

Однак центральні банки та їхні партнери з роздрібного сектору повинні враховувати ризики нової технології, такі як кіберзагрози та можливі наслідки для фінансової і монетарної політики. Для успішного запуску необхідно розробити поетапний план, який міститиме заходи з управління ризиками.

Визнаючи важливість цифрових платежів для сприяння фінансовій доступності, центральні банки все частіше прагнуть розширити свій інструментарій для задоволення платіжних потреб громадян, використовуючи інновації в галузі цифрових платежів. Цифрові валюти центрального банку (CBDC) є одним з таких інструментів, популярність якого зростає протягом останніх кількох років. У англомовних джерелах такі валюти отримали скорочену назву, яким також будемо оперувати у межах цього дослідження.

Мотиви впровадження CBDC центральними банками включають зміцнення фінансової стабільності, підвищення ефективності монетарної політики, удосконалення платіжних систем і покращення фінансової інклюзії. За даними CBDC Tracker Атлантичної ради станом на квітень 2023 року, «114 країн, на які припадає понад 95% світового ВВП, розглядають можливість запровадження цифрової валюти центрального банку» [57]. З них одинадцять країн вже використовують CBDC (Ямайка — остання з них із JAM-DEX), а 18 країн, включно з Україною, запустили пілотні проекти. Також фінансові санкції проти Росії змусили країни шукати платіжні системи, що не залежать від долара. Наразі триває дев’ять транскордонних оптових тестів CBDC і сім проєктів у сфері транскордонних роздрібних платежів, що майже вдвічі більше, ніж у 2021 році.

Станом на квітень 2023 року 32 країни перебувають на стадії розробки CBDC, а більшість із 39 країн все ще проводять дослідження. Запровадження цифрової валюти вимагає обережного підходу через наявні ризики, такі як правові вимоги до конфіденційності та безпеки даних [57]. Це потребує

додаткових досліджень щодо відповідності CBDC чинному законодавству. Таким чином, прогрес у розробці готових продуктів може ускладнюватися через низку правових і регуляторних викликів як на національному, так і на міжнародному рівнях, особливо в межах Європейського Союзу.

Загалом, правові проблеми, пов'язані з обігом CBDC, продовжують загострюватися. Зростає кількість публікацій, присвячених двом ключовим питанням. Одне з них - як центральні банки повинні створювати роздрібні цифрові гроші і чи бажано, щоб CBDC замінили фізичну готівку (Т. Кейстер та Д. Санчес (2023) [58], М.К. Бруннермайер, Х. Джеймс та Дж. П. Ландау (2019) [59]). З іншого боку, йдеться про системні наслідки такої валюти і про те, як впоратися з пов'язаними з ними ризиками та нестабільністю, які вони можуть спричинити ((Ф. Аллен, С. Гу, Д. Джагтіані (2022) [60], М. К Бруннермайер, Х. Джеймс, і Дж. П. Ландау (2019) [52], Д. Ніпельт (2018) [61], Дж. Фернандес-Віллаверде, Д. Санчес, Л. Шиллінг, Х. Уліг (2021) [56], А. Венеріс, А. Парк, Ф. Лонг та П. Пурі (2021) [62]).

Впровадження цифрових валют центральних банків (CBDC) стало предметом інтенсивних дискусій, зокрема через системні наслідки, які можуть виникнути в результаті їх широкомасштабного застосування. Ф. Аллен, С. Гу та Д.Джагтіані (2022) [60] наголошують на тому, що хоча CBDC можуть значно підвищити ефективність платіжних систем, вони також можуть створювати ризики фінансової нестабільності, зокрема шляхом зміни структури депозитів та впливу на ліквідність банківської системи.

Бруннермайер, Джеймс і Ландау (2019) [52] зазначають, що введення CBDC може спричинити значні трансформації в грошово-кредитній політиці та механізмах фінансового посередництва. Зокрема, йдеться про потенційне зменшення ролі комерційних банків у процесі емісії грошей, що, своєю чергою, здатне посилити волатильність фінансових потоків, особливо в періоди криз.

Ніпельт (2018) [61] підкреслює, що введення CBDC може посилити "банківські набіги" через спрощення доступу вкладників до ліквідних активів під

час кризових ситуацій. Це може призводити до дестабілізації фінансової системи через швидкі та масові переміщення активів між банками і цифровою валютою центрального банку.

Фернандес-Віллаверде, Санчес, Шиллінг та Уліг (2021) [56] акцентують увагу на тому, що ефективне впровадження CBDC вимагає розробки детальних механізмів контролю за потенційними ризиками кібербезпеки, фінансової стабільності та захисту персональних даних. Саме ризики конфіденційності та прозорості транзакцій є ключовими аспектами, які необхідно ретельно врегулювати.

Венеріс, Парк, Лонг та Пурі (2021) [62] додатково наголошують на необхідності чіткої нормативної бази, яка б передбачала обов'язкове забезпечення підзвітності транзакцій, водночас захищаючи конфіденційність громадян. Це є особливо важливим у контексті протидії відмиванню коштів (ПВК) і фінансуванню тероризму (ФТ).

Н. Почер та А. Венеріс у своїй роботі «Конфіденційність і прозорість у CBDC: схеми ПВК/ФТ, розроблені за проектом» [64] пропонують техніко-юридичну таксономію підходів, яка дозволяє досягти балансу між конфіденційністю та прозорістю. Їхній підхід передбачає застосування криптографічних методів, які забезпечують відповідність вимогам з ПВК/ФТ, але при цьому мінімізують втручання в приватність користувачів.

Кейстер та Санчес (2023) [58] додають важливий аспект щодо створення роздрібних цифрових грошей центральними банками. Вони стверджують, що центральні банки повинні ретельно зважити наслідки впровадження CBDC, оскільки їх широке використання може суттєво змінити грошову динаміку і навіть поставити під питання існування фізичної готівки. У контексті заміни фізичної готівки, Бруннермайер, Джеймс і Ландау (2019) [52] підкреслюють необхідність обережного підходу. Вони застерігають, що повна заміна готівки на CBDC може призвести до виключення певних соціальних груп з фінансової системи та посилення ризиків кібернетичних атак.

Таким чином, системні наслідки впровадження CBDC потребують комплексного підходу до управління ризиками. По-перше, необхідне чітке регулювання взаємодії CBDC з комерційними банками для запобігання фінансовій дестабілізації. По-друге, важливо розробити та імплементувати передові технологічні рішення у сфері кібербезпеки та конфіденційності, які забезпечуватимуть прозорість і водночас приватність. Нарешті, необхідна глобальна координація нормативно-правового поля, яка дозволить уникнути регуляторного арбітражу та сприятиме ефективному міжнародному контролю над обігом цифрових валют центральних банків. Центральні банки, зокрема, повинні враховувати соціальні, технологічні та економічні наслідки повної заміни фізичної готівки на CBDC, забезпечуючи таким чином фінансову інклюзивність та стабільність.

Спираючись на наявний науковий доробок, вбачається за доцільне окреслити перспективи якісних трансформацій з відповідних питань у правовому регулюванні CBDC в Україні, що на даний час є малодослідженим у науковій площині.

Водночас, як вже зазначалося вище, впровадження е-гривні може призвести до низки позитивних, і негативних наслідків. Зокрема, з одного боку вона сприятиме оптимізації фінансового моніторингу, доступності платежів, швидкості трансакцій, зниженню вартості міжнародних переказів, протидії корупції завдяки прозорості трансакцій тощо, а з другого – загрожуватиме конфіденційності та безпеці платежів. Наприклад, засновник Cardano Чарльз Хоскінсон розглядає CBDC як інструмент контролю за населенням і вважає її найнебезпечнішим новаторством у грошово-кредитній політиці [64].

Крім того, на думку вчених Американського інституту економічних досліджень (American Institute for Economic Research) упровадження CBDC є небезпечним. «Зустріч із загрозою авторитарного суперника шляхом використання небезпечних технологій соціального контролю повністю суперечить суспільству. Було б доцільніше інвестувати в покращання платіжної

системи, а не в заміну цієї системи на CBDC, яка надасть уряду безпрецедентний контроль над фінансовими операціями» [65] .

Слід зауважити, що питання ризиків конфіденційності та безпеки платежів, пов'язаних із запровадженням CBDC, мають глобальний характер. Наприклад, згідно з інформацією на офіційному сайті Європейського центрального банку після публікації звіту Євросистеми про потенційний цифровий євро, у рамках публічного обговорення (яке розпочалось в жовтні 2020 р.) на адресу регулятора надійшло понад 8 тисяч коментарів, з яких 41 % становлять коментарі щодо «конфіденційності платежів» [66].

Протягом 2022 р. було підготовлено звіти Європейського центрального банку «Прогрес на етапі дослідження цифрового євро (вересень 2022 р.) та «Прогрес на етапі дослідження цифрового євро – другий звіт» (грудень 2022 р.). Перший звіт охоплює такі теми, як механізм переказу, конфіденційність та інструменти контролю кількості цифрових євро в обігу. Другий звіт присвячений ролям посередників, моделі розрахунків, фінансуванню та вилученню коштів, а також моделі розподілу цифрового євро [67].

Робота у відповідному напрямі ще триває. Завершення досліджень щодо можливого дизайну цифрової валюти було заплановано на осінь 2023 р., але досі триває. Лише після цього Рада керуючих ЄЦБ вирішить, чи переходити до етапу реалізації та запуску цифрового євро у практику. При цьому відповідно до інформації Європейської комісії на офіційному сайті виконавчий орган Європейського Союзу планує опублікувати законопроєкт про підтримку цифрового євро та стратегії щодо віртуальних світів у травні 2023 р.

Незважаючи на те, що Європейський центральний банк ще не вирішив, чи випускати е-євро, Єврокомісія вказала, що можуть знадобитися нові закони, аби підтвердити статус цифрового євро як законного платіжного засобу та встановити правила боротьби з ВК.

Подібна практика спостерігається і США. Так, було прийнято указ № 14067 від 09.03.2022 [68], відповідно до якого президент Джозеф Байден

підтримав дослідження впровадження CBDC у практику та наголосив на необхідності рішучих кроків для зниження ризиків, які цифрові активи можуть становити для споживачів, інвесторів і захисту бізнесу, включно з конфіденційністю та безпекою даних. Цей нормативно-правовий акт спричинив шквал критики та появу законопроєктів про конфіденційність CBDC із боку членів Конгресу. Наприклад, представник США і голова робочої групи з фінансових технологій Стівен Лінч на підтримку розроблення американської цифрової валюти представив Закон про електронну валюту і безпечне апаратне забезпечення (Electronic Currency and Secure Hardware) у квітні 2022 р. Мета закону полягає в розробленні пілотної програми для цифрового долара, яка імітує «функції фізичної готівки, що поважають конфіденційність», закликаючи до включення «ключових гарантій безпеки та функціональності», зокрема: «(1) анонімність, (2) конфіденційність і (3) мінімальне генерування даних про трансакції» [69].

Законопроєктна робота втілилися в серію міжвідомчих звітів про наслідки CBDC США, де основна увага приділяється приватності за задумом (ідея про те, що права на приватність повинні бути враховані при розробленні будь-якого продукту або системи на початкових етапах).

Наприклад, Міжвідомча технічна оцінка, проведена у вересні 2022 р., виявила кілька наслідків проєктування CBDC, пов'язаних із захистом приватності, у тому числі потенційну можливість: (1) «порушити поточний баланс між конфіденційністю індивідуальних даних та особливими потребами правоохоронних органів щодо нагляду за фінансовими операціями на предмет незаконної діяльності»; (2) «створити ризики для конфіденційності, пов'язані зі збором, зберіганням та передачею платіжної інформації і пов'язаної з нею інформації, що ідентифікує бізнес та особу»; (3) «спричинити вимоги щодо повідомлення про порушення даних і реагування на них» на державному та міжнародному рівнях. Крім того, Міністерство фінансів визначило конфіденційність як ключовий аспект упровадження CBDC, підкресливши, що

«розроблення CBDC може вимагати переоцінки наявних стандартів конфіденційності» загалом, включно з будь-якими подальшими законодавчими рішеннями, які можуть стосуватися «сірих зон» в американському законодавстві про конфіденційність [70].

Серед найактуальніших питань, на яких наголошується в загальнодоступних звітах як ЄС, так і США щодо впровадження цифрової валюти, виокремлюються:

- доцільність залучення посередників,
- важливість дотримання політики ЗСК і ПВК/ФТ, законів і нормативних актів з одночасним дотриманням законів і нормативних актів про фінансову конфіденційність, і
- характер і ступінь захисту конфіденційності, що надається фізичним особам за допомогою загальнодоступних DLT, таких як технологія блокчейн.

Крім того, залишаються невирішеними питання щодо: обрання централізованої чи децентралізованої моделі бухгалтерської книги обігу цифрової валюти; визначення суб'єктів, які матимуть доступ до ідентифікаційної інформації та даних про трансакції, зібраних і збережених у системі CBDC, і обмежених обставин, за яких до них можна отримати доступ; особливостей реагування системи CBDC на витоки даних або інші інциденти безпеки даних і відповідати вимогам звітування про витоки даних як усередині країни, так і в усьому світі.

Щодо питання доцільності залучення посередників, то слід відзначити наявність різних підходів у відповідному напрямі. Водночас, якщо розглянути проєкти CBDC у світі, то з 11 запущених на міжнародному рівні CBDC усі країни обрали посередницьку структуру. З 15 систем CBDC, які вступили в пілотну фазу, лише вісім чітко прийняли посередницьку модель, тоді як решта все ще розглядають її переваги та ризики на противагу моделі без посередників (яка дозволяє фізичним та юридичним особам відкривати рахунки безпосередньо в

установах центрального банку). Серед яскравих прикладів посередницької моделі слід назвати пілотні проєкти CBDC КНР, Норвегії, Швеції та інших країн.

Зокрема, пілотна система CBDC у КНР, яку називають проектом e-CNY, є яскравим прикладом посередницької структури. Право випускати китайські е-юані належить державі, а операційна система зосереджена навколо Народного банку Китаю (НБК). НБК випускає китайські е-юані «уповноваженим операторам», тобто уповноваженим комерційним банкам, і управляє е-юанями протягом усього їхнього життєвого циклу. Після випуску відповідні установи обмінюються та розповсюджують е-юані серед населення через традиційні відносини між споживачем та банківським рахунком (рис. 1.2).



Рис.1.2. Архітектура e-CNY пілотного проекту НРК з побудови національного CBDC

Джерело: Аналітичний звіт пілотного проекту НБУ щодо е-гривні [71].

У Швеції посередницька модель має такий вигляд. На першому рівні Riksbank випускає або викуповує е-крони в обраних посередників у мережі, таких як банки (Handelsbanken або Tietoevry). На другому рівні посередники розподілятимуть е-крони кінцевим користувачам, надаючи їм псевдоніми, що використовуються як мережеві адреси для платежів CBDC (рис. 1.3).

Учасники зможуть отримувати або викуповувати цифрову валюту шляхом списання або поповнення резервів, що зберігаються безпосередньо учасниками, або через представника в системі грошових переказів у режимі реального часу Riksbank, відомій у Швеції як RIX. У тестовій моделі вузол e-krona учасників у мережі інтегрований з їхніми внутрішніми обліковими та платіжними системами. Handelsbanken упровадив свій вузол e-krona у власному IT-середовищі, тоді як вузол e-krona Tietoevry перебуває в IT-середовищі Riksbank. Незважаючи на це, клієнти обох банків мали змогу здійснювати трансакції в спільній мережі е-крони.

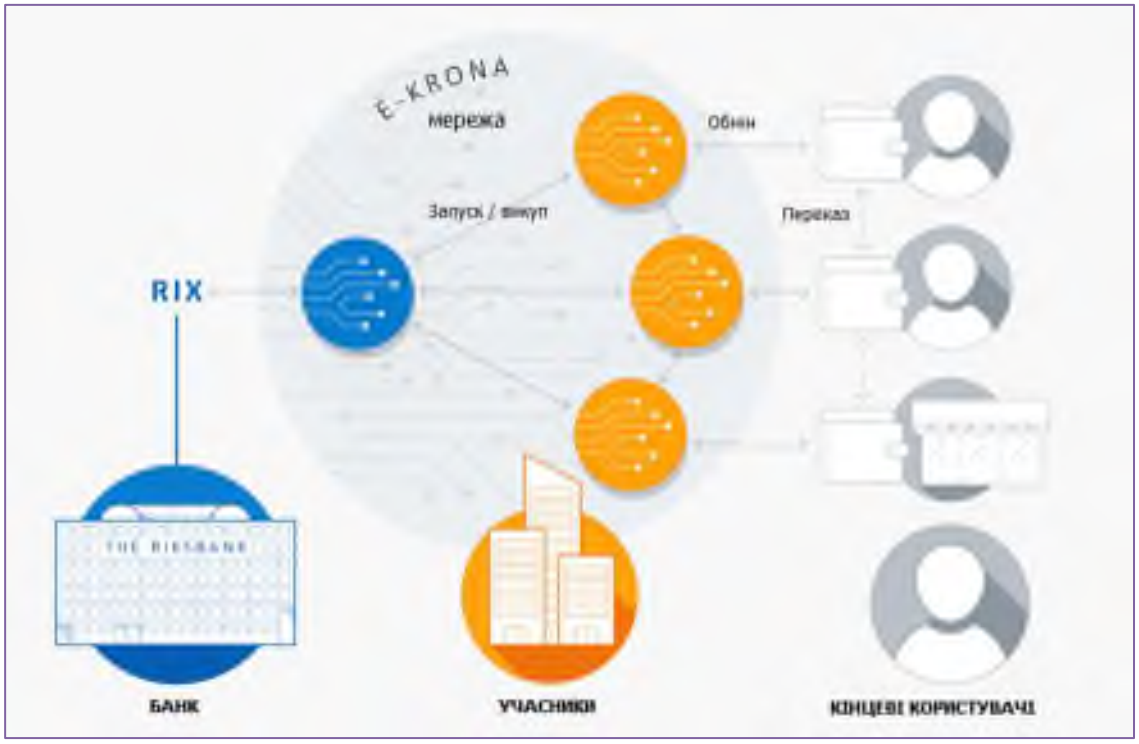


Рис.1.3. Архітектура e-krona пілотного проекту Riksbank з побудови національного CBDC

Джерело: Аналітичний звіт пілотного проекту НБУ щодо е-гривні [72]

Мережева модель Corda, яку обрав центральний банк Швеції та в якій інформація надається центральним банкам, органам фінансового регулювання і фінансовим посередникам лише за принципом службової необхідності, забезпечує рівень конфіденційності, подібний до дворівневої моделі, що використовується сьогодні центральними банками. Для запобігання подвійним

витратам у цій моделі фахівці відстежують вхідні й вихідні дані трансакцій і спроби подвійних витрат, зазначаючи ідентифікатори трансакцій.

У Норвегії CBDC також планується розповсюджувати за дворівневою архітектурою: Norges Bank випускатиме CBDC банкам, які потім зараховуватимуть їх на рахунки своїх клієнтів (кінцевих споживачів). Утім, на рівні регулятора існують суперечливі думки стосовно такої посередницької моделі. Зокрема, у звіті «Запровадження цифрової валюти центрального банку – необхідні законодавчі зміни» (Introduction of central bank digital currency – necessary legislative amendments) [73] Helge Syrstad висловлює сумніви щодо відповідного підходу з таких причин.

По-перше, окремі види платежів, наприклад, процентні, можуть вимагати прямих відносин між центральним банком і кінцевим користувачем. По-друге, технічний дизайн CBDC може викликати труднощі, пов'язані з роллю центрального банку як емітента. Зокрема, у цьому випадку виникає питання, чи можна вважати CBDC, перераховані посередникам «уповноваженим операторам» (переведені з однієї книги в іншу), «справжніми» грошима центрального банку, адже за таких обставин вони є «синтетичними». «Синтетичні» CBDC вважатимуться приватним платіжним засобом, за який центральний банк не несе жодної відповідальності. Однак поряд із висловленими зауваженнями автор пропонує шляхи вирішення порушених питань. А це свідчить все-таки про превалювання позиції відносно обрання посередницької моделі цифрової валюти [73].

Так чи інакше, модель із можливістю збереження за банками (або їх частиною) функції посередників між центральним банком та індивідуальними власниками валюти, котрі мають рахунки в CBDC, видається прийнятнішою. Адже вона гарантуватиме непорушність балансу між доступністю конфіденційної інформації та захистом приватних інтересів.

Слід зазначити, що проєкт КНР щодо CBDC є прикладом операційної моделі централізованого реєстру, який управляється Народним банком Китаю, з

використанням концепції «контрольована анонімність» для забезпечення конфіденційності трансакцій. Цей метод гарантує, що трансакції залишаються приватними для тих, хто не входить до системи, за винятком НБК, який може відстежувати рух електронних платежів у цифровій валюті, а також зв'язок між адресами та ідентифікацією користувача відомий центральному банку лише через процедуру політики «Знай свого клієнта». Однак регулятор вживає додаткових заходів стосовно захисту від незаконного державного нагляду шляхом використання брандмауерів для будь-якої інформації, пов'язаної з CBDC, призначення «спеціального персоналу для управління інформацією» і забороною всіх «довільних інформаційних запитів» [74].

На відміну від проєкту КНР щодо CBDC аналогічні проєкти Швеції та Норвегії є прикладами операційної моделі технології розподіленого реєстру з використанням, відповідно, платформ Corda та Ethereum. Зокрема, трансакції з е-кроною «реєструються не в центральній базі даних, а у вузлах учасників, які беруть безпосередню участь у трансакції» [75]. Це означає, що всі власники гаманців е-крони, котрі ініціюють трансакції, мають доступ до публічного цифрового реєстру е-крони і можуть вносити до нього зміни. Те, як шведська система е-крони працює на практиці, викликає занепокоєння стосовно конфіденційності даних про особу та трансакції, у тому числі з боку центрального банку Швеції (Riksbanken).

Зокрема, у звіті про другий етап пілотного проєкту е-крони регулятор визнав, що «не можна відкидати можливість того, що дані в мережі обробляються у спосіб, який не відповідає законодавству про фінансову таємницю та захист даних». Riksbank також попередив, що для того, аби пілотна система е-крони повністю відповідала законодавству про захист даних, можуть знадобитися консультації з органами захисту даних Швеції та Європейського Союзу стосовно того, як технологія блокчейн співвідноситься з Регламентом (ЄС) 2016/679 Європейського парламенту та Ради від 27.04.2016 про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних,

а також про скасування Директиви 95/46/ЄС (Загальний регламент захисту даних (GDPR)) [76].

Слід звернути увагу, що дослідницька служба Європейського парламенту звернулася до цих питань ще у 2019 р., виявивши три критичні суперечності між DLT та GDPR: (1) GDPR передбачає відповідальність «принаймні однієї фізичної або юридичної особи», до якої суб'єкти даних – резиденти ЄС можуть звертатися для забезпечення своїх прав, однак DLT замінює єдиного відповідального суб'єкта кількома суб'єктами, що «перешкоджає розподілу відповідальності та підзвітності»; (2) GDPR вимагає, щоб дані були «змінені або видалені, якщо це необхідно для дотримання статей 16 і 17, однак DLT за своєю конструкцією зазвичай не дає жодному учаснику права на зміну або видалення; (3) принципи мінімізації даних, покладені в основу GDPR, порушуються DLT, які зазвичай зберігають інформацію у відкритому доступі та в кількох вузлах системи» [76].

Централізована модель гарантує, що лише банки матимуть повноваження щодо деталей трансакцій та ідентифікаційних даних з метою дотримання вимог законодавства, забезпечуючи при цьому захист усіх персональних даних та даних про трансакції, які контролюються обраними фінансовими установами, що мають інфраструктуру для захисту приватності, та обмежуються ними. Централізована модель усуне будь-яку потенційну дисгармонію з GDPR, якщо система буде доступною для резидентів ЄС або сумісною із системами CBDC ЄС у майбутньому.

В майбутньому екосистема цифрових активів стане постійною складовою фінансового ландшафту, співіснуючи з сучасною банківською системою, що базується на посередницькій діяльності. Традиційні фіатні валюти лишатимуться основними, але важливу роль гарантування ліквідності забезпечать приватні стейблкоїни.

Можна передбачати, що CBDC матимуть ключове значення у транскордонних платежах і розрахунках. Роздрібні CBDC можуть стати

невеликим складником грошової бази, відіграючи роль, подібну тій, яку сьогодні відіграє готівка.

І транскордонні розрахунки, і готівка на традиційних фінансових ринках сприяють використання їх у злочинній діяльності, особливо у відмиванні нелегальних активів. Щодо CBDC, то вони підвищують прозорість операцій за рахунок блокчейн-технології, містять процедури ПВК/ФТ, такі як ідентифікація та верифікація клієнта, оцінка його ризиковості та діяльності.

З розвитком цифрових технологій, ці процедури виконуються в мережі Інтернет у віддаленому режимі. Прикладом є впроваджені процедури комплаєнсу в ліцензованій діяльності ППВА за допомогою програмних продуктів блокчейн-аналітики [77]. Завдяки такому програмному забезпеченню процедури оцінки ризику клієнта та його операцій теж автоматизовані [78, 53].

За принципами проведення блокчейн-аналітики ідентифікувати учасників операції з віртуальними активами можна завдяки фінансовим обмінним операціями банківських і платіжних установ, централізованих криптобірж та обмінників (ППВА). Через упровадження регулювання на державному та глобальному рівні блокчейн-аналітичні компанії є також носіями інформації про своїх клієнтів. Але ефективнішим інструментом антилегалізаційних процедур може стати обмін віртуальних активів на CBDC, через які інформація про учасників трансакції в блокчейні стає абсолютно прозорою, процедури ПВК/ФТ – автоматичними. Це ще одне обґрунтування запуску CBDC центральними банками для підвищення фінансової стабільності та гіпотези про те, що готівка не зникне, однак можуть значно знизитись її обсяги. Така колаборація віртуальних активів і CBDC прогнозовано стане інструментом і антикорупційної діяльності та запобіжником будь-яких злочинів із використанням віртуальних активів.

Водночас реалізації таких проєктів перешкоджають, крім відсутності політичної полі здійснювати їх на національному рівні, загрози для обох цифрових активів з боку кіберзлочинності. Дж. Ліпскі з Atlantic Council зазначив:

«Ризиками конфіденційності та кібербезпеки можна керувати за допомогою відповідально розроблених цифрових валют центрального банку» [79]. Існують різноманітні дизайни CBDC, починаючи з централізованих баз даних і закінчуючи розподіленими реєстрами та системами на основі токенів. Перш ніж робити висновки про ризики для кібербезпеки та конфіденційності, важливо докладно розглянути кожен із цих дизайнів. Також варто порівняти ці конструкції з поточною фінансовою системою, щоб визначити, чи можуть нові технології пропонувати безпечніші варіанти.

Багато запропонованих варіантів дизайну CBDC, зокрема роздрібних, передбачають централізований збір даних про трансакції, що створює серйозні ризики для конфіденційності та безпеки. Занепокоєння стосовно проєктів, які мають зберігати конфіденційність, полягає в тому, що це може призвести до зниження прозорості для регуляторів.

Регуляторним органам зазвичай потрібне достатнє розуміння, щоб виявляти підозрілі трансакції, для виявлення відмивання грошей, фінансування тероризму та іншої незаконної діяльності. Криптографічні методи можуть використовуватись для розроблення CBDC, які забезпечують рівень конфіденційності, подібний до готівки, до певного порога, даючи змогу державним органам здійснювати необхідний регуляторний нагляд.

Останнім часом деякі центральні банки прийшли до висновку, що CBDC може створювати значні ризики для кібербезпеки та конфіденційності. Проте вони також визнали, що існують різноманітні варіанти дизайну CBDC на вибір, включаючи нові варіанти, які ще не були повністю випробувані. Вибір конкретного варіанту дизайну CBDC повинен відбуватися на основі потреб країни та пріоритетів політики [79].

Загалом слід розуміти, що при правильному проєктуванні CBDC може бути так само безпечною, як і наявні фінансові системи. Потрібно збалансувати питання кібербезпеки з іншими аспектами, щоб забезпечити оптимальний результат.

Це дослідження підтверджує, що фрагментовані зусилля зі створення CBDC можуть створювати проблеми сумісності й транскордонні ризики кібербезпеки. Незалежно від того, чи вирішать країни запровадити CBDC, Федеральна резервна система США повинна сприяти розробленню глобальних стандартів для CBDC. Європейський Союз у процесі розроблення законодавства стосовно діяльності крипторинку (Регламент MiCA [80]) одночасно для впровадження єдиним пакетом прийняв Регламент DORA щодо операційної стійкості цифрових технологій у секторі фінансових послуг [81]. Його спрямовано на створення всеосяжної й уніфікованої основи для гармонізації процесів та стандартів, пов'язаних із операційною стійкістю цифрових технологій у фінансовому секторі. Крім того, ЄС оновив Директиву 2011/16/ЄС про адміністративне співробітництво у галузі оподаткування DAC8 [82], яка вводить правила податкової прозорості для криптоактивів. До єдиного пакета також додано оновлений Регламент про переказ коштів, що включив криптотрансакції TFR [83], аналогічний Правилу подорожей.

Ще у 2020 р. Європейська комісія ухвалила нову Стратегію цифрових фінансів для ЄС (Digital Finance Strategy for the EU) [84], яка має на меті трансформувати європейську економіку впродовж найближчих десятиліть. Оновлення цієї стратегії відбулося в липні 2022 р. Основна мета стратегії — підвищити конкурентоспроможність фінтех-сектору та технологій, водночас знижуючи ризики й забезпечуючи фінансову стабільність європейської економіки. Фінансові технології (фінтех, англ. Fintech) — це технології, які використовуються у фінансових послугах або допомагають компаніям керувати фінансами, впроваджуючи нові додатки, програми, процеси та бізнес-моделі. На сьогодні фінтех є основою для всіх онлайн-трансакцій, таких як грошові перекази, кредитування, оплата комунальних послуг тощо. До фінтеху належать як численні технологічні стартапи, так і великі організації, що прагнуть покращити й оптимізувати фінансові послуги.

Станом на 2023 р. криптовалюта продовжувала здобувати популярність у Європейському Союзі. Згідно з даними, опублікованими в серпні 2023 р., частка громадян, котрі інвестують у цифрові активи, у деяких країнах зросла. Зокрема, у Словаччині цей показник досяг 12 %, що свідчить про зростання інтересу до криптовалют порівняно з попередніми роками За даними дослідження CoinGecko, Нідерланди посідають друге місце в Європі за рівнем зацікавленості у криптовалютах, на них припадає 7,30 % криптоактивів на континенті [85]. Прогнози щодо загальної ринкової капіталізації криптоактивів залишаються оптимістичними. За оцінками експертів криптовалютної біржі Binance, до 2025 р. вона може перевищити 8 трлн дол. США [85].

Європейською комісією визначено напрями розроблення майбутніх основних стандартів ЄС, а саме:

- ЄС повинен пам’ятати про постійні дослідження та експериментальну роботу щодо цифрових валют ЄЦБ. Це має сприяти подальшим дослідженням з оцінки життєздатності CBDC;
- ЄС повинен узгодити свої дії стосовно глобальних проєктів стабільних валют з постійною роботою міжнародних органів, що встановлюють стандарти, таких як Рада фінансової стабільності (Financial Stability Board, FSB);
- ЄС повинен оцінити адекватний підхід щодо фінансових установ, які мають на балансі віртуальні активи та/або займаються криптоактивами;
- для наближення європейських рамок ПВК/ФТ з урахуванням поточних реалій у криптопросторі ЄС слід розглянути низку регуляторних дій, зокрема: розширення визначення ВА, розширення переліку зобов’язаних суб’єктів, а саме віднесення до ППВА геймерів, приділення достатньої уваги ролі майнерів, досліджуючи, чи ефективно децентралізовані торгові об'єкти впроваджують систему управління ризиками у сфері ПВК/ФТ;
- ЄС слід продовжувати інвестувати в ініціативи, які доповнюють набір інструментів розслідування правоохоронних органів, що намагаються

відстежувати злочини ВК/ФТ та інші протизаконні дії, такі як ухилення від сплати податків через ВА;

- ЄС потрібно оцінити розвиток CBDC, яка забезпечує баланс між законним попитом громадян на захист клієнтів і необхідністю дотримання стандартів ПВК/ФТ, спираючись на роботу дослідницької мережі EUROChain;
- ЄС повинен додатково вивчити питання запровадження європейського контролю за ВК/ФТ;
- щоб створити рівні умови та забезпечити належний захист інвесторів по всьому ЄС, доцільно запровадити правову кваліфікацію криптоактивів як фінансових інструментів. Більше того, законодавство ЄС про фінансові послуги слід привести у відповідність до унікальних характеристик криптосектору, щоб забезпечити ефективне застосування наявного фінансового регулювання до криптоактивів, які є фінансовими інструментами;
- ЄС необхідно запровадити в практику відповідні вимоги щодо розкриття ризику, аби інвестори та/або споживачі могли бути поінформовані про потенційні ризики до інвестування коштів у ВА, що не кваліфікуються як фінансові інструменти (MiFID II) [86] та як електронні гроші (EMD2) [87] (рис. 1.10);
- ЄС повинен розглянути можливість запровадження стандартів кібербезпеки, яких дотримуватимуться посередники, що пропонують сервісні послуги в межах ЄС;
- ЄС повинен стежити за технічною доцільністю чорного списку монет та включення до нього певних віртуальних активів з метою набагато ширшого застосування, ніж лише подолання атак-вимагачів, зокрема і щодо потенційних наслідків на крипторинку загалом.

ВА не прив’язані до національних кордонів, а також ВК/ФТ та інших незаконних видів діяльності, для яких вони іноді використовуються. Для отримання належних результатів наглядових та правоохоронних органів у боротьбі зі злочинною діяльністю, в якій використовуються криптоактиви, їм

потрібно співпрацювати й обмінюватися інформацією, що відбувається несистемно. Як зазначає Європейська комісія у своїй останній наднаціональній оцінці ризиків щодо європейської системи ПВК/ФТ [88], транскордонне співробітництво та координація між національними органами влади у сфері ПВК/ФТ все ще залишається недостатнім. Для вирішення цієї проблеми 5 грудня 2019 р. Рада ЄС (ECOFIN) офіційно запропонувала Комісії «вивчити можливості, переваги та недоліки нагляду за відмиванням коштів і надати повноваження і відповідальність новоствореному органу Європейського Союзу з незалежною структурою та прямими повноваженнями щодо певних зобов'язаних суб'єктів […]» [89].

Запровадження європейського органу ПВК/ФТ може мати різні переваги, особливо якщо в ньому працюватиме висококваліфікований ІТ-персонал, здатний аналізувати ризики ВК/ФТ, які створюють нові технології. Це може сприяти обміну інформацією, стати новим пулом знань та забезпечити більш незалежний підхід до випадків ВК/ФТ порівняно з національними ПФР.

Щодо впровадження CBDC заміна анонімних, невідстежуваних готівкових коштів на державні відстежувані або їх приватні еквіваленти може теоретично сприяти попередженню багатьох випадків ВК та інших злочинних дій. Якщо вся платіжна інформація буде миттєво доступною або легкодоступною для правоохоронних органів, нелегальні суб'єкти фактично будуть змушені припинити свої операції. Однак навряд чи громадяни найближчим часом повністю відмовляться від готівкових платежів, не говорячи вже про згоду на повний урядовий контроль за кожною їхньою транзакцією. З політичної точки зору створення повністю безготівкового суспільства, яке є «ідеальним сценарієм» для наглядових органів, наразі видається, швидше, утопічною ідеєю.

Для адекватного вирішення проблем, визначених чинною фінансовою нормативно-правовою базою щодо криптоактивів, слід розрізняти віртуальні активи, які є фінансовими інструментами, віртуальні активи, шо не є фінансовими інструментами, та електронні гроші (рис.1.4).



Рисунок 1.4. Сфера застосування законодавства ЄС про фінансові послуги щодо криптоактивів

Джерело: за матеріалами [89].

Стосовно криптоактивів, які є фінансовими інструментами згідно з MiFID II, можна розглянути два напрями дій.

Перша дія стосується кваліфікації криптоактивів як фінансових інструментів. Як згадувалося, нині немає єдиної точки зору щодо того, коли криптоактив кваліфікується як фінансовий інструмент MiFID II. Це пов'язано здебільшого з тим, що під час упровадження MiFID II до власного національного законодавства держави – члени ЄС визначали термін «фінансовий інструмент» по-різному: деякі застосовували обмежувальний перелік прикладів для визначення терміна «цінні папери, що підлягають переказу», інші використовували ширше тлумачення [86]. Щоб створити рівні умови та забезпечити адекватний захист інвесторів по всьому ЄС, необхідна спільна точка зору на правову кваліфікацію криптоактивів як фінансових інструментів. Це може мати форму запиту до європейського регулятора ринку цінних паперів (ESMA) надати подальші вказівки з тлумачення переліку фінансових інструментів у MiFID II щодо криптоактивів. Законодавець ЄС має право застосувати єдине визначення поняття як до «переказних цінних паперів» [90] та/або внести зміни до переліку фінансових інструментів у MiFID II, щоб пояснити їх застосування до криптоактивів.

Спираючись на роботу ESMA та інших органів, що встановлюють стандарти, таких як IOSCO [91], другою дією, яку може розглянути законодавець ЄС, є приведення законів ЄС у сфері фінансових послуг у відповідність до унікальних характеристик криптосектору. Як слушно зазначив ESMA, існують сфери, що вимагають перегляду конкретних вимог або навіть внесення

додаткових положень, аби забезпечити ефективне застосування чинних нормативних актів до криптоактивів, які є фінансовими інструментами [91]. Можуть знадобитися подальші дослідження, щоб точно визначити, які положення потребують оновлення.

Щодо криптоактивів, котрі не кваліфікуються як фінансові інструменти у MiFID II, а також електронні гроші EMD2, ЄС має впроваджувати нові правила, пристосовані до конкретних ризиків та викликів, які криптоактиви спричиняють. Якщо нічого не робити, інвестори не будуть зацікавлені цією сферою діяльності, тому ми погоджуємося з ESMA, що другий сценарій, коли впроваджуються нові правила, є найбільш доцільним напрямом дій [91].

Дослідження IOSCO чітко показало, що «багато питань та ризиків, пов’язаних з торгівлею криптоактивами, які тут слід розуміти в їхньому найширшому значенні і які, таким чином, охоплюють більше, ніж активи інвестиційного типу, або те, що це дослідження назвало інвестиційними токенами, подібні до емісій та ризиків, пов’язаних із торгівлею традиційними цінними паперами чи іншими фінансовими інструментами на місцях торгів» [92]. Доречно, щоб це було зрозуміло, тому в ЄС необхідно запровадити відповідні вимоги стосовно розкриття ризику щодо крипто активів, які не кваліфікуються як фінансові інструменти чи електронні гроші (у тому числі стосовно емітента, проєкту, прав, що додаються до криптоактиву, використовуваної технології та потенційного конфлікту інтересів), для того щоб інвестори та/або споживачі могли би бути обізнаними про потенційні ризики переказу коштів за такі криптоактиви [93].

Питання полягає в тому, чи достатньо цього для вирішення питання регуляторного арбітражу між державами – членами ЄС та забезпечення належних стандартів захисту споживачів/інвесторів. Чи ЄС слід зробити більше і прийняти ширший режим для нефінансових інструментів / криптоактивів, що не належать до електронних грошей, та пов'язаної з ними діяльності, і, наприклад, запровадити вимоги до ліцензування для брокерів, менеджерів з

активів та інших посередників? Розглядаючи це, як слушно зазначив ESMA, ЄС повинен пам’ятати про компроміси, які можуть мати ширше регулювання криптоактивів, наприклад, ризикувати їх легітимізацією та заохочувати до більшого прийняття [93]. Тому ESMA радить на цьому етапі зосередити режим нагляду щодо криптоактивів, які не є фінансовими інструментами та електронними грошима, на попередженні покупців про ризики щодо цих криптоактивів, а не на жорсткішому режимі.

Багато нефінансових інструментів/криптоактивів, що не належать до електронних грошей, створюють ризики та проблеми, подібні до традиційних фінансових інструментів або електронних грошей. Однак, на нашу думку, ЄС повинен зазначити, що залежно від їх конструкції та того, чи можна ними торгувати на вторинних ринках, також може бути доцільно розуміти, що вони практично не мають жодного стосунку до фінансових ринків. Наприклад, коли утиліті-токен не може торгуватись (такий токен зазвичай називають «чистим» [90]), його можна викупити лише за певні товари чи послуги, подібні до неторгового ваучера. Подібний інструмент, імовірно, вимагає іншого нагляду.

Загалом ми погоджуємося з ESMA, що якщо законодавець ЄС повинен розглянути можливість прийняття подальшого регулювання, запропонований режим нагляду має бути достатньо гнучким, аби охопити широкий спектр характеристик та факторів ризику нефінансових інструментів / крипто валют, які не пов'язані з електронними грошима та забезпеченими віртуальними активами [93]. Більше того, законодавство повинне бути якомога нейтральнішим для технологій, щоб зробити їх максимально надійними в майбутньому [91].

Субсидіаційність – це прийняття на міжнародному рівні уникнення регуляторного арбітражу, особливо даної прикордонної природи. Віртуальні активи – глобальне явище: вони створюються приватними суб'єктами в різних країнах світу, є транскордонними за своїми програмами та інфраструктурою, доступними, передаються, обмінюються й торгуються майже з будь-якої точки світу. Як результат, вони створюють регуляторні виклики не лише в межах ЄС.

Для вирішення цих проблем наглядовим органам доведеться втрутитися. В окремих країнах законодавці вже вжили заходів (приклади у сфері захисту інвесторів включають Швейцарію, Мальту та Францію) або планують це зробити. Такі національні ініціативи не обов'язково узгоджуються між собою, що призводить до регуляторного арбітражу. Аби уникнути останнього, норми щодо криптоактивів мають розроблятися на європейському рівні, бажано на основі впровадження міжнародних стандартів.

Щоб додатково проілюструвати, чому встановлення міжнародних стандартів є ключовим, ми далі беремо правила ПВК/ФТ за взірець.

Так само, як криптовалюта, відмивання коштів та фінансування тероризму є глобальними явищами, що не зупиняються на кордонах ЄС. Злочинці та терористи під час їхньої діяльності зазвичай шукають лазівки та прогалини в нормативно-правовій базі з протидії злочинності та її фінансуванню. Отже, якщо в країні чи регіоні діють правила ПВК/ФТ, які є для них більш сприятливими, у тому розумінні, що вони залишають більше свободи для своєї незаконної діяльності, то вони, швидше за все, започаткують злочинний бізнес саме в цих країнах або регіонах і використовуватимуть їх як шлюз для відмивання своїх доходів. Це, безсумнівно, справедливо і щодо діяльності з криптоактивами [94]. Якщо, наприклад, США дотримуватимуться суворіших правил ПВК/ФТ щодо криптоактивів, ніж ЄС (або навіть окремі країни-члени), діяльність ВК/ФТ через віртуальні активи, ймовірно, буде перенесена на територію ЄС. Однак якщо однакові стандарти ПВК/ФТ додержуватимуться в обох регіонах, то шанси на ефективне викорінення такої діяльності будуть набагато більші. Таким чином, є сенс установлювати стандарти ПВК/ФТ на міжнародному рівні. MONEYVAL як міжурядовий орган, що формує політику FATF, робить це.

ЄС та його держави-члени повинні продовжувати сприяти роботі MONEYVAL і FATF, а міжнародні стандарти, встановлені FATF, мають своєчасно та всебічно впроваджуватись у законодавство ЄС для забезпечення

повної відповідності фінансової системи на внутрішньому ринку та на міжнародному рівні.

До 2021 р. у цьому плані ЄС, на наш погляд, міг би бути досконалішим. Як проілюстровано вище, найновіші правила ЄС щодо ПВК/ФТ для віртуальних валют, викладені в документі AMLD5 [24], застаріли задовго до того, як держави-члени мали перенести їх до національного законодавства стосовно ПВК/ФТ, тобто до 10 січня 2020 р., і явно відставали від відповідних міжнародних стандартів. Аби уникнути нерівних конкурентних умов та правової невизначеності у транскордонному контексті, були необхідні регуляторні дії на вищому рівні.

Тому Європейська комісія 24 вересня 2020 р. ухвалила новий розширений пакет цифрових фінансів, який має на меті змінити європейську економіку в найближчі десятиліття, а саме підвищити конкурентоспроможність фінтех-сектору та технологій континенту, одночасно пом’якшуючи ризики та забезпечуючи фінансову стабільність європейської економіки [83].

Важливо, що нова стратегія ЄС включила новий всеосяжний Регламент щодо криптоактивів під назвою «Ринки криптоактивів» (MiCA), розроблений з метою оптимізації технології DLT та регулювання віртуальних активів у ЄС із метою захисту користувачів та інвесторів [84]. Цей Регламент, а також внесення змін до Директиви Європейського парламенту та Ради ЄС від 23.10.2019 «Про захист осіб, які повідомляють про порушення законодавства Союзу» [95] розроблялися з 2018 р. Його метою є сприяння державним регуляторам у контролі за обігом криптоактивів та діяльності ППВА у ЄС, а також запровадження уніфікованого режиму ліцензування для всіх держав-членів. Крім того, MiCA має на меті «гармонізувати європейські рамки для випуску та торгівлі різними типами криптотокенів у рамках європейської стратегії цифрових фінансів» [96].

Документ MiCA зосереджується на правилах, що регулюють наразі такі типи крипто активів, як стейблкоїни, а також постачальників послуг, пов’язаних

з оборотом крипто активів, які називаються Crypto assets service provider (CASP) (термін також використовується в нормативно-правових базах інших країн, наприклад, Японії та Південній Африці). Ми будемо дотримуватись загалом термінології, визначеної в Рекомендації 15 FATF [223], тобто Virtual assets service provider (ППВА), а розглядаючи Директиву ЄС про регулювання криптоактивів термінології, використаної в тексті Директиви, а саме CASP [78].

Європейська комісія стверджує, що вона намагалася бути справедливою, «де це можливо», і що «вимоги, які висуваються до постачальників послуг криптоактивів, пропорційні ризикам, створеним наданими послугами» [78]. Європейська комісія створила MiCA, аби забезпечити споживачам ЄС доступ до інноваційних, але безпечних криптоактивів без шкоди для стабільності ринку. Можна стверджувати, що захист користувачів криптоактивів є його головним завданням, яке має бути збалансоване з потребою в новітніх інвестиційних продуктах, а також із регуляторними та фінансовими ризиками, пов’язаними з ширшим використанням потенційно небезпечних активів, таких як стейблкоїни. Наприклад, емітенти стабільних монет і криптооператори, чиї ринкові обсяги перевищують «значні» пороги, підпадатимуть під суворіші вимоги належної перевірки.

MiCA є результатом процесу, який розпочався після швидкого зростання біткоїна у 2017 р. Це піднесення суспільного інтересу та інвестицій у криптовалюти змусило європейських регуляторів звернути увагу на небезпеку, яку нерегульовані віртуальні активи становлять для інвесторів і ринків, що включає ризики ВК/ФТ. ВК/ФТ. Регламент MiCA вводить 28 визначень, пов’язаних із криптоактивами (табл. 1.3).

Таблиця 1.3

Термінологія Регламенту MiCA

«криптоактиви»	цифрове представлення вартості або прав, які можуть передаватися та зберігатися в електронному вигляді, використовуючи технологію розподіленої книги або подібну технологію.
«технологія розподіленого реєстру» («DLT»)	тип технології, що підтримує розподілений запис зашифрованих даних
«службовий токен»	тип крипто активу, який призначений для надання цифрового доступу до товару або послуги, доступний на DLT, і приймається лише емітентом цього токена.
«забезпечений активами токен»	тип крипто активу, який прагне підтримувати стабільну вартість, посилаючись на вартість кількох фіатних валют, які є законним платіжним засобом, одного чи кількох товарів, одного чи кількох криптоактивів, або комбінації таких активів.
«токен електронних грошей» («е-валютний токен»)	тип крипто-валютного активу, головна мета якого полягає в тому, щоб використовуватися як засіб обміну і який має на меті підтримувати стабільну вартість, посилаючись на вартість фіатної валюти, яка є законним платіжним засобом.
«постачальник послуг, пов'язаних з оборотом криптоактивів»	будь-яка особа, чиєю роботою або бізнесом є надання однієї або кількох послуг, пов'язаних з оборотом криптоактивів третім сторонам на професійній основі

Джерела: складено автором на основі [78]

Послуги, пов'язані з оборотом криптоактивів, означають будь-які послуги та дії, перераховані далі, що стосуються будь-якого криптоактиву:

- зберігання та управління криптоактивами від імені третіх сторін;
- функціонування торгової платформи для криптоактивів;
- обмін криптоактивів на фіатну валюту, яка є законним платіжним засобом;
- обмін криптоактивів на інші криптоактиви;
- виконання замовлень на криптоактиви від імені третіх сторін;
- розміщення криптоактивів;

- отримання та передача замовлень на криптоактиви від імені третіх сторін;
- надання консультацій щодо криптоактивів.

Як згадувалося раніше, CASP визначається в Регламенті MiCA як «будь-яка особа, чиєю професією або бізнесом є надання однієї або кількох послуг криптоактивів третім сторонам на професійній основі» [78]. Це визначення є ширшим, ніж визначення FATF постачальника послуг віртуальних активів (ППВА).

Регламент має на меті регулювати кожне цифрове представлення цінностей або прав, що можуть передаватися або зберігатися в електронному вигляді, використовуючи технологію DLT або схожу.

Так само, як традиційні фінансові компанії зобов'язані публікувати проспекти для пропозиції цінних паперів громадськості, емітенти всіх криптоактивів, згідно з MiCA, повинні попередньо оприлюднити проспект емісії (інформаційний документ щодо умов випуску) англійською або офіційною мовою країни ЄС. Цей документ має містити ключову інформацію про характеристики, права та обов'язки, а також основну технологію і проєкт. Проспект емісії необхідно подати до компетентних органів щонайменше за 20 днів до його публікації, але його затвердження не вимагається. Після розміщення на офіційному вебсайті емітента документ стає доступним для первинного розміщення на території всієї Європейської економічної зони (ЄЕЗ).

Проспект емісії не вимагається у таких випадках:

- вона адресована виключно кваліфікованим інвесторам або менше ніж 150 інвесторам у кожній країні-члені;
- загальна сума пропозиції не перевищує 1 млн євро (1,17 млн дол. США) протягом 12 місяців;
- криптоактиви пропонуються безкоштовно, тобто через «аеродропи» (за умови, що одержувачі не зобов'язані надавати персональні дані, а емітент не отримує комісій чи вигоди від третіх сторін);

- активи пропонуються як винагорода за майнінг;
- випускаються крипто активи, які раніше були доступні в ЄС (за винятком стейблкоїнів).

Держави-члени повинні гарантувати, що емітенти криптоактивів несуть відповідальність за інформацію, викладену в офіційному документі, відповідно до норм національного законодавства. Крім того, споживачі мають право протягом 14 днів відмовитися від придбання токена або криптоактиву, якщо його не внесено до списку, за умови, що покупка здійснена безпосередньо.

З огляду на складність технології розподіленого реєстру (DLT) і пов'язані з нею ризики, емітенти зобов'язані забезпечити надійну кібербезпеку для захисту коштів інвесторів. У разі недотримання цих вимог національні регулятори мають право призупинити їхню діяльність [78].

Особливу увагу в Регламенті MiCA приділено так званим стейблкоїнам. Попри те, що Європейська комісія вважає нині ринок криптоактивів відносно невеликим («скромним»), існують побоювання щодо впливу «глобальних стейблкоїнів» (таких як Libra та її наступники), що потенційно можуть загрожувати фінансовій стабільності європейських ринків. Хоча MiCA не пропонує чіткого визначення стейблкоїнів, регламент охоплює два типи токенів, які зазвичай класифікують як стейблкоїни і використовуються для обміну чи оплати. Згідно з розділом 1 Проєкту, це токени забезпечені валютними цінностями або іншими активами і токени електронних грошей [78].

Токени, забезпечені валютними цінностями чи активами, мають підкріплення у вигляді кількох фіатних валют, одного чи кількох товарів, одного чи кількох криптоактивів або комбінації таких активів (так звані резервні активи). Токени електронних грошей прив'язані виключно до однієї фіатної валюти.

Регламент пропонує спеціалізовану структуру для регулювання «значущих» емітентів стейблкоїнів, зобов'язуючи дотримуватися посилених вимог до капіталу, захисту інтересів інвесторів і нагляду з боку Європейського

банківського регулятора (EBA). Ці вимоги охоплюють аспекти управління, уникнення конфлікту інтересів, резервні активи, їхнє зберігання, інвестиційну діяльність і підготовку супровідної документації.

Компанії, які бажають надавати послуги, пов'язані з обігом криптоактивів, зобов'язані отримати попередній дозвіл від компетентних органів країн – членів ЄС. Цей дозвіл буде дійсним на всій території Європейського Союзу. Водночас кредитні установи та компанії, що вже мають авторизацію на надання фінансових послуг відповідно до MiFiD, звільняються від цієї вимоги. Якщо в окремій країні ЄС вже існує національний режим ліцензування для ППВА, регулятори запроваджують спрощену процедуру переходу, щоб компанії могли перейти від національної ліцензії до ліцензії європейського ППВА, що діє в усіх країнах ЄС.

Подібно до правил MiFiD європейські ППВА підлягатимуть додатковим вимогам, залежно від їхнього розміру та рівня ризику. Ці вимоги включатимуть положення щодо капіталу, систем управління, підготовки персоналу, страхового покриття тощо (табл. 1.4).

Таблиця 1.4

Регуляторні вимоги до постачальників послуг, пов'язаних з оборотом криптоактивів

Тип CASP	Статутний капітал CASP	Інші вимоги
Зберігання та адміністрування криптоактивів	€ 125,000	Зберігачі криптоактивів повинні зберігати криптоактиви своїх клієнтів за адресами DLT, які є відокремленими від його власних адрес. Зберігачі криптоактивів повинні подавати щоквартальні звіти про позиції криптоактивів, які вони утримують для кожного клієнта. Клієнти можуть притягувати свого зберігача криптоактивів до відповідальності за збитки, які є результатом злому або збоїв у роботі.

Продовження таблиці 1.4

Комерційні операції через крипто-торговельні платформи [Багатопрофільні торгові площадки/ Організовані торгові площадки (БТП/ОТП)]	€ 150,000	Повинні встановити правила зарахування та призупинення операцій з криптоактивами, надісланих або отриманих платформою. Роздрібні клієнти можуть отримати доступ до торгівлі БТП. Маркери конфіденційності, які перешкоджають ідентифікації користувача та історії трансакцій, заборонені. Оператори не можуть торгувати на своїй платформі зі своїми власними рахунками. Платформа повинна постійно публікувати ціни пропозицій та запитів, а також обсяги трансакцій. Розрахунки по трансакціям на DLT мають бути здійснені в день їх проведення.
Обмін на фіатну валюту або інші криптоактиви (торгівля за власний рахунок)	€ 150,000	Оператори ППВА повинні публікувати свою політику щодо типів клієнтів, прийнятої цінової політики, або дані про механізм ціноутворення (ціна та обсяги) щодо трансакцій, здійснених на біржовій платформі
Виконання ордерів на операції з криптоактивами	€ 50,000	ППВА зобов'язані використовувати політику та процедури, які забезпечать найкращий можливий результат для виконаних замовлень клієнтів.
Розміщення криптоактивів	€ 50,000	ППВА повинні чітко пояснювати трансакційні та комісійні витрати, інформувати клієнта щодо запропонованих строків угоди, процедури та ціни розміщення криптоактивів.
Прийом і передача ордерів на операції з криптоактивами	€ 50,000	Під час передачі замовлень клієнтів ППВА не мають права приймати будь-які види платежів або надавати переваги в ході маршрутизації замовлень клієнтів на рахунок певної платформи для торгівлі криптоактивами.
Консультування з питань операцій з криптоактивами	€ 50,000	Консультанти з питань інвестування в крипто інструменти повинні збирати відповідну інформацію від клієнтів і оцінювати їхні знання та досвід щодо інвестування в криптоактиви. Надавані поради мають бути зважені відносно до цієї оцінки та повинні включати чітке пояснення та попередження щодо інвестиційних ризиків.

Джерело: Складено за матеріалами [97]

Усі криптоактиви, допущені до торгівлі на біржовій платформі, підлягатимуть регуляторним заходам, спрямованим на запобігання поширеним

зловживанням, які традиційно асоціюються з діяльністю криптобірж. Ці заходи передбачають пряму заборону на шахрайську поведінку.

У разі порушення цих правил компетентні органи можуть застосовувати фінансові санкції: до 5 000 000 євро або 3% річного обороту для юридичних осіб і до 700 000 євро для фізичних осіб. Ці штрафи діють окремо від санкцій, передбачених національним законодавством, яке також залишається чинним [97].

Захист інвесторів залишається центральним пунктом Регламенту, і тому необхідно виконувати подальші зобов'язання з належного розподілу активів, збереження коштів, структури бізнесу та кваліфікації керівництва. Послуги, пов’язані з оборотом криптоактивів в межах ЄС можуть надавати лише юридичні особи, які мають зареєстрований офіс у державі-члені ЄС і отримали дозвіл як GGDF згідно зі статтею 55 Регламенту [96].

Європейські ППВА, що пропонують транскордонні послуги, не зобов’язані мати фізичну присутність у всіх державах-членах ЄС, де вони хочуть надавати послуги, крім своєї країни походження.

Регламент MiCA не стосується безпосередньо питань ризиків ВК/ФТ, однак цей Регламент був розроблений для подальшої гармонізації законодавства ЄС із 40 Рекомендаціями FATF шляхом узгодження повною мірою термінології і класифікації послуг [92].

Будь-яке законодавство, прийняте у сфері криптоактивів, має бути конкретним, розрахованим на майбутнє та мати можливість йти в ногу з інноваціями та технологічними розробками. Тому «криптоактиви» та «технологія розподіленої книги» мають бути визначені якомога ширше, щоб охопити всі типи криптоактивів, які наразі не підпадають під дію законодавства ЄС про фінансові послуги.

Таке законодавство має також сприяти досягненню цілей боротьби з відмиванням грошей та фінансуванням тероризму. Тому будь-яке визначення «криптоактивів» має відповідати визначенню «віртуальних активів»,

викладеному в рекомендаціях Робочої групи з фінансових заходів FATF. З тієї ж причини будь-який перелік послуг, пов’язаних з оборотом крипто-валютних активів, також повинен охоплювати перелік послуг, пов’язаних з оборотом віртуальних активів, які, ймовірно, викликають занепокоєння щодо відмивання грошей і визначені так само в FATF.

Значне зростання криптовалютних ринків з 2020 року багато в чому можна пов’язати з стрімким зростанням популярності децентралізованих фінансів (DeFi). Однак для багатьох учасників крипторинку цей новий сектор виявився джерелом значних викликів, зокрема, через високу цінову волатильність, явне маніпулювання ринком і випадки відмивання грошей, які призвели до втрат для роздрібних інвесторів.

Не дивно, що DeFi дедалі частіше привертає увагу регуляторів. Європейський Союз не є винятком, і вже з’явилися припущення, що регламент MiCA може становити серйозну загрозу для існування індустрії DeFi [97].

Цілком ймовірно, що до моменту набуття чинності MiCA ландшафт DeFi суттєво зміниться, подібно до того, як ринок ICO зазнав значних трансформацій після початкового буму. Вимога щодо легальної присутності не створить сіру зону для існування цієї індустрії, і будуть цілком зрозумілі вимоги до проектів DeFi з можливістю роботи в ЄС чи пошуку клієнтів з ЄС.

Незважаючи на цей тривалий шлях легалізації крипторинку Регламент MiCA, безсумнівно, назавжди змінить ландшафт цифрових активів у Європі, а його суворі вимоги щодо відповідності вимогам можуть становити зростаючу загрозу для секторальних крипто ринків, таких як децентралізовані фінанси (DeFi).

Проекти DeFi до того часу потраплять до однієї з двох категорій: регульовані та нерегульовані. Якщо середовище ЄС є більш каральним, ніж інші юрисдикції, це, ймовірно, призведе до регуляторного арбітражу. Залишається незрозумілим, чи буде решта світу приєднатися до цієї системи [93].

Звичайно запропоновані правила Проєкту MiCA будуть застосовні і до будь-якого неєвропейського CASP, який прагне вийти на ринок клієнтам ЄС. Серед вимог буде потреба в юридичній особі в країні ЄС та ліцензії, але є й інші потенційні вимоги, такі як додаткове ліцензування для тих, що займається консультативною діяльністю, залежно від виду діяльності. Це не рамка, яка впливає лише на ЄС, вона матиме глобальні наслідки.

У 2019 році FATF запровадила нові жорсткі правила, зокрема Правило подорожей ППВА, які впроваджуються європейською мережею з кількістю понад 200 членів.

Визначення CASP від MiCA має певну схожість з визначенням VASP FATF, але є ширшим за обсягом, щоб забезпечити охоплення більшої кількості організацій (табл. 1.5).

Таблиця 1.5

Порівняльна характеристика європейських і міжнародних визначень операторів крипторинку

CASP	VASP
(a)зберігання та управління криптоактивами від імені третіх сторін; (b) функціонування торгової платформи для криптоактивів; (c) обмін криптоактивів на фіатну валюту, яка є законним платіжним засобом; (d) обмін криптоактивів на інші криптоактиви; (e) виконання замовлень на криптоактиви від імені третіх сторін; (f) первинне розміщення криптоактивів; (g) отримання та передача замовлень на операції з криптоактивами від імені третіх сторін (h) надання консультацій щодо операцій з криптоактивами	I. обмін між ВА та фіатними валютами; II. обмін між однією або кількома формами ВА; III. передача ВА; IV. збереження та/або адміністрування ВА або інструментів, що дозволяють контролювати ВА; V. участь та надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажем ВА.

Джерело: складено автором

Європейські постачальники послуг криптоактивів та інвестори тривалий час страждали від фрагментарних і заплутаних правил, які значно відрізнялися у країнах – членах ЄС. Хоча MiCA, безсумнівно, ускладнить ведення бізнесу

CASP, він повинен покласти край цим фрагментованим національним законодавчим режимам і забезпечити чітку регуляторну структуру для CASP, згідно з якою вони ь працюватимуть.

Важливо, що MiCA спростить процес ліцензування для постачальників послуг, поширивши ліцензування країн – членів ЄС на всі країни-члени, тим самим заощадивши CASP значний час, витрати та робочу силу.

В основу MiCA покладено захист інвесторів криптовалютних активів, які вже давно не є жертвами нестримних ринкових зловживань, шахрайства та зламу, і це має сприяти залученню нових інвесторів.

MiCA забезпечує чітку структуру для розроблення політики щодо криптоактивів, яка допоможе гармонізувати ринок ЄС і зупинити фрагментацію регулювання. Статус MiCA як пропонованого регламенту ЄС замість директиви (наприклад, 5-ї Директиви про боротьбу з відмиванням грошей, відомої як AMLD5), що робить транспозицію дискреційною, а не негайно виконаною, дає змогу регуляторним органам держав ЄС зрозуміти, що втекти від вимог після його офіційного оприлюднення не вдасться [181].

Отже, цілком імовірно, що офіційне застосування MiCA означитиме закінчення національної криптополітики всіх держав – членів ЄС на користь єдиної, цілеспрямованої нормативної бази, яка повинна дозволити постачальникам послуг, пов’язаних з оборотом крипто активів у ЄС, працювати з більшою легкістю в усіх країнах. на всіх ринках, хоча й за суворішими правилами.

1.3. Сутність і таксономія цифрових активів

Віртуальні активи – глобальне явище: вони створюються приватними суб'єктами в різних країнах світу, є транскордонними за програмами та інфраструктурою і легкодоступними, передаються, обмінюються та торгуються майже з будь-якої точки світу.

Першою криптовалютою на ринку став Bitcoin, але з часом з'явилися інші криптовалюти, які прагнули вдосконалити його функціонування. Ці альтернативні монети отримали назву альткоїнів. До них належать Namecoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Dogecoin. Вони використовують одну спільну технологію розподіленого реєстру (DLT), на основі якої здійснюється їхній майнінг. Ці криптовалюти не забезпечені реальними активами та залишаються високоволатильними.

Два ключові напрями подальшого розвитку ринку віртуальних активів включали стрімке зростання кількості приватних токенів, які випускалися на платформах через первинне розміщення монет (ICO), та появу стейблкоїнів і цифрових валют центральних банків (CBDC). Ці нові тенденції змусили регуляторні органи, організації зі стандартизації та науковців перейти від терміна «криптовалюти» до ширшого поняття «криптоактиви» [98].

У деяких країнах світу при спробах легалізувати майнінг криптовалют у законодавстві було використано термін «цифрові валюти», який за своєю суттю відповідає криптовалютам, а в подальшому був змінений на «цифрові активи».

Термінологія та таксономія цифрових активів широка і постійно розвивається в контексті розвитку криптовалют, блокчейну та суміжних інформаційно-телекомунікаційних технологій.

Слід наголосити, що ІТ-діяльність настільки швидко змінюється, що наукова думка не встигає створювати теоретичний базис та досліджує явища, які вже сформовані й функціонують у практичній сфері. У свою чергу, такий стрімкий розвиток нової цифрової економіки, трансформація бізнес-процесів, створення нових фінансових продуктів, квазіфінансових інструментів тощо призвели до неоднозначного трактування понять «цифрові активи», «віртуальні

активи», «цифрові валюти», «криптовалюти» тощо. З огляду на предмет нашого дослідження увагу буде зосереджено на дослідженні сутності поняття «цифрові активи».

Нині немає єдиного підходу до визначення поняття «цифрові активи». Неузгодженість стосується не лише формулювання цього терміна, а й загального концептуального підходу до його змісту. Формулювання визначення «цифрові активи» може варіюватися залежно від мети нормативного регулювання, рівня розвитку країни та спеціалізації законодавчого акта, в якому це поняття використовується. У більшості країн таке визначення взагалі не закріплене на законодавчому рівні.

Розуміння визначення «цифрових активів» можна умовно поділити на два: широке і вузьке. Широкий підхід закріплений у Переглянутому уніфікованому Законі про довірений доступ до цифрових активів (Revised Uniform Fiduciary Access to Digital Assets Act), розробленому Комісією з уніфікації права США. Хоча цей документ не є обов'язковим, його прийняли 34 штати, включно з Міссурі, Меном та Джорджією, використовуючи однакове визначення цифрових активів.

Згідно з цим законом, **цифровий актив** — це електронний запис, на який особа має певні права чи інтереси, і підкреслюється, що актив повинен мати саме електронну форму. Ключовою характеристикою є його електронна об'єктивізація [99].

Визначення цифрових активів у цьому контексті охоплює й активи криптографічного походження. Положення модельного акта поступово інтегруються в законодавство окремих штатів. Наприклад, ідентичне визначення цифрових активів закріплено в Законі штату Нью-Йорк № A9910A від 26.04.2016 [100]. Однак не всі штати дотримуються єдиного підходу. У штаті Вайомінг із липня 2019 р. діє закон, який прирівнює цифрові активи виключно до віртуальних валют. За цим законом, цифрові активи є виразом економічних і майнових прав або прав на доступ, зберігаються в цифровому форматі та

охоплюють цифрові споживчі активи, цифрові цінні папери та віртуальну валюту [98].

Цифрові споживчі активи визначаються як цифрові активи, призначені для особистого чи побутового використання, зокрема токени блокчейну. Цифрові цінні папери — це цифрові активи, які є цінними паперами в електронній формі. Віртуальна валюта визначається як цифровий актив, що використовується як засіб обміну, одиниця рахунку або збереження вартості, але не визнається урядом США як офіційна валюта.

Цей вузький підхід обмежує поняття цифрових активів до криптографічних одиниць, таких як віртуальні валюти. Схожим до зазначеного акта є модельний закон Канади — Уніфікований закон про доступ до цифрових активів довіреними особами, розроблений Конференцією з уніфікації права Канади. Він визначає цифровий актив як «запис, створений, відтворений, переданий або збережений у цифровій формі за допомогою електронних, магнітних, оптичних або інших подібних засобів» [101].

Цікавий підхід до визначення цифрових активів застосовано на Бермудських Островах. У 2018 р. там було ухвалено Закон про діяльність у сфері цифрових активів (Digital Asset Business Act). Це спеціалізований нормативно-правовий акт, який регулює правові засади обігу цифрових активів.

Відповідно до цього Закону, цифровий актив — це будь-який об'єкт, що існує в бінарній формі, визначає майнові права та є цифровим виразом вартості, який:

– використовується як засіб обміну, одиниця розрахунку або засіб збереження вартості, але не є законним платіжним засобом;

– слугує для вираження активів, таких як боргові зобов'язання або право власності засновника;

– може представляти інші активи або права на них;

– забезпечує доступ до програм, послуг або продуктів у контексті функціонування розподіленого реєстру.

Закон також визначає види діяльності у сфері цифрових активів, зокрема випуск і продаж віртуальних монет, токенів, надання послуг з обміну та електронних гаманців для цифрових активів. Поняття «цифрові активи» охоплює й віртуальні валюти, але залишає відкритим список форм цифрових активів, що допускає можливість включення нових видів. Таким чином, цей підхід можна охарактеризувати як вузький підхід до визначення «цифрового активу» [102].

Законодавці Королівства Таїланд теж обрали спеціалізований (вузький) підхід до визначення цифрових активів. У 2018 р. в країні було ухвалено Декрет про діяльність у сфері цифрових активів (Emergency Decree on Digital Asset Businesses). Відповідно до цього акта цифрові активи визначаються як криптовалюти та цифрові токени, що детально окреслює основи регулювання обігу таких активів [103].

Отже, нині існують два підходи до визначення цифрових активів — широкий і вузький. Однак останнім часом вузький підхід набуває популярності в нормативному визначенні цього поняття. Важливо також розуміти цифровий актив з точки зору його найактуальнішого значення, а саме забезпеченості реальними активами.

На сучасному етапі розвитку вітчизняної наукової думки відсутні комплексне тлумачення та єдині підходи серед вчених до визначення поняття «цифрові активи». Такий стан певною мірою ускладнює розуміння сутності та обігу цифрових активів, а також викликає інформаційну асиметрію спотворюючи трактування наявної інформації, закладеної в базис їх існування. Наявність такого неоднозначного тлумачення зумовлює подальше поглиблення суперечностей серед як теоретиків, так і практиків ринку цифрових активів.

Зокрема, серед учених і експертів-практиків справді існують різні підходи до визначення поняття «цифрові активи», що зумовлено різноманітністю форм, функцій і сфер застосування цих активів. Розбіжності в підходах можна пояснити тим, що цифрові активи розглядаються з різних аспектів.

По-перше, технологічний аспект. Цифрові активи можуть бути пов’язані з різними технологіями, тож і визначення залежатиме від того, яку технологію вважають основною для конкретного цифрового активу. Як приклад можна навести криптовалюту, яку переважно розглядають як окремий вид цифрових активів – децентралізовану валюту Bitcoin [104].

По-друге, правовий аспект. Передусім юридичні та регуляторні підходи до визначення цифрових активів можуть відрізнятися залежно від країни. Наприклад, у деяких юрисдикціях цифрові активи розглядаються як фінансові інструменти, в інших – як товар або навіть як окремий клас активів. Це, у свою чергу, створює різні підходи до їхнього визначення в науковій літературі.

По-третє, економічний аспект. Так, з економічної точки зору науковці та практики можуть класифікувати цифрові активи залежно від функції у фінансових ринках: як засіб обміну, засіб збереження вартості або інвестиційний інструмент. Різні економісти можуть акцентувати увагу на різних аспектах цифрових активів, що впливає на їх визначення.

По-четверте, міждисциплінарний підхід. Цифрові активи можуть вивчатися з точки зору різних наукових дисциплін: економіки, права, інформаційних технологій, фінансів. Це може призводити до різних підходів і визначень залежно від того, які аспекти вважаються найважливішими.

По-п’яте, різні форми цифрових активів. Існує багато типів цифрових активів, кожен з яких має особливості: криптовалюти, цифрові токени, NFT, віртуальні предмети з відеоігор і навіть цифрові документи. Кожен із цих видів може мати своє специфічне визначення залежно від контексту.

Можна стверджувати, що відсутність єдиного підходу до визначення цифрових активів свідчить про складність та багатогранність цього поняття. Кожен підхід відображає різні аспекти та контексти, в яких цифрові активи використовуються або вивчаються. У зв'язку з цим у наукових і практичних колах тривають дискусії щодо створення більш універсального визначення, яке б об'єднало ці різні підходи.

Тож і ми в цьому дослідженні спробуємо подати авторське визначення поняття «цифрові активи». Для цього передусім буде здійснено аналіз наукової літератури, присвяченої дослідженню таксономії та термінології цифрових активів.

На сучасному етапі розвитку економічної науки питання термінологічної диференціації цифрових активів є надзвичайно актуальним і водночас проблемним. Більшість сучасних учених виокремлюють щонайменше п’ять ключових груп понять, які використовуються для позначення цифрових активів, демонструючи різні аспекти і підходи до їхнього визначення.

Перша група безпосередньо пов'язана з поняттям «цифрові активи». Це визначення представлено в наукових працях таких авторів, як Дж. П. Бантинкс [105], Г. Х. Грей [106], Е. Харбінья [107], А. Кудь та І. Пипенко [108], М. Д.Уокер [109], які акцентують увагу на економічній сутності та ринкових характеристиках цифрових активів.

Друга група охоплює термін «активні дані», концепція якого досліджується Р. Е. Петерсоном [110], Лі Яксіонгом та Ні Шанем [111], а також Ши Ай-сінь, Гао Діном, Се Цзіном [112] і Цінь Жуншеном [113]. Ці автори підкреслюють інформаційний характер цифрових активів та їхню роль у процесах цифровізації та управління інформаційними ресурсами.

Третя група зосереджена на понятті «цифрова валюта» або «криптовалюта». Дослідження в цій галузі виконано Н. Захаровою [114], Д. М. Ленцем [116], Дж. Оуенсом [117] та С. П. Вінком [118]. Ця група авторів акцентує увагу на монетарних і фінансових характеристиках криптовалют, їхній функції як засобу платежу та збереження вартості.

Четверта група виокремлює поняття «токени», яке розглядається у роботах З.С. Пестовської [119], Б. Хайнса [120] та Б.Ю. Москвіна [121]. Вони наголошують на юридичних і технологічних особливостях токенів, їхній ролі у забезпеченні прав власності та доступу до цифрових послуг чи активів.

П’ята група зосереджується на «віртуальних активах», дослідження яких проводили Т. Гудима [122] та О. Черних [123]. Цей підхід звертає увагу на загальну цифрову форму активів, їхнє застосування в економічній діяльності та регуляторні питання.

Водночас існує значна група науковців, аналітиків і практиків (зокрема Д. М. Ленц, Ж. Овенс, С. П. Вінк), які не розмежовують ці поняття, вважаючи їх синонімічними і використовуючи одночасно у своїх дослідженнях. Це спричиняє певне «змішування» понятійного апарату, що призводить до теоретичних суперечностей і неоднозначності в розумінні сутності цифрових активів.

Таким чином, сучасний стан наукової дискусії свідчить про необхідність подальшого уточнення, диференціації та уніфікації термінів. Подолання існуючих теоретичних розбіжностей є важливою умовою для формування ефективної регуляторної політики та подальшого розвитку цифрової економіки.

Повертаючись до предмета нашого дослідження, проаналізуємо наукові підходи до визначення сутності поняття «цифрові активи». Як ми вже зазначали, у вчених немає одностайності з цих питань.

Вперше термін «цифрові активи» запропонував у 1996 р. Х. Мейєр [124], а у 2006 р. В. Нікерк [125] визначальний цифрові активи як будь-який текстовий або медіапроєкт, відформатований як двійковий вихідний код, що містить права на використання. У 2013 р. А. Тойгар [126] підтримав та розвинув (поглибив) цю точку зору, вважаючи, що цифрові активи – це право власності на дані, які зберігаються у двох формах на комп’ютері чи в Інтернет-хмарі. Слід зауважити, що основна спільна характеристика згаданих досліджень – існування у двійковій формі.

Разом із тим інша група вчених зосереджується на економічній природі активів цифрових активів, наголошуючи на тому, що саме така їхня характеристика може принести власникам/підприємствам очікувані економічні вигоди. Так, у тому ж 2013 р. Ван Сяогуан [127] визначив цифрові активи як немонетарний актив із потенційною економічною цінністю, який належить або

контролюється особою чи установою, існує у формі цифрової інформації, утримується для продажу в повсякденній діяльності або перебуває у виробничому процесі.

На думку Харбінья Е. [107] і Уокер М. Д. [109], будь-яка оцифрована сутність є цифровим активом. Так само і Бантинкс Дж. П. [105] визначає, що цифровим активом можуть бути будь-які цифрові дані від програмного коду до файлів на комп'ютері. Водночас він наголошує на відмінності цифрових активів від криптовалюти. Також окремі аналітики-науковці звертають увагу на відмінність дефініцій «криптовалюта» і «цифровий актив» (Бантинкс Дж. П. [105], Грей Г. Х. [106], Харбінья Е. [107], Куд А. та Пипенко І. [108], Уокер М. Д. [109]). Утім, окрема група фахівців навпаки, ототожнює цифрові активи з криптовалютою (Ленц Д. М., Вінк С. П.) [116,118].

Деякі автори, як-от Вінк С. П. та Овенс Ж. [118,117] намагаються обґрунтувати сутність поняття «цифрові активи» через окремі аспекти оподаткування.

Отже, розглянемо таксономію цифрових активів на основі наукових робіт Робочої групи при Європейській комісії та Раді Європи. Першою спробою дослідження сутності криптовалют стало Керівництво, опубліковане в липні 2018 р. під назвою «Криптовалюти та блокчейн: правовий контекст і наслідки для фінансових злочинів, відмивання грошей та ухилення від податків» [128], що сприяло їх інтеграції в 5-ту директиву ЄС стосовно ПВК/ФТ (AMLD5) [24].

Порівняння останніх стандартів FATF щодо ПВК/ФТ для віртуальних валют і AMLD5 продемонструвало, що перша європейська програма ПВК/ФТ щодо віртуальних валют значно відставала від міжнародних стандартів у цій сфері. Але для розуміння формування визначення розглянемо порівняльну таблицю (табл. 1.6).

Таблиця 1.6

Порівняння Рекомендацій AMLD5 та FATF

	5AMLD	FATF
АКТИВИ	Віртуальні валюти означають цифрове подання вартості, яке не випускається і не гарантується центральним банком або державним органом, не обов'язково прирівнюються до законодавчо встановленої валюти і не має юридичного статусу валюти чи грошей, але приймаються як засіб обміну, які можна передавати, зберігати та торгувати в електронному вигляді (Стаття 3 (18) AMLD4.) [129].	Віртуальний актив - це цифрове представлення вартості, яке може торгуватися цифровим способом або передаватися, а також може використовуватися для платіжних або інвестиційних цілей. Віртуальні активи не включають цифрові подання фіатних валют, цінних паперів та інших фінансових активів. [223].
ЗОБОВ'ЯЗАНІ ОСОБИ	Постачальники, що займаються обмінними послугами між віртуальними та фіатними валютами. Постачальник зберігача-гаманця означає організацію, яка надає послуги із захисту приватних криптографічних ключів від імені своїх клієнтів, зберігання, зберігання та передачу віртуальних валют (Стаття 3 (19) AMLD4) [129]	Постачальник послуг з віртуальних активів означає будь-яку фізичну або юридичну особу, на яку інші дії не поширюються згідно з Рекомендаціями, і як бізнес здійснює одну або кілька з таких видів діяльності або операцій для іншої фізичної чи юридичної особи або від її імені обмін між ВА та фіатними валютами; обмін між однією або кількома формами ВА; переказ ВА; - зберігання та/або адміністрування ВА або інструментів, що дозволяють контролювати ВА; участь та надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажом ВА [223].

Джерело: побудовано автором за [129, 223, 24]

Враховуючи нову термінологію в Рекомендації 15 FATF «Нові технології», а саме введення термінів ВА та ППВА, європейські науковці А. Снієрс, Р. Хьюбен [85,128,91] з дослідницької групи «Бізнес та право» Університету Антверпена (Бельгія) розробили таксономію віртуальних активів з метою створення відповідного цій таксономії європейського законодавства. Наступне керівництво «Криптоактиви – ключові події, регуляторні проблеми та відповіді» [130] було оприлюднено у квітні 2020 р.

Для адекватного вирішення проблем, визначених чинною фінансовою нормативно-правовою базою щодо криптоактивів, науковці вирішили розрізняти віртуальні активи, які є, по суті, оцифрованими фінансовими інструментами, та ті, що є, по суті, оцифрованими токенами електронних грошей, і всі інші віртуальні активи.

Незважаючи на часте використання терміна «віртуальні активи», немає загальновизнаного визначення того, що являє собою криптоактив. Різні визначення було прийнято регулюючими органами та органами, що встановлюють стандарти, з метою їхньої моніторингової та наглядової роботи або для інших цілей:

- Робоча група ЄЦБ з криптоактивів визначила цей термін дуже вузько, як «будь-який актив, записаний у цифровій формі, що не є і не представляє ні фінансової вимоги, ні фінансової відповідальності будь-якої фізичної чи юридичної особи і який не втілює майнового права проти суб'єкта господарювання» [131];
- IOSCO визначив цей термін як «тип приватного активу, який насамперед залежить від криптографії та DLT або подібної технології як частина його сприйманої чи властивої вартості, і може представляти актив, такий як валюта, товар чи цінний папір, або бути похідним інструментом. на товар або цінний папір [94]»;
- FSB запропонувала подібне визначення: як «вид приватного активу, що залежить насамперед від криптографії та розподіленого реєстру або подібної технології як частина їхньої сприйманої або властивої вартості [132, с. 10]». Це визначення також згадується в документації BIS [133];
- згідно з визначенням FSB, ESMA визначив криптоактив як «тип приватного активу, що передусім залежить від криптографії та DLT або подібних технологій як частина їхньої сприйманої чи властивої вартості». ESMA використовує цей термін для позначення і так званих віртуальних валют, і «цифрових токенів» (які він визначає як «будь-яке цифрове представлення

інтересу, що може мати цінність, право на отримання вигоди або виконання визначених функцій чи може не мати певної мети або використання»). Відповідно до ESMA криптоактив додатково означає актив, що не емітується центральним банком [97];

- EBA визначив криптоактив подібним чином як «актив, що: а) залежить переважно від криптографії та DLT або подібної технології, як частина його сприйнятої або властивої вартості; б) може використовуватися як засіб обміну та/або для інвестиційних цілей та/або для доступу до товару чи послуги» [89].

За винятком визначення Цільової групи ЄЦБ з криптоактивів (яке, схоже, охоплює лише те, що можна назвати традиційними «незабезпеченими» криптовалютами (такими як біткоїн та лайткоїн), усі наведені визначення мають дуже широке трактування. Двома повторюваними компонентами є (1) приватний характер активу та (2) використання криптографії і DLT або подібних технологій.

Беручи до уваги обсяг мандата ЄЦБ, цілком зрозумілим є обмежений обсяг визначення криптоактивів цільовою групою ЄЦБ. Однак це дослідження прагне вийти за рамки і охопити більше, ніж лише традиційні «незабезпечені» криптовалюти. Тому він продовжує ґрунтуватися на визначенні EBA та визначає криптоактив як приватний цифровий актив, що:

- записується на певній формі цифрової розподіленої книги, захищеної криптографією;
- не видається і не гарантується центральним банком або державним органом;
- може використовуватися як засіб обміну та/або для інвестиційних цілей та/або для доступу до товару чи послуги.

Як зазначають ESMA [97] та EBA [89] у звітах за січень 2019 р. щодо криптоактивів (та ICO), було доцільно розширити сферу визначення віртуальних валют до всіх типів криптоактивів, а також включити інвестиційні та утиліті-

токени. Причина проста: токени використовують ту саму технологію, що і криптовалюти. Їх можна передавати та зберігати в електронному вигляді і, у багатьох випадках, торгувати на тих самих платформах, що і криптовалютами [134]. Їхня конструкція робить їх придатними до виконання ролі «транспортного засобу» для переміщення економічної цінності незалежно від здійснюваної функції. Іншими словами, вони однаково придатні для діяльності ВК/ФТ, як і криптовалюти. Щоб створити адекватніший режим ПВК/ФТ, ЄС повинен дотримуватися найновіших стандартів FATF, вносити відповідні зміни до європейської системи протидії відмиванню коштів та фінансуванню тероризму і, можливо, навіть виходити за рамки.

Дослідження показують, що традиційні «незабезпечені» криптовалюти, такі як біткоїн, як і раніше, залишаються найбільш широко використовуваними криптоактивами у ВК/ФТ. Однак, з огляду на останні тенденції в криптопросторі, така ситуація може змінитися. ЄС було б доцільно застосувати режим ПВК/ФТ як технологічно нейтральний і якомога відкритіший, щоб ураховувати поточні зміни [186] та уникати необхідності вживати регуляторних заходів щоразу, коли особа змінює свою звичну поведінку.

Віртуальні активи можуть набувати різних форм і мати різні характеристики. Теоретично можна здійснити поділ між криптовалютами, криптоактивами та токенами.

Криптовалюти (або монети), такі як біткоїн і лайткоїн, – це віртуальні активи, що використовуються як одиниці рахунку. Вони можуть становити рівнозначну альтернативу законному платіжному засобу, виданому урядом.

Водночас токени – це віртуальні активи, які пропонують своїм власникам певні економічні та/або управлінські та/або корисні/споживчі права. Взагалі це цифрове представлення інтересів або прав на (доступ) до певних активів, продуктів чи послуг. Токени зазвичай випускаються на наявній платформі або блокчейні для залучення капіталу з метою нових підприємницьких проєктів або

для фінансування стартапів або розвитку нових (технологічно) інноваційних послуг.

У деяких юридичних джерелах криптовалюти також називають «платіжними», «обмінними» або «валютними» токенами. Однак така термінологія може викликати плутанину та має недоліки. Токени переважно представляють право на певний актив або певне зобов'язання, тоді як криптовалюти, особливо традиційні «незабезпечені» криптовалюти, зазвичай не містять внутрішніх прав чи правил.

Криптовалюти стали першим видом криптоактивів, що з'явилися на ринку, а створення біткоїна датується кінцем 2008 – початком 2009 р. Токени, що випускаються емітентом у процесі трансакцій, зазвичай у межах залучення фінансування, набули широкої популярності з кінця 2017 р., і ця тенденція зберігається досі. Вони становлять так зване друге покоління криптоактивів.

Поява та зростаюча популярність криптовалют і їхніх базових технологій спонукали різні центральні банки досліджувати доцільність випуску власних цифрових валют для оптових розрахунків або як доповнення чи заміну фізичних банкнот та монет (CBDC). CBDC — це цифровий актив або оцифрований інструмент, випущений центральним банком для здійснення платежів та розрахунків у роздрібних або оптових операціях [135]. Оскільки він випускається центральним банком і є його зобов'язанням, його можна вважати «суверенною валютою». Різні центральні банки та фінансові регулятори наголошують, що випуск CBDC не залежить від використання конкретної технології, наприклад, розподіленого реєстру (DLT).

CBDC можуть мати низку переваг, проте викликають і певні занепокоєння, зокрема в контексті монетарної політики. Попри те, що як криптовалюти, так і CBDC є цифровими валютами, їм властиві принципові відмінності. Криптовалюти, що є підкатегорією криптоактивів, мають приватний характер, зазвичай використовують технологію DLT і не випускаються та не гарантуються центральним банком. Натомість CBDC – державний інструмент, який

випускаються офіційним регулятором і має гарантії центрального банку. Тому важливо чітко розмежовувати криптовалюти та криптоактиви загалом і CBDC (рис. 1.5) [64].

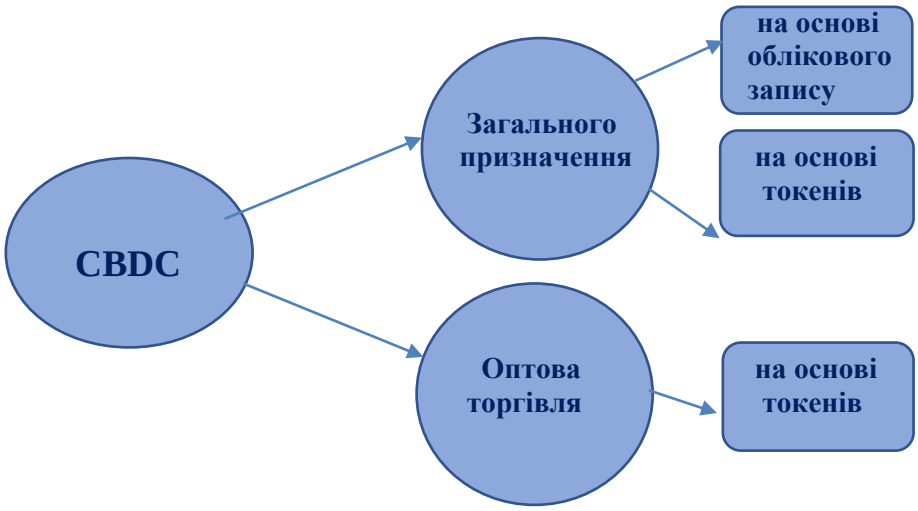


Рисунок 1.5 Класифікація CBDC

Джерело: складено автором

Криптовалюти можуть бути забезпеченими («стабільними») чи незабезпеченими. Перша хвиля криптовалют, яка розпочалася з біткоїнів та сотень наступних їхніх клонів, фактично розглядається їхніми користувачами як «щось цінне». Вони не представляють будь-який базовий актив, вимогу чи зобов'язання, що робить їх схильними до високої волатильності. Було б коректніше назвати їх традиційними «незабезпеченими» криптовалютами [106].

Дуже мінливий характер традиційних криптовалют, що не мають резервного забезпечення, ускладнює їхнє використання як повноцінної валюти, тобто як засобу обміну, накопичення вартості та одиниці рахунку. Це перешкоджає їхньому широкому впровадженню. Тому центральні банки зазвичай утримуються від використання терміна «криптовалюти» для загального позначення таких криптоактивів.

Деякі прихильники криптовалют визнали, що висока волатильність цін першої хвилі криптовалют стала значною перешкодою для їхнього прийняття як засобу платежу та збереження вартості. Для вирішення цієї проблеми вони запропонували так звані стейблкоїни (stablecoins).

Стейблкоїн — це різновид або підкатегорія криптовалют, що, як правило, прив’язана до вартості іншого активу або кошика активів і призначена для підтримання стабільної вартості. Як і традиційні «незабезпечені» криптовалюти, стейблкоїни створені для виконання функцій валюти. Однак, на відміну від традиційних криптовалют, що зазвичай є децентралізованими та не мають ідентифікованого емітента або установи, відповідальної перед користувачами, стейблкоїни здебільшого представляють зобов’язання конкретного емітента щодо базових активів, фондів або інших фінансових прав. Іншими словами, вони мають певне забезпечення, а не просто розглядаються як «щось цінне» самі по собі. Прикладами стабільних монет, які вже перебувають в обігу, є, серед, інших Tether (USDT), різноманітні DAI (DAI) та Gemini Dollar (GUSD).

Стейблкоїни мають низку однакових властивостей із «токенами» та іноді навіть ідентифікуються як такі. Як і токени, стабільні монети зазвичай випускаються на наявному блокчейні й утілюють вимогу до ідентифікованого емітента або на активи, що підтримують монети. Однак, хоча токени випускаються з цілком конкретним функціональним призначенням або певною метою (наприклад, для надання власникам прав власності та/або прав, подібних до дивідендів, або для забезпечення доступу до певного продукту чи послуги), у стабільних монет таких функцій переважно немає. Вони призначені для використання в ролі засобу обміну загального призначення: для здійснення можливості купівлі-продажу товару чи послуги, що надається кимось іншим, ніж емітент. Тому їх слід відрізняти від стейблкоїнів, а не ідентифікувати як такі [111].

Стейблкоїни — це криптовалюти, вартість яких прив’язана до вартості іншого активу або кошика активів, таких як валюти, товари чи фінансові інструменти. Стейблкоїнам властивий вищий потенціал, ніж іншим криптовалютам, що зазнають ризику високого ступеня волатильності.

Незважаючи на те, що стейблкоїни можуть отримувати цінність від будь-якого базового активу, їх можна поділити на три категорії [136]:

– стейблкоїни, забезпечені державними резервами, такі як Tether, USDC, BUSD, які забезпечені резервами в грошовому еквіваленті, як-от фіатна валюта, депозити;

– публічні алгоритмічні стейблкоїни, такі як DAI, TerraUSD, що підтримуються смарт-контрактами та алгоритмами, які автоматично захищають прив'язку;

– інституційні стейблкоїни, такі як JPM Coin, що випускаються в приватних мережах для внутрішнього/корпоративного використання (рис. 1.6).

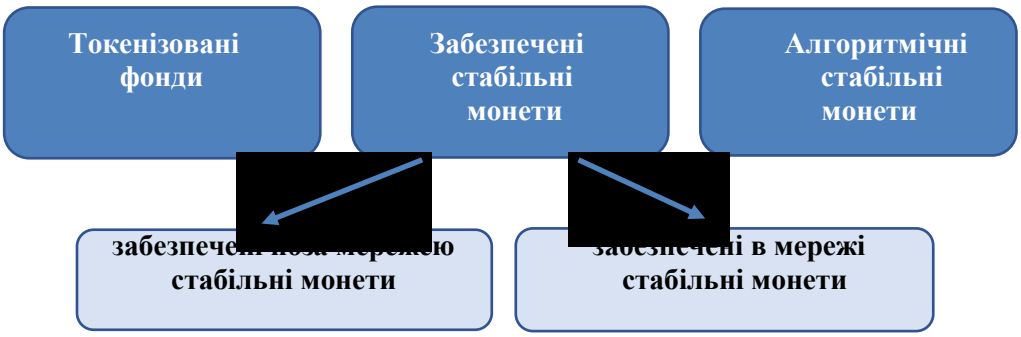


Рисунок 1.6. Класифікація стейблкоїнів.

Джерело: складено автором

Тоді як стейблкоїни майже не змінюють своєї вартості, оскільки прив'язані до реальних активів, алгоритмічні стейблкоїни є більш ризикованими та схильними до волатильності. Водночас стейблкоїни загалом є менш ризикованими порівняно з традиційними криптовалютами. Їхній дизайн та механізм управління відіграватимуть ключову роль у визначенні їхнього торгового життєвого циклу та прийнятті обґрунтованих інвестиційних рішень.

Деякі компанії активно досліджують можливості використання стейблкоїнів, забезпечених державними резервами, щоб отримати вигоду з крипторинку. Наприклад, банк ANZ випустив стейблкоїн, прив'язаний до австралійського долара, що дозволяє користувачам купувати та продавати цифрові активи, криптовалюти та NFT [137]. Тим часом Mitsubishi UFJ Bank планує запустити Progmacoin для клірингу та розрахунків за цифровими цінними

паперами [138]. Окрім цього, низка інших компаній досліджує альтернативні варіанти використання стейблкоїнів.

Токени можуть бути інвестиційними, утиліті токенами або їх гібридними формами. Подібно до того, як в даний час існує більше однієї категорії крипто валют, існує також більше однієї категорії токенів. Токени можуть приймати різні форми з різноманітними особливостями. З моменту їх концепції були розроблені різні підходи для їх класифікації та визначення. Більшість регулюючих органів та науковці прагнуть відрізняти так звані «інвестиційні» токени від так званих «утиліті» (маркетингових) токенів [138].

Інвестиційні токени - іноді їх також називають токенами цінних паперів або жетонами активів - це ті токени, які, як правило, забезпечують права їхніх власників у формі прав власності та/або прав, подібних до дивідендів. Відомим прикладом інвестиційного токена є «токен BNK», який надає його власнику право на щотижневу комісію, що виплачується в криптовалюті «ефір» (ETH). Інвестиційні токени, як правило, випускаються з метою залучення капіталу (тобто за допомогою ICO) і демонструють схожість із традиційними борговими та пайовими інструментами. Однак термін «інвестиційний токен» також використовується для позначення традиційних цінних паперів або інших активів, які пройшли процес токенізації (тобто які були зареєстровані на блокчейні у вигляді токена) [138].

Утиліті-токени — це токени, які надають власникам доступ до певної програми, продукту чи послуги, зазвичай на основі новоствореної блокчейн-інфраструктури. Вони зазвичай використовуються виключно для доступу до продуктів або послуг, розроблених емітентом токенів, і не приймаються як засіб оплати за інші товари чи послуги. Таким чином, утиліті-токени відрізняються від криптовалют.

Прикладами утиліті-токенів є Golem (GNT) та Filecoin (FIL), які забезпечують доступ до певних послуг: обчислювальних потужностей (Golem) та зберігання даних (Filecoin). Подібно до інвестиційних токенів, утиліті-токени

також випускаються для залучення фінансування, зазвичай з метою подальшого розвитку програми, продукту чи послуги емітента. Однак, на відміну від інвестиційних токенів, їхня основна мета — не створення майбутніх грошових потоків для інвесторів, а забезпечення доступу до продуктів чи послуг емітента та одночасне формування бази користувачів. Вартість утиліті-токенів зазвичай визначається їхньою функціональною корисністю [138].

Інвестиційні та утиліті-токени можуть надавати власникам певні управлінські права в емітенті. Наприклад, інвестиційні токени можуть передбачати право голосу щодо розподілу прибутку, тоді як утиліті-токени можуть надавати право голосувати за оновлення функціональної структури послуг емітента. Після випуску обидва типи токенів можуть бути розміщені на вторинних ринках, зокрема на так званих «криптовалютних біржах», де їх можна обмінювати на фіатні гроші або інші криптоактиви (зазвичай криптовалюти).

Хоча теоретично можна провести чітку межу між криптовалютами та токенами, а також розрізнити інвестиційні та утиліті-токени, на практиці це не завжди просто. Багато криптоактивів поєднують ознаки кількох категорій, виконуючи одночасно інвестиційні, маркетингові або платіжні функції. Такі активи зазвичай називають «гібридними токенами», і вони створюють особливі виклики для регулювання.

Прикладом гібридного токена, точніше інвестиційно-маркетингового гібриду, є Crypterium (CRPT). Він використовується для оплати комісій за транзакції при користуванні послугами емітента (банківське рішення), надає право на знижки на майбутні послуги та можливість отримання доходу. Ці дослідження можна представити у вигляді наступної схеми розподілу (рис. 1.7).

Варто зауважити, що запропонована систематика не є незмінною та остаточною. Багатоманітність підходів до визначення терміна «віртуальні активи» зумовлює певну варіативність у його тлумаченні. Крім того, наведена класифікація відображає сучасний стан розвитку крипторинку, який постійно

еволюціонує. Відповідно, концепції та визначення, актуальні сьогодні, можуть зазнати змін або потребувати уточнення в майбутньому.

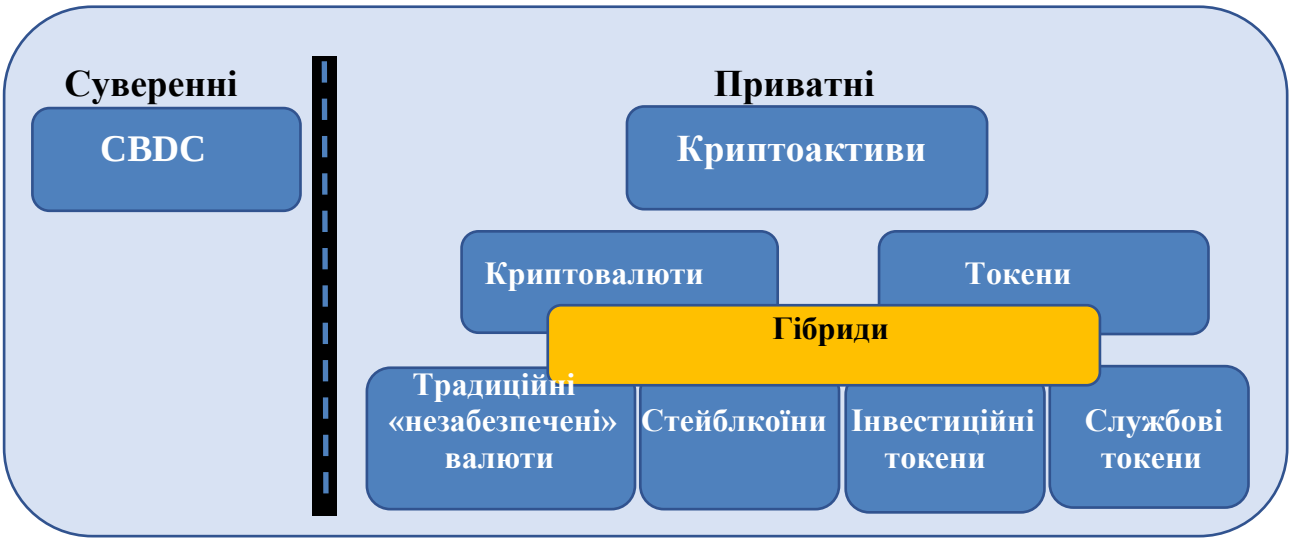


Рис. 1.7. Таксономія криптоактивів.
Джерело: складено за матеріалами [128]

Ще одним підходом до класифікації віртуальних активів став розподіл за сутністю криптоактивів та відповідності органу регулювання в Європейському Союзі. Ми окреслили підходи європейських регуляторів до визначення віртуальних активів. Нагадаємо, MiCA регулює криптоактиви, які не охоплюються Директивою про ринки фінансових інструментів (MiFID II) та Директивою про електронні гроші (EMD2). Застосування Директиви залежить від сутності інструменту, а не від технології, використовуваної для його випуску («субстанція над формою»). Тому MICA регулюватиме три підкатегорії криптоактивів (табл. 1.7).

Таблиця 1.7

Підкатегорії криптоактивів, що регулюються в проєкті MiCA

1. **Службові токени**, які випускаються з нефінансовими цілями для надання цифрового доступу до програми, послуг або ресурсів, доступних в мережах DLT.

Продовження таблиці 1.7

2. **«Токени, забезпечені валютними цінностями та активами»**, які мають на меті підтримувати стабільну вартість шляхом «посилання на кілька валют, які є законним платіжним засобом, один або кілька товарів, один чи кілька криптоактивів або кошик таких активів». і згодом виступають як засіб платежу для купівлі товарів і послуг і як засіб збереження вартості.
3. **«Токени електронних грошей»**: криптоактиви зі стабільною вартістю лише на основі однієї фіатної валюти, яка має на меті функціонувати подібно до електронних грошей (заміна фіатної валюти в платежах), як визначено в Директиві ЄС 2009/110/ЕС.

Джерело: Складено автором за матеріалами [80]

MiCA не застосовуватиметься до криптоактивів, що кваліфікуються як:

– фінансові інструменти (як визначено у ст. 4(1), п. (15) Директиви 2014/65/ЄС);

– електронні гроші (як визначено у п. (2) ст. 2 Директиви 2009/110/ЄС, за винятком випадків, коли вони кваліфікуються як токени електронних грошей відповідно до цього Регламенту);

– депозити (як визначено в ст. 2(1), п. (3) Директиви 2014/49/ЄС;

– структуровані депозити (як визначено у ст. 4(1), п. (43) Директиви 2014/65/ЄС);

– сек'юритизація (як визначено у п. (1) ст. 2 Регламенту ЄС 2017/2402) (рис. 1.8).

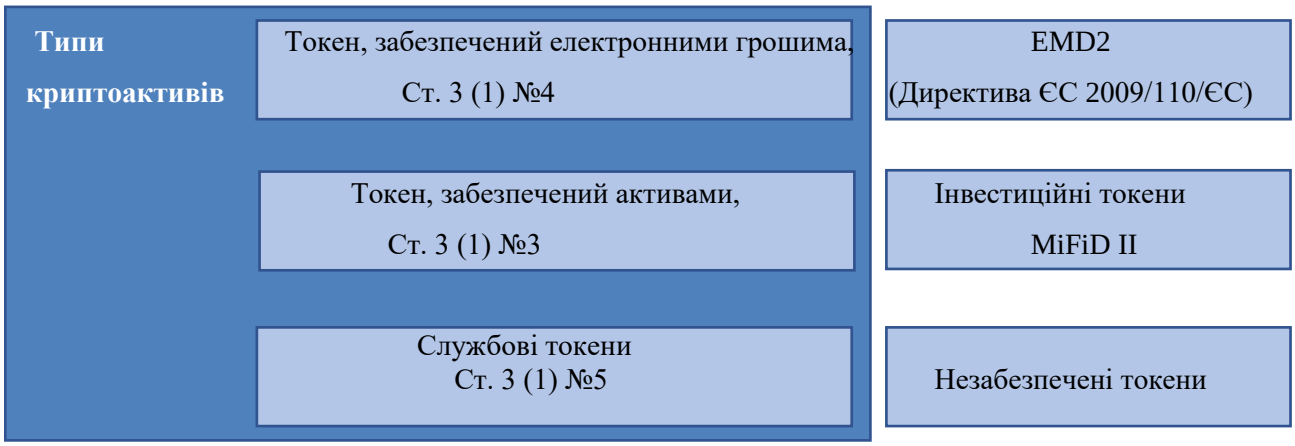


Рис. 1.8. Таксономія криптоактивів.

Джерело: складено за матеріалами [127]

Варто зазначити, що згадані директиви ЄС та регламент MiCA не регулюють обіг NFT і діяльність ринку ВА в децентралізованих фінансах (DeFi), за винятком стейблкоїнів, та Метавсесвіті. Далі надано визначення та пояснено сутність цих явищ у блокчейн-мережах.

NFT, або невзаємозамінні токени (англ. non-fungible token), – особливий вид криптовалюти, який не можна обміняти на інші токени, на відміну від більшості криптовалют і багатьох мережевих або службових токенів. Це унікальні активи, що існують тільки у власних криптосистемах, і кожен із них є окремим криптографічним токеном з обмеженою кількістю [139]. NFT являє собою одиницю даних у цифровій книзі, відомій як блокчейн, де кожен NFT відповідає унікальному цифровому об’єкту, роблячи його невзаємозамінним.

Децентралізовані фінанси (англ. Decentralized Finance, DeFi) — це екосистема загальнодоступних децентралізованих фінансових сервісів на основі публічних блокчейнів, які дають змогу використовувати фінансові послуги, такі як запозичення, кредитування і трейдинг, без необхідності покладатися на централізовані організації.

За спрощеним визначенням експертів централізованої криптобіржі WhiteBIT, «DeFi — це фінансова технологія, базована на захищених розподілених реєстрах. Це середовище, яке дає змогу використовувати фінансові послуги без необхідності покладатися на централізовані організації. У системі DeFi фінансові послуги надаються через децентралізовані додатки (dApps), більшість з яких розгорнуто на платформі Ethereum. DeFi протистоїть централізованій фінансовій системі, надаючи людям можливість пірингового обміну» [140].

Метавсесвіт, або метасвіт (англ. metaverse, від грец. μετά- та англ. universe), — мережа віртуальних просторів, орієнтована на соціальну взаємодію. Це віртуальне середовище, де люди через свої графічні зображення можуть спілкуватися між собою та взаємодіяти з цифровими об'єктами за допомогою технологій віртуальної, доповненої або змішаної реальності [141].

Ринок NFT стрімко зріс завдяки обіцянкам прозорості обігу та прав власності. У 2021 р. обсяг глобального ринку невзаємозамінних токенів (NFT) досяг 17,6 млрд дол. США, що майже у 215 разів більше, ніж у 2020 р. Кількість покупців NFT зросла до 2,3 млн осіб порівняно з 75 тис. у 2020 р. У 2022 р. ринок NFT продовжив зростання, досягнувши обсягів торгів у 57,2 млрд дол. США. Однак у 2024 р. обсяги торгівлі NFT знизилися на 19 % порівняно з 2023 р., досягнувши 137 млрд дол. США. Кількість продажів NFT теж зменшилася на 18 %, досягнувши 50 млн. Ці дані свідчать про значну волатильність ринку NFT, з періодами як стрімкого зростання, так і спаду [142].

З появою Метавсесвіту NFT отримують більшу корисність. Експерти Gartner Inc. прогнозують, що до 2026 р. 25 % людей будуть проводити принаймні одну годину на день у Метавсесвіті для роботи, покупок, навчання, реалізації соціальних чи розважальних цілей [140]. NFT можуть слугувати засобом обміну вартості в економіці токенів. Оскільки токени унікальні, NFT можна використовувати для корисних предметів, таких як покупка землі, як показано в Метавсесвіті Decentraland, а також для отримання квитків на різні події в цьому просторі [141].

Зацікавленість глобальних компаній у NFT та Метавсесвіті теж зростає. Nike випустила колекцію NFT віртуальних кросівок і потрапила в заголовки новин, продавши їх за 134 тис. дол. США [148]. Платіжна система Mastercard подала заявку на 15 торгових марок у проєктах Метавсесвіту щодо надання послуг, пов’язаних з оборотом NFT, включно з проведенням платежів із використанням кредитних карток [146].

З боку інвесторів так само спостерігається зростання зацікавленості у проєктах Метавсесвіту. Fidelity Investments запустила ексклюзивний біржовий фонд, щоб запропонувати інвесторам ознайомитися з продуктами та послугами, пов’язаними з Метавсесвітом [147]. Однак разом зі стрімким зростанням інтересу до Метавсесвіту та розвитком економіки творців NFT існує загроза відкриття неліквідного ринку та використання його в злочинних цілях.

Відповідно до звітів американського транснаціонального банку Citibank, загальний адресний ринок послуг, пов'язаних із Метавсесвітом, оцінюється в межах від 8 до 13 трлн дол. США з 5 млрд користувачів до 2030 р. [148]. Метавсесвіт можна розглядати як наступний рубіж для залучення клієнтів у банківський сектор, який нині переважно розвивається від традиційного до цифрового банкінгу, але також стоїть на порозі масового використання децентралізованих фінансів.

Американський транснаціональний банк JP Morgan у той час, коли запустив «Onyx Lounge» у Метавсесвіті Decentraland, став першим глобальним банком, який увійшов у проєкти Метавсесвіту [149]. Такі банківські установи, як HSBC і Standard Chartered, теж занурилися в розроблення власних бізнес-проєктів у Метавсесвіті. HSBC оголосив про свій план придбати земельну ділянку в Метавсесвіті в онлайн-проєкті, створеному у вигляді Метавсесвіту у форматі P2E (play-to-earn), який дає змогу заробляти гроші під час гри, – The Sandbox, щоб надати інноваційний досвід для любителів спорту, кіберспорту та ігор [150]. HSBC запустив фонд для дослідження можливостей інвестування в Метавсесвіт для своїх заможних клієнтів в Азії, тоді як британський міжнародний фінансовий конгломерат Standard Chartered співпрацює з The Sandbox для створення Метавсесвіту [151], а фінансова платіжна компанія Worldline створила спеціальну віртуальну демонстраційну залу в The Sandbox [148].

NFT започаткували нову еру цифрових товарів і також мають потенціал для трансформації фінансових індустрій. Компанії, які надають фінансові послуги, почали вивчати та інвестувати в NFT і проєкти, пов'язані з Метавсесвітом.

Mastercard співпрацює з Coinbase, щоб користувачі могли робити покупки за допомогою своїх кредитних карток на ринку NFT Coinbase [153]. NFT з'являються як застава в просторі кредитування DeFi, де власники токенів можуть отримувати доступ до коштів без ліквідації своїх унікальних активів.

Спрощення NFT-торгівлі стало певною мірою несподіваним явищем для державного регулювання фінансових послуг.

NFT також відкривають нові можливості для шифрування та керування конфіденційними даними, оскільки забезпечують безпечний, прозорий і захищений від несанкціонованого доступу механізм, пропонують користувачам безпечні засоби для захисту та управління їхніми особистими даними й цифровими активами за допомогою цифрової ідентифікації [154]. NFT використовують для токенізації документів, таких як акредитиви, у фінансуванні торгівлі, щоб усунути посередників і ефективніше запобігати шахрайству.

Токенізація, управління активами, зберігання та інтеграційні послуги (наприклад, зв'язування NFT з різними платформами чи навіть Метавсесвітом) створюють нові можливості для операторів цифрових активів. Наприклад, компанія Goldman Sachs вивчає використання NFT для токенізації реальних активів, таких як фінансові інструменти. Завдяки широким перспективам у цій сфері очікується, що фінансова індустрія й надалі використовуватиме NFT та Метавсесвіт для бізнес-орієнтованих цілей і надання інноваційних послуг своїм клієнтам [155].

З розширенням взаємодії споживачів із Метавсесвітом компанії фінансових послуг мають можливість ідентифікувати нових клієнтів, залучати їх у Метавсесвіт і пропонувати послуги, пов'язані з ним, такі як гаманці та зберігання цифрових активів. Страхові компанії також повинні адаптувати свій портфель до віртуального середовища і створювати нові рішення, що відповідатимуть очікуванням клієнтів у Метавсесвіті. Традиційні страхові провайдери вже роблять перші кроки: AXA France, наприклад, придбала ділянку у The Sandbox для своєї присутності в Метавсесвіті [156].

Вплив NFT і Метавсесвіту на фінансові послуги ще потребує часу для повного розкриття потенціалу. NFT стикаються з технічними, юридичними та регуляторними викликами, які необхідно подолати перед повним упровадженням, а також з викликами в регулюванні, що зумовлює занепокоєння,

оскільки окремі країни, такі як Китай, планують обмежити фінансову діяльність, пов’язану з NFT [157].

Стандартизація та регулювання можуть істотно сприяти впровадженню та корисності NFT у різних сферах застосування. ООН схвалила проєкт компанії Tencent, спрямований на розроблення технічної основи та безпекової системи для NFT [158]. Для прискорення стандартизації віртуального середовища також було створено Форум стандартів Metaverse, який об’єднав понад 30 організацій, включно з Microsoft, Meta, W3C, Nvidia, Qualcomm, Sony, Unity, Epic Games та ін. [159]. Однак ці ініціативи можуть потребувати часу, тому важливо застосувати збалансований підхід до використання зазначених вище цифрових інновацій.

Волатильність криптовалют, як і вразливість до атак, повільність трансакцій і значні витрати на електроенергію, пов'язані з методами перевірки, можуть стримувати їхнє сприйняття суспільством. Водночас віртуальні активи, зокрема стейблкоїни, отримують дедалі більший попит як на роздрібних ринках, так і серед інституційних інвесторів. Традиційні фінансові компанії та ППВА мають адаптуватися, щоб стати надійними радниками для своїх клієнтів у їхній власній діяльності з цифровими активами.

Для зниження ризиків фінансової стабільності з боку криптоекосистеми може знадобитися скоординоване регулювання між централізованими (CeFi) та децентралізованими фінансами (DeFi). Пропозиції Базельського комітету з банківського нагляду щодо криптоактивів банків є важливим кроком до глобальних стандартів, які допоможуть вирішити міжнародні питання.

Європейський Союз завершує створення нормативної бази для діяльності ринку ВА для захисту інвесторів і підтримки фінансової стабільності у 27 державах-членах.

У рамках оцінки ризиків створюються детальна класифікація та систематизація різних типів ВА і ППВА, а також описуються основні загрози у сфері ПВК/ФТ, які вони можуть спричиняти. Аналіз загроз охоплює використання ВА та діяльність ППВА на різних етапах відмивання злочинних

коштів, включно зі злочинами-попередниками, такими як торгівля наркотиками, шахрайство, підробка та крадіжка.

Оцінка ризику встановлює рівень невід'ємного ризику для восьми типів і підтипів ВА. Псевдонімні ВА, наприклад, Bitcoin, та анонімні ВА, такі як Monero (Додаток Б), мають дуже високий рівень невід'ємного ризику через високий ступінь анонімності, зручність використання та особливості безпеки (табл. 1.8).

Для проведення детальної оцінки ризику необхідно розглянути різні типи ВА, оскільки ці типи матимуть різні профілі ризику залежно від їхніх властивостей. Огляд різних типів та підтипів ВА у в світі, з описом прикладів та комбінованою ринковою вартістю, наведено в Додатку Б.

Таблиця 1.8

Оцінка ризику використання віртуальних активів в операціях щодо відмивання коштів, отриманих злочинним шляхом.

Типи	Підтипи	Невід'ємний ризик
Платіжні ВА (криптовалюти)	Псевдоанонімні	Дуже Високий
	Анонімні	Дуже Високий
	Платформи	Високий
	Stablecoins (Монети)	Середній
Утіліті (службові) ВА		Низький
Інвестиційні ВА	Забезпечені ВА	Низький
	Платформа ВА з функціями забезпечення	Середній
ВА закритих екосистем		Дуже Низький

Джерело: побудовано автором

На основі ВА, описаних у додатку, можуть бути створені традиційні фінансові інструменти, пов'язані з ВА, наприклад, інвестиційні фонди, деривативи, пов’язані з ВА, та ті, що інвестують у ВА або ф’ючерси на основі вартості певних ВА.

Віртуальні активи мають унікальні технологічні характеристики, що забезпечують псевдоанонімні й анонімні трансакції, швидку передачу вартості через кордони та безособові ділові відносини. Анонімні криптоактиви створені

для забезпечення підвищеного рівня приватності та анонімності під час здійснення трансакцій. Прикладами таких криптоактивів є Monero та Zcash (Додаток Б), які використовують сучасні криптографічні технології для повного приховування даних про трансакції. Анонімні криптоактиви послуговуються різними механізмами та протоколами для забезпечення приватності трансакцій. До основних методів належать:

- кільцеві підписи, що приховують особу відправника, створюючи кілька можливих варіантів підпису, серед яких неможливо визначити справжній;
- генерація прихованих одноразових адрес гаманців для кожної трансакції, що ускладнює відстеження отримувача.

З огляду на високий рівень анонімності використання таких криптоактивів може нести надвисокі ризики. В окремих країнах вони заборонені, зберігання їх на анонімних гаманцях вимагає додаткових заходів безпеки, щоб уникнути зломів або крадіжок.

Псевдоанонімні криптовалюти, такі як біткоїн, забезпечують відносний рівень приватності. Хоч адреси користувачів і деталі трансакцій є загальнодоступними в публічному блокчейні, встановлення зв’язку між конкретними особами та їхніми трансакціями потребує додаткового аналізу, здебільшого за допомогою блокчейн-аналітики, що здійснюється контрагентами ліцензованих ППВА та фінансовими установами. Таким чином, часткова анонімність зберігається до моменту впровадження політик та процедур ЗСК, ЗСТ і заходів ПВК/ФТ.

На відміну від цього, неанонімні криптовалюти, такі як Ripple (XRP), є повністю прозорими, оскільки вся інформація про трансакції та баланси гаманців є відкритою для загального доступу. Це робить їх менш привабливими для осіб, котрі прагнуть зберегти конфіденційність фінансових операцій.

Водночас такі властивості криптовалют можуть сприяти розвитку різноманітних фінансових продуктів і послуг, зокрема фінансування торгівлі, транскордонних платежів та врегулювання фінансових інструментів. Традиційні

фінансові установи визнають ці переваги. Наприклад, згідно з опитуванням Банку міжнародних розрахунків, проведеним серед 63 центральних банків, більшість із них розглядають можливість випуску віртуальних активів, підтриманих центральним банком [161].

Українські дослідники теж здійснюють наукові розвідки щодо обґрунтування сутності віртуальних і цифрових активів. У вітчизняних нормативно-правових актах не міститься поняття/визначення цифрових активів. Натомість використовується поняття ВА, що визначаються в Законі України «Про віртуальні активи» як нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування й оборотоздатність ВА гарантуються системою забезпечення обороту ВА. ВА можуть посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав [162].

Також нещодавно змінами до Цивільного кодексу України внесено ново дефініцію — «цифрова річ»: «Цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність. Цифровою річчю є віртуальні активи, цифровий контент та інші блага» [163].

З наведених вище визначень, що містяться в Цивільному кодексі України та Законі України «Про віртуальні активи», можна побачити тотожність із визначенням поняття «цифрові активи» науковцями.

Серед досліджень і пропозицій щодо визначення «цифрового активу» доцільно виділити методичний посібник «Прогнозування впливу цифрових активів на соціально-економічний розвиток підприємства», в якому автори ґрунтовно розглядають комплекс базових понять цього феномену. Поєднавши поняття «цифровий» та «актив», автори визначають цифровий актив як цінність, виражену в цифровому вигляді, а також зазначають що такий актив являє собою набір цифрових (двійкових) даних, які є автономними, унікально ідентифікованими та мають певну цінність [164].

Під час уточнення поняття цифрового активу автори дотримувалися певних критеріїв і розглядали його сутність з економічної, правової, інформаційної, ціннісної позиції. Дослідниками з цих позицій було обґрунтовано поняття «цифровий актив» як інформаційний ресурс, похідний від права на цінність і такий, що обертається в розподіленому реєстрі у вигляді унікального ідентифікатора. Запропоноване поняття «цифровий актив» представлено складовими (економічною, правовою, інформаційною, ціннісною), що характеризуються взаємозв'язком і взаємозалежністю [24].

Цифрові та віртуальні активи ототожнює А. С. Овчаренко, котрий також зауважує, що поняття «криптовалюта» є вужчим [165]. А. А. Кудь, М. А. Мащенко, І. С. Пипенко, І. В. Соболева визначають цифровий актив як цінність, виражену в цифровому вигляді, набір цифрових (двійкових) даних, що є автономними, унікально ідентифікованими та мають певну цінність [166]. Такий підхід схожий на позиції зарубіжних учених, які ми розглянули вище.

Доктор юридичних наук О. О. Дмитрик визначає, що цифрові активи необхідно розглядати як видове поняття, що становить певні цифрові об'єкти. При цьому вони можуть представляти вартість і бути збереженими та можуть обмінюватися в цифровій формі. Автор виокремлює ознаки цифрових активів: 1) електронна форма, тобто відсутність фізичної матеріальності, збереження на певних цифрових пристроях; 2) їхнім підґрунтям, як правило, виступає така новітня технологія як блокчейн, що дає їм змогу функціонувати без централізованого контролю або посередників, тобто забезпечує децентралізацію; 3) наявність криптографічного захисту, оскільки кожен актив має унікальний ключ для доступу; 4) анонімність і відносна безпека, бо власники цифрових активів можуть здійснювати певні анонімні трансакції, не розкриваючи своїх особистих дані; 5) відсутність посередників чи фінансових установ при їхньому русі; 6) різноманітність, оскільки вони використовуються на різні цілі (зокрема інвестування, збереження вартості, проведення трансакцій і створення цифрових колекцій мистецтва та ігор тощо) і, як наслідок, охоплюють віртуальні активи,

криптовалюти (Bitcoin, Ethereum), токени, NFT (невзаємозамінні токени), цифрові цінності, смарт-контракти і багато інших видів цифрових ресурсів [166].

А. А. Кудь визначає, що «цифровий актив – це інформаційний ресурс, похідний від права на цінність і такий, що обертається в розподіленому реєстрі у вигляді унікального ідентифікатора [164].

Цікавим є підхід до систематизації поняття «цифрові активи» та їхнього співвідношення з криптовалютами і токенами у З. С. Пестовської (табл. 1.9).

Таблиця 1.9

Взаємозв'язок понять криптовалют, токенів і цифрових активів

Цифровий актив - це нематеріальний актив, який створюється, продається та зберігається у цифровому форматі	
Криптовалюта	Токени криптовалют
унікальні підкласи цифрових активів, які використовують криптографію, передову техніку шифрування, яка гарантує справжність криптоактивів за рахунок усунення можливості підробки або подвійного витрачання коштів	
криптовалюти є власними активами блокчейна (BTC або ETH), яким можна торгувати, використовувати для обміну, для заощадження, для стимулювання користувачів до безпеки мережі криптовалюти	токени створюються як частина платформи, яка побудована на існуючому ланцюжку блоків (як токени ERC-20, які становлять екосистему Ethereum), є одиницями вартості, які організації або проекти, засновані на блокчейні, розробляють поверх існуючих мереж блокчейнів
криптовалюти є природним активом певного протоколу блокчейнів	токени створюються платформами, які будуються поверх цих блокчейнів
можуть зберігати цінність і обмінюватися	плюс можуть бути розроблені для представлення фізичних активів або традиційніших цифрових активів, або певної корисності або послуги

Джерело: Пестовська З.С. Токенізація економіки України: мрія чи реальність [166].

Ще один підхід до систематизації поняття «цифрові активи» та їхнього співвідношення з криптовалютами і токенів у статті Віталія Гавви «Цифрові фінансові активи: визначення та класифікація» запропоновано через введення терміна «цифрові фінансові активи» [168](рис. 1.9).



Рисунок 1.9. Види цифрових фінансових активів.

Джерело: за матеріалами [168]

Такий підхід до класифікації цифрових активів може бути застосований в обґрунтуванні підходів до оподаткування цифрових активів у частині оподаткування службових (utility) токенів податком на додану вартість, подібно до товарів у цифровій формі, але не має аналогів у міжнародних та європейський таксономіях.

Підсумовуючи викладене, зауважимо, що поняття «цифрові активи» значно еволюціонувало протягом останніх кількох десятиліть (від першої згадки про них і до сьогодні), відображаючи швидкий технологічний прогрес, поглиблення цифровізації фінансово-економічних відносин, а також зміну сприйняття цифрової власності.

Дослідження еволюції теоретичних підходів до визначення сутності поняття «цифрові активи» дало нам змогу здійснити періодизацію та виокремити етапи розвитку дефініції:

1-й етап (1990–2000 рр.). На цьому етапі розвитку наукової думки термін «цифрові активи» переважно стосувався будь-якого виду цифрового контенту або даних, що мали цінність: цифрових документів, зображень, аудіофайлів та відео. Термін «цифрові активи» здебільшого використовувався в контексті цифрових медіа та систем управління контентом (CMS). Наприклад, компанії почали усвідомлювати важливість ефективного управління своїми цифровими активами, такими як логотипи та маркетингові матеріали.

2-й етап (2000–2009 рр.). Цей етап характеризується появою інтернету та електронної комерції. З розвитком інтернету, електронної комерції та соціальних мереж поняття цифрових активів розширилося, охопивши вебсайти, доменні імена та цифрові акаунти (наприклад, профілі в соціальних мережах, електронні пошти). Цінність цих цифрових активів стала більш очевидною, оскільки компанії почали істотно залежати від онлайн-присутності та цифрового маркетингу. Зокрема, доменні імена стали визнаватися як цінні активи, іноді вартістю в мільйони доларів.

3-й етап (2009–2010 рр.). Цей етап став переломним з появою криптовалюти та технології блокчейну. Запуск біткоїна у 2009 р. є початком нової ери для цифрових активів. Криптовалюти та інші токени, базовані на блокчейні, почали визнаватися як новий клас цифрових активів. Ці активи унікальні тим, що вони децентралізовані, є цифровими представленнями цінності, які можна обмінювати або використовувати в трансакціях. Термін «цифрові активи» почав частіше використовуватися в контексті фінансових технологій (fintech) і децентралізованих фінансів (DeFi). Технологія блокчейн також представила концепцію «токенізації», де фізичні активи (наприклад, нерухомість чи мистецтво) могли бути представлені у вигляді цифрових токенів.

4-й етап (кінець 2010 – початок 2020-х років). Характеризується зростанням популярності NFT. Невзаємозамінні токени додали новий вимір до цифрових активів. На відміну від криптовалют, які є взаємозамінними (один біткоїн еквівалентний іншому), NFT унікальні й представляють власність на конкретний цифровий об'єкт, наприклад, цифрове мистецтво, музику чи віртуальну нерухомість. Вибуховий інтерес до NFT розширив розуміння цифрових активів, охопивши не лише фінансові інструменти, а й цифрові колекційні предмети, твори мистецтва та інші форми цифрової власності.

5-й етап (2020 р. – донині). Характеризується регуляторним та інституційним визнанням. Коли цифрові активи стали більш поширеними, вони привернули увагу регуляторів та інституцій. Цифрові активи тепер включають

криптовалюти, NFT, токени цінних паперів і цифрові представлення традиційних фінансових активів. Фінансові установи, уряди та регуляторні органи дедалі частіше зосереджуються на тому, як визначати, регулювати й інтегрувати цифрові активи в ширшу економіку. Також виникла концепція CBDC, яка представляє цифрову форму національної валюти.

На сьогодні термін «цифрові активи» стосується широкого спектра активів, які існують у цифровій формі. Цей термін продовжує охоплювати традиційний цифровий контент, такий як медіафайли та доменні імена, однак тепер він широко використовується в різних галузях, включно з фінансами, правом, технологіями та медіа. Постійний розвиток блокчейну та децентралізованих технологій продовжує формувати і розширювати визначення та застосування цифрових активів. З економічної точки зору, за ОЕСР та міжнародної консалтингової компанії PricewaterhouseCoopers, до цифрових активів відносять криптовалюти, стейблкоїни, невзаємозамінні токени (NFT), цифрові валюти центробанків (CBDC) та інвестиційні токени [165; 166].

У свою чергу, ґрунтовний аналіз термінології та таксономії цифрових активів дав змогу сформулювати узагальнене й комплексне авторське визначення. Так, з урахуванням фінансово-економічної природи явища, під цифровими активами ми розуміємо будь-яке цифрове представлення вартості, записане в криптографічно захищеній розподіленій книзі (блокчейні) або подібній технології, які існують виключно у цифровому середовищі та мають майнову цінність. Вони складаються із суверенних (CBDC) та приватних криптоактивів (ВА).

Таке визначення імплементує стандарти міжнародного та європейського права. Варто підкреслити, що європейський підхід до формування нормативно-правового середовища для віртуальних активів, реалізований через Регламенти ЄС у поєднанні з Директивами, забезпечує уніфікованість підходів і термінології в сфері державного регулювання цифрової економіки. Це впроваджується без необхідності змін до національного законодавства країн-членів ЄС.

Рівень прийняття цифрових активів в усьому світі збільшується. Кількість віртуальних активів з ринковою капіталізацією щонайменше на 1 млн. дол. США зросла з 30 до приблизно 1000 найменувань між 2015 і 2020 р., а загальна капіталізація всіх ВА наближається до 300 млрд. дол. США [160](табл. 1.10).

Таблиця 1.10

Глобальний Індекс сприйняття криптоактивів у Топ-20 країнах світу

Країни	Загальний рейтинг індексу	Показник обсягу централізованих сервісів	Показник обсягу крипто-валютних обмінників	Показник обсягів P2P трансакцій	Показник обсягів операцій в DeFi	Показник обсягів роздрібних операцій в DeFi
В'єтнам	1	5	5	2	7	6
Філіппіни	2	4	4	66	13	5
Україна	3	6	6	39	10	14
Індія	4	1	1	82	1	1
США	5	3	3	111	3	2
Пакистан	6	10	10	50	22	16
Бразилія	7	7	7	113	8	7
Таїланд	8	12	12	61	5	3
Росія	9	8	8	109	11	12
Китай	10	2	2	144	6	4
Нігерія	11	18	18	17	20	17
Туреччина	12	9	9	121	19	15
Аргентина	13	13	13	26	21	25
Марокко	14	19	19	21	33	18
Колумбія	15	23	23	10	27	29
Непал	16	17	17	19	34	41
Велика Британія	17	14	14	71	12	11
Еквадор	18	37	37	6	45	56
Кенія	19	43	43	5	9	34
Індонезія	20	16	16	129	18	13

Джерело: складено автором за матеріалами [171]

Глобальний Індекс сприйняття криптоактивів [171] за своєю методологією складається з п'яти субіндексів, кожен з яких ґрунтується на використанні різних типів криптовалютних сервісів у країнах. Експерти блокчейн-аналітичної компанії Chainanalysis оцінили 146 країн за п'ятьма показниками, обчисливши геометричне середнє значення для кожної країни в усіх цих показниках. Потім це значення нормалізується на шкалі від 0 до 1, що дає визначити оцінку для

кожної країни, яка відображає її загальний рейтинг. Чим ближчий остаточний бал країни до 1, тим вищий її рейтинг.

Незалежно від сприйняття криптоактивів вони навряд чи зникнуть. Коли в одному регіоні світу забороняється їх майнінг, він здійснює релокацію у сприятливіші місця. Наприклад, заборона майнінгу в Китаї у 2021 р. призвела до того, що більшість індустрії перемістилася до США, Казахстану та інших країн [172, 173]. Якщо в одному регіоні запроваджуються надмірно суворі регуляторні вимоги та оподаткування, ринок ВА швидко змінює юрисдикцію для власної діяльності, часто протягом кількох днів.

Криптотехнологія дає змогу виробникам, чиї виробничі потужності оснащені датчиками перевірки безпеки та системами відстеження поточної діяльності на основі блокчейну, перевіряти, чи вони виробляють відновлювану енергію, а потім миттєво представляти цю інформацію як унікальні одноразові токени. У середовищі DeFi ці токени можуть стати заставою для кредиторів. Модель надає інвесторам певну форму віддаленої безпеки, зокрема щодо програмованих криптовалют, стейблкоїнів або CBDC .

Перспективи отримання корисної інформації полягають у здатності технології негайно перетворювати дані на торгові активи, що є результатом її автоматизованого, майже миттєвого однорангового розрахунку та можливості визначати унікальні цифрові одиниці будь-якого розміру та вартості.

Ефективність є потенційно величезною, якщо порівнювати, скажімо, з аналогічним світом зелених облігацій, які вимагають багатьох рівнів бюрократії та базуються на ретроактивних даних, для створення та перевірки яких потрібний тривалий час. Однак це не означає, що в криптоіндустрії немає проблем. Фінансовий крах криптобіржі FTX виявив небезпеку культури спекуляцій, яка породила негативний вплив на обсяги інвестування в діяльність ринку ВА через шахрайство [174].

Такі події в індустрії вимагають упровадження чітких регуляторних норм та ефективних підходів до державного регулювання. Важливо уникати

використання застарілих регуляторних моделей традиційної централізованої фінансової системи для децентралізованих криптопроєктів, оскільки їхня діяльність має особливості. Наприклад, якщо застосувати централізоване рішення і спробувати змусити незалежні групи розробників з відкритим кодом нести відповідальність за користувачів протоколів DeFi, з якими вони взаємодіють, це може призвести до підвищення, а не зменшення ризиків.

Трьома основними джерелами нещодавніх фінансових криз стали централізовані сервіси (Centralized finances, CeFi) — Celsius, Voyager Digital та Three Arrows Capital. Водночас один із великих провалів, що фактично виявився схемою Понці, відомий як Terra Luna, був лише формально віднесений до DeFi. Справжні DeFi-проєкти, такі як Aave та Compound, показали свою стійкість під час цього інтенсивного стрес-тесту [175].

Проте в DeFi існують інші значні ризики. Згідно з оцінками компанії Immunefi, що спеціалізується на криптобезпеці, у II кв. 2022 р. було втрачено 670 млн дол. США через зловживання смарт-контрактами та їх зломи [175,176]. Щоб DeFi зміг залучити нових користувачів, їм знадобляться значно сильніші гарантії безпеки їхніх коштів.

Необхідно знайти баланс. Державні регуляторні органи повинні встановити суворіші фідуціарні вимоги для менеджерів послуг централізованих операторів ринку ВА, розглядаючи їх як брокерські компанії або інші регульовані фінансові установи. Однак для операцій у DeFi важливо співпрацювати з галуззю, щоб розробити рішення для саморегулювання, що використають технологічні переваги та децентралізовану структуру цієї сфери. Серед ідей є розширення системи «винагород за помилки», яка заохочує розробників за виявлення та виправлення інцидентів, упровадження обов’язкових періодичних аудитів програмного забезпечення, фінансового аудиту розробників та проведення частих стрес-тестів моделей кредитного плеча та застави.

Насамперед необхідно досягти консенсусу щодо визначення децентралізованої системи та того, чи правильно проєкти, які прагнуть розвиватися в цьому напрямі, реалізують свої наміри. Тому всі зацікавлені сторони зі сфер DeFi і традиційних фінансів (англ. – traditional finance (TradFi)) повинні спочатку узгодити рамки регулювання та загальну термінологію, а потім встановити стандарти й правила. Це складне завдання, але його потрібно виконати.

Висновки до розділу 1.

1. Ризик-орієнтований підхід у сфері ПВК/ФТ став сучасним стандартом регулювання фінансової системи. Він передбачає фокусування зусиль на найбільш серйозних загрозах та гнучке управління новими ризиками в міру їх виникнення Однак фундамент цього підходу закладено задовго до цифрової доби – у класичних економічних теоріях ризику середини XX століття. Автором проаналізовані принципи теорії ризику та невизначеності Френка Найта, теорії очікуваної корисності фон Неймана–Моргенштерна, портфельна теорії Гаррі Марковіца та економічна теорії регулювання ризиків Стіглера–Пельцмана трансформації для їхньої до обороту цифрових активів. У сфері ПВК/ФТ в умовах функціонування крипторинку та цифрової економіки спостерігається еволюція цих теорій, а саме від найтівського усвідомлення невизначеності – до прийняття гнучких стратегій на випадок появи невідомих загроз; від теорії очікуваної корисності – до вдосконалення стимулів і покарань, що змінюють раціональний розрахунок злочинця, і включення поведінкових чинників; від портфельної теорії – до бачення цілісного «портфеля ризиків» і оптимізації зусиль проти фінансових злочинів у різних напрямах одночасно; від економічної

теорії регулювання – до вироблення збалансованих, стійких до обхідних маневрів правил для нових фінансових технологій.

Автором зазначено, що розвиток цифрових фінансів приніс нові проблеми, яких не було за часів Найта чи Марковіца, на стику класичних теорій та сучасних реалій виникає низка міждисциплінарних викликів та автором наголошено на доцільності об'єднання зусиль різних дисциплін. Автор пропонує розглядати ризик-орієнтований підхід ПВК/ФТ як міждисциплінарний продукт: він ґрунтується на економічній ідеї оптимального розподілу ресурсів (МРТ Марковіца), враховує ймовірності та корисності (фон Нейман–Моргенштерн), розрізняє вимірювані та невимірювані чинники (Найт), і прагне ефективного регулювання попри поведінкові реакції (Стіглер–Пельцман). Цей підхід закріплений у методах оцінки ризиків в сфері ПВК/ФТ.

Таким чином, класичні теорії ризику не втрачають значення – вони перетворюються. Автором обґрунтовано, сьогоднішні виклики на кшталт криптовалют чи DeFi спонукають науку і практику оновити ці теорії, додавши до них багатовимірність та технологічну оснащеність. Полеміка між традиційним і новим зрештою веде до синтезу: виникають нові теоретичні конструкції (як-то поведінкова теорія регулювання або моделі ризику, керовані ШІ), що спираються на класичні засади, але здатні відповісти на питання XXI століття. В дисертації зазначено, що ефективна ПВК/ФТ значною мірою залежатиме від того, наскільки ефективно інтегрується економічна мудрість минулого з науково-технічним прогресом сучасності. Така інтеграція забезпечить сталий міждисциплінарний розвиток теорій ризику на благо безпеки фінансової системи й суспільства.

2. У межах дисертаційного дослідження автором обґрунтовано, що розвиток ринку ВА та цифрових технологій стали ключовими детермінантами оновлення міжнародних та європейських стандартів у сфері ПВК/ФТ. Автор зазначив, що така нормативна еволюція стала відповіддю на глобальні виклики, пов'язані з динамікою інновацій у сфері фінансів і використанням ВА в

трансзлочинній діяльності, та зумовила необхідність адаптації регуляторної бази до нових форм ризиків.

На думку автора, концептуально важливим у цьому контексті є європейський підхід до регулювання ВА, реалізований через Регламенти ЄС у поєднанні з Директивами. Це, як зазначено автором, забезпечує уніфікацію правових норм та термінології у сфері цифрової економіки на рівні Європейського Союзу, що є важливою передумовою для гармонізації регуляторної практики в державах-членах. Застосування таких правових інструментів дозволяє ефективніше реалізовувати ризик-орієнтований підхід у практиці ПВК/ФТ та забезпечувати належну координацію між національними та наднаціональними регуляторами.

Крім того, в дослідженні акцентовано, що розробка та тестування CBDC стало предметом глибоких макроекономічних досліджень. Зокрема, центральні банки аналізують вплив цифрових валют на інфляцію, грошову масу, банківську систему та кредитування. Такі дослідження, на думку автора, є основою для оновлення теоретичних підходів у регулюванні грошового обігу в умовах цифровізації, зокрема розширення економічної теорії регулювання ризиків і формування інституційних моделей, які враховують специфіку цифрового середовища.

3. У результаті проведеного ґрунтовного аналізу термінологічного апарату та таксономії цифрових активів в дисертаційній роботі було сформульовано узагальнене авторське визначення, яке врахувало їхню фінансово-економічну природу. Цифрові активи доцільно трактувати як цифрове представлення вартості, зафіксоване у криптографічно захищеному розподіленому реєстрі (зокрема, блокчейні), що існує виключно в цифровому середовищі та має майнову цінність. У структурному поділі таких активів виокремлено суверенні (CBDC) і приватні криптоактиви (ВА), що включають різноманітні форми цифрової вартості. Відособлення таких категорій, як стейблкоїни та інвестиційні

токени, дало змогу більш глибоко дослідити економічну поведінку користувачів та механізми збереження і передачі цифрової вартості.

Ключовим аспектом запропонованого автором підходу є інтеграція ризик-орієнтованої парадигми оцінки цифрових активів у контексті ПВК/ФТ. Через призму ризик-орієнтованого підходу цифрові активи постають не лише як інноваційні інструменти, а й як потенційні вектори фінансових зловживань. Встановлення чіткої ідентифікації активів, оцінки пов'язаних із ними ризиків і вразливостей дозволяють забезпечити більш цільову ПВК/ФТ. В дослідженні запропоновано зміщення фокусу регуляторної політики – від універсального контролю до адресного управління ризиками, пов'язаного зі злочинною діяльністю, зокрема ВК/ФТ.

Таким чином, уточнення сутності цифрових активів і їх класифікація крізь призму ризик-орієнтованого підходу не лише розширюють межі економічної науки, а й формують методологічне підґрунтя для розробки ефективних регуляторних стратегій у цифровій економіці. Це сприяє побудові безпечного, прозорого та стійкого до зловживань середовища обігу цифрових активів у відповідності до міжнародних стандартів FATF, ЄС та Базельського комітету.

Основні положення розділу містяться в роботах [36; 50; 122; 173; 176; 254; 258; 264]

РОЗДІЛ 2.
МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ВПРОВАДЖЕННЯ МІЖНАРОДНИХ ТА ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ПВК/ФТ НА НАЦІОНАЛЬНОМУ РІВНІ

2.1. Міжнародні та європейські методологічні стандарти оцінки ризику в сфері ПВК/ФТ та їх впровадження на наднаціональному, національному та секторальному рівнях

Ризик-орієнтований підхід (РОП) є фундаментальним принципом сучасної системи ПВК/ФТ. Впровадження цього підходу зумовлене необхідністю адаптивного реагування на нові загрози, пов’язані із цифровими активами, що формують специфічні ризики для фінансових систем.

Міжнародні стандарти FATF визначають ризик-орієнтований підхід як ключову основу ефективної системи ПВК/ФТ, закріплену у Рекомендації 1 FATF [24]. Країни повинні проводити системну оцінку ризиків відмивання коштів та фінансування тероризму і застосовувати відповідні заходи пропорційно до цих ризиків.

Оцінка ризиків у сфері цифрових активів ґрунтується на аналізі потенційних загроз, пов’язаних зі злочинною діяльністю, використанням криптовалют для ВК, ухилення від податків, ФТ, вразливостей системи, що включають псевдонімність транзакцій, глобальний масштаб діяльності, наявність анонімізуючих сервісів, відсутність уніфікованого регулювання, та наслідків реалізації таких ризиків.

Основними критеріями оцінки ризиків є тип клієнтів, географічна складова, продукти та послуги, а також канали їх доставки. Оцінка ризику

базується на визначенні ймовірності реалізації загрози через конкретну вразливість і потенційного масштабу негативних наслідків.

Ризик-орієнтований підхід став невід’ємною складовою міжнародних стандартів ПВК/ФТ щодо цифрових активів, який довів свою ефективність в умовах постійних технологічних змін. Його інтеграція у національні системи моніторингу дозволяє ефективно управляти новітніми фінансовими ризиками, підтримуючи водночас інноваційний потенціал цифрової економіки.

Згідно з міжнародною практикою, важливим елементом управління ризиками є забезпечення взаємозв'язку між різними типами ризиків та елементами управління ними [17, с. 159]. Прикладами цього є:

- графічне відображення алгоритмів процесів, ролей та відповідності учасників і їхніх взаємозв'язків;
- визначення каналів інформування про ризики;
- розвиток навичок управління ризиками, включно з навчанням відповідного персоналу;
- формування позитивної культури управління ризиками;
- ідентифікація ризиків і призначення відповідальних за управління ними;
- оцінка ризиків і визначення прийнятного рівня;
- планування заходів реагування;
- моніторинг і перегляд ризиків;
- звітність щодо управління ризиками;
- забезпечення впевненості керівництва, що ризики ефективно контролюються;
- підвищення рівня зрілості управління ризиками, що оцінюється за ефективністю практик і досягнутими результатами;
- експертні оцінки.

Для успішного досягнення цілей установи необхідно враховувати ризики на кожному етапі діяльності. Міжнародна практика передбачає впровадження таких послідовних кроків для реалізації системи управління ризиками.

1-й етап. Ідентифікація невизначеностей у діяльності установи.

2-й етап. Визначення показників, що відображають рівень невизначеності.

3-й етап. Виявлення факторів ризику, пов'язаних з невизначеністю.

4-й етап. Оцінка ризиків на основі методів їх вимірювання.

5-й етап. Застосування якісних методів аналізу ризиків.

6-й етап. Використання кількісних методів оцінки ризиків.

7-й етап. Прогнозування рівнів ризиків.

8-й етап. Управління ризиками: застосування методів їх мінімізації.

Перші три етапи разом називають ідентифікацією ризиків, що проводиться через аналіз причин та наслідків у їхньому чіткому взаємозв'язку. Однією з найпоширеніших помилок при ідентифікації ризиків є підміна або змішування понять «проблема», «причина» і «наслідки». Тому перед початком процесу встановлення причинно-наслідкових зв'язків важливо чітко зрозуміти значення цих термінів, як показано на рис. 2.1.



Рис.2.1. Причинно-наслідкові зв'язки в підході до оцінки ризику

Джерело: побудовано автором

Проблема зазвичай є очевидною і не потребує додаткових пояснень. Причина — це явище або процес, що вже існує і призводить до певних змін у середовищі, завжди передує наслідкам і є основою для оцінки подій, що «відбуваються не так». Наслідки — прямі результати певної проблеми. Варто зазначити, що одна причина може призводити до багатьох наслідків, і, навпаки, кілька причин можуть зумовити один наслідок.

Важливо усунути причину ризику, оскільки це дасть змогу уникнути повторення проблем і вдосконалити процеси, контроль та управління ризиками в організації. Міжнародна практика пропонує різні методи ідентифікації ризиків, такі як:

– чек-листи (переліки питань для перевірки виконання процесів);

– аналіз блок-схем (послідовний аналіз процесів із графічною візуалізацією);

– бенчмаркінг (порівняння з еталонними критеріями для впровадження найкращих практик);

– сценарне планування (аналіз зовнішніх чинників і можливих сценаріїв розвитку подій).

Ці методи можуть використовуватися для ідентифікації ризиків під час опитувань, мозкових штурмів або робочих нарад. Підходи «згори донизу» (top-down) та «знизу догори» (bottom-up) теж комбінуються для повного охоплення ризиків у всій організації.

Наступним етапом управління ризиками є їхнє оцінювання. Хоча термін «оцінка ризиків» іноді розуміється як одноразова дія, у діяльності організації цей процес є безперервним і регулярним, що охоплює всі рівні управління. Мета оцінки полягає у визначенні того, які з ідентифікованих ризиків є достатньо важливими і суттєвими для розгляду керівництвом. Оцінка ризиків базується на таких критеріях, як імовірність їх виникнення та вплив на здатність організації виконувати свої функції для досягнення встановлених цілей, завдань та місії.

Теплову карту моніторингу ризиків використовують як візуальний інструмент для оцінки та відображення рівнів ризику в організації чи проєкті. Вона допомагає визначити найбільш критичні загрози та пріоритети для управління ризиками. Найчастіше використовується для виявлення загроз у банківській діяльності, криптовалютних операціях, процедурах ПВК/ФТ у фінансовому секторі, для аналізу вразливостей ІТ-систем та оцінки ймовірності

атак в кібербезпеці та для оцінки операційних та стратегічних ризиків в проєктному менеджменті підприємницької діяльності.

Наприклад, оцінювання може проводитися у такому форматі (табл.2.1):

Таблиця 2.1.

Теплова карта моніторингу ризиків

За впливом ризиків на здатність установи виконувати функції для досягнення встановленої мети (місії), цілей та завдань		За ймовірністю виникнення ризику		
Критерій ризику	Числове значення	Низька ймовірність	Середня ймовірність	Висока ймовірність
Низький рівень впливу	1	1 (1 х 1) (зелена зона)	2 (1 х 2) (зелена зона)	3 (1 х 3) (жовта зона)
Середній рівень впливу	2	2 (2 х 1) (зелена зона)	4 (2 х 2) (жовта зона)	6 (2 х 3) (червона зона)
Високий рівень впливу	3	3 (3 х 1) (жовта зона)	6 (3 х 2) (червона зона)	9 (3 х 3) (червона зона)

Джерело: побудовано автором

За ймовірністю виникнення в Тепловій карті моніторингу ризиків їх поділяють на:

- низьку ймовірність – ризики, які ніколи не траплялися або виникають дуже рідко; можливість їх появи майже відсутня або вкрай мала;
- середню ймовірність – ризики, які можуть траплятися рідко, але можуть виникнути в майбутньому, зокрема ті, що вже мали місце в діяльності установи;
- високу ймовірність – ризики, які мають майже 100-відсоткову ймовірність виникнення або події, що нещодавно траплялися в діяльності установи.

За рівнем впливу в Тепловій карті моніторингу ризиків їх поділяють на:

- низький вплив – ризик мінімально або незначно впливає на спроможність організації, не створюючи серйозних перешкод для досягнення

цілей, виконання завдань та функцій; відсутній або малозначущий вплив на реалізацію процесів чи досягнення запланованих показників;

- середній вплив – ризик істотно знижує спроможність організації, але може бути усунений чи скоригований протягом короткого часу, незначно заважаючи досягненню цілей та реалізації процесів;
- високий вплив – ризик суттєво підриває здатність організації виконувати завдання та досягати цілі; коригування або відновлення можливе частково чи відбувається повільно.

Після оцінювання ризиків за критеріями ймовірності та впливу їм можна присвоїти відповідні рівні: високий, середній або низький. У разі змін рівня ризику слід оновити оцінку ризику, методи реагування та заходи контролю.

На третьому – шостому етапах здійснюється послідовний процес спочатку виявлення, а потім кількісної оцінки ризикових факторів невизначеності. Спочатку застосовуються якісні, а потім кількісні методи аналізу.

Якісний аналіз є відносно простим, і його основна мета полягає у визначенні можливих типів ризиків та факторів, що впливають на їхній рівень під час виконання конкретної діяльності. Важливо враховувати інтереси учасників цієї діяльності, включно з потенційними партнерів та конкурентів. Також якісний аналіз передбачає оцінку очікуваних позитивних результатів порівняно з можливими негативними наслідками діяльності. Цей підхід дає змогу ефективніше організувати діяльність, що вимагає подальшого кількісного аналізу.

Кількісний аналіз ризиків є важливим доповненням до якісного і дає змогу виразити ризики в числовій формі для їх аналізу та порівняння. Він полягає у визначенні розміру окремих ризиків та загального ризику діяльності. При цьому оцінюються ймовірність виникнення події та її вплив на ситуацію. Складність кількісного аналізу зумовлена такими характеристиками ризику, як невизначеність, імовірність, альтернативність, суб'єктивність і недостатність інформації.

Кількісна оцінка стає особливо важливою, коли організація має вибір між кількома альтернативними напрямами діяльності з урахуванням своїх пріоритетів. Проте вибір не завжди робиться на користь варіанта з найбільшим економічним ефектом. У певних випадках доцільніше обрати варіант із меншим економічним результатом, але з більшою ймовірністю реалізації та нижчим рівнем ризику. До кількісних методів відносять:

- статистичний аналіз;
- аналіз чутливості (вразливості);
- аналіз сценаріїв та розроблення дерева рішень;
- імітаційне моделювання ризиків за методом Монте-Карло.

Кількісна оцінка ризиків базується на таких ключових критеріях:

1) Рішення в умовах ризику оцінюються з огляду на ймовірність досягнення очікуваного результату та можливі відхилення від нього. Найкращим вважається рішення з меншим рівнем ризику порівняно з іншими.

2) Витрати на здійснення ризикованого рішення теж мають значення – перевага надається варіантам із меншими витратами.

3) Третій критерій стосується часу, необхідного для реалізації рішення. Найкращим є те, яке вимагає менше часу.

Критерієм кількісного оцінювання ризику є ймовірність отримання результату меншого за значення, яке вимагається:

$$К = В \text{ x } (Рп - Рф) \qquad (2.1)$$

де К –критерій оцінювання ризику;

В — ймовірність;

Рп — значення результату, що вимагається (те, що планується);

Рф — отриманий результат (фактичний).

Урахування ризику полягає в коригуванні управлінських рішень відповідно до оцінених рівнів ризику. Це може відображатися у плануванні показників результативності й організації процесу їх досягнення. Критерієм

кількісного врахування ризику є абсолютна величина, що обчислюється за формулою:

$$К = У \text{ x } В(У) \qquad (2.2)$$

де К — ступінь ризику;

У — очікувані втрати;

В(У) – ймовірність втрат.

Якісний аналіз зазвичай проводиться на стадії розроблення моделі діяльності з визначенням основних шляхів мінімізації ризику. До якісних методів належать:

- метод експертних оцінок;
- метод визначення періоду окупності інвестицій;
- метод аналогій;
- метод коригування процентної ставки на ризик;
- використання показників дисперсії та стандартного відхилення;
- метод критичних значень.

З розвитком цифрових технологій до якісних методів додано:

- метод класифікації (логістична регресія (LR, англ. logistic regression), класифікатор випадкових лісів (RF, англ. random forest)), метод найближчих сусідів (KNN, англ. k-nearest neighbor method), адаптивний бустинг (AdaBoost, англ. adaptive boosting) та екстремальний градієнтний бустинг (XGBoost, англ. eXtreme Gradient Boosting);
- методи оцінки VaR (англ. Value-at-Risk) (параметричної оцінки, історичного моделювання);
- метод прогнозування ймовірності ліквідації (PD, англ. predicted default), який поєднує щоденний діапазон щоденних наборів даних, таких як ціни відкриття, максимуму, мінімуму та закриття (OHLC, англ. open-high-low-close) з моделями ймовірності нульової ціни (ZPP, англ. zero price probability), часових рядів та кредитного скорингу;

- метод прогнозування динаміки щоденної волатильності (проста модель випадкового блукання, моделі HAR-RV (англ. heterogeneous autoregressive model of the realized volatility), ARFIMA (англ. autoregressive fractionally integrated moving average) та CARS (англ. creating a research space);
- метод зведення;
- метод машинного навчання.

Найчастіше в практиці оцінки економічного ризику застосовується статистичний метод. Однак трапляються ситуації, коли через брак достовірної інформації використання цього методу стає неможливим. У таких випадках широко використовуються методи, що ґрунтуються на досвіді та інтуїції, тобто евристичні методи або методи експертних оцінок.

Метод експертних оцінок зазвичай застосовують, коли статистичних даних немає. Для оцінки ризиків за цим методом проводять аналіз думок досвідчених фахівців-експертів. Основні завдання індивідуальних експертних оцінок полягають у прогнозуванні майбутніх подій і явищ, а також оцінці їх у поточний момент.

На сьомому етапі прогнозується розвиток ризиків, а на восьмому етапі застосовуються методи їх попередження.

Протягом тривалого часу категорія «ризиків» застосовувалася для аналізу явищ на мікрорівні, зокрема на ринках з асиметричною інформацією та під час ухвалення інвестиційних рішень. Це відбувалося в умовах нерівномірного розподілу інформації в просторі та часі, причому основна увага приділялася розрахунку ймовірності можливих результатів, що робило акцент на кількісному підході.

Ризик-орієнтований підхід почав активно впроваджуватися на фінансових ринках у другій половині XX ст. До цього періоду інвестори та фінансові установи дотримувалися більш консервативних стратегій, уникаючи ризику та надаючи перевагу стабільним активам, таким як облігації. Однак із розвитком фінансової теорії та портфельного управління на початку 1950-х років з'явилася

концепція ризик-орієнтованого підходу. Зокрема, модель Марковіца, представлена Гаррі Марковіцем у 1952 р., запровадила поняття ефективного фронту та ризикової премії [19]. Ця модель показала, що можна оптимізувати баланс між доходом і ризиком, розподіляючи активи в портфелі.

Надалі ризик-орієнтований підхід підтримали роботи таких науковців, як Вільям Шарп, Джон Лінтнер і Ян Мосіні, котрі допомогли глибше зрозуміти взаємозв'язок між ризиком і прибутковістю, а також удосконалили стратегії управління інвестиційними портфелями [20-22].

Отже, середина XX ст. стала початком активного розвитку ризик-орієнтованого підходу, який сьогодні є одним із ключових підходів до управління активами. Наукові дослідження в цій сфері тривають, зокрема в напрямі регулювання цифрових активів. Хоча попередні дослідження зосереджувалися на традиційних фінансових ринках, зростання популярності цифрових активів і нові ризики, пов'язані з їх обігом, свідчать про необхідність поглибленого вивчення ризик-орієнтованого регулювання саме в цьому секторі.

Водночас успішність методу аналізу ризиків у цих межах сприяла його поширенню на інші об’єкти, зокрема на галузеві та регіональні ризики. З розвитком глобалізації економічних процесів дослідження ризиків на рівні країн стало невід’ємною частиною державного та приватного управління. Активізація глобальних економічних процесів та зміна факторів національного розвитку не тільки призводять до посилення ризикових чинників на макрорівні та зростання впливу глобальних і регіональних ризиків, а й змінюють їх структуру в кількісному та якісному вимірі. У сучасній структурі ризиків дедалі більшу роль відіграють глобальні ризики, які впливають на масштаб і характер національних, галузевих та корпоративних ризиків. Це привертає увагу науковців та політиків до глобальних ризиків, зокрема світових економічних криз.

Вразливість світової економіки зросла на тлі відсутності наднаціональних механізмів прогнозування та стримування небезпечних чинників, що надає ризикам системного характеру.

Здебільшого серед чинників глобальних економічних криз є транснаціональна злочинність. Світова економічна криза 2008р. стала поштовхом до розроблення та впровадження ризик-орієнтованого підходу у сфері протидії відмиванню коштів, отриманих злочинним шляхом, та фінансуванню тероризму на глобальному рівні.

Оцінка й управління ризиками відмивання коштів мають відносно коротку історію. Керівництво FATF «Національна оцінка ризиків відмивання коштів і фінансування тероризму» [177] було опубліковане лише в лютому 2013 р., але активно оновлюється головним антилегалізаційним органом на підставі аналізу взаємних оцінок країн щодо імплементації 40 Рекомендацій FATF [178].

Методологія охоплює дві ключові складові оцінки впровадження міжнародних стандартів FATF:

1) технічна відповідність;

2) результати, індикатори та інші фактори, що застосовуються для оцінки ефективності впровадження. Технічна відповідність стосується впровадження конкретних вимог FATF, зокрема законодавчої бази, обов'язкових правозастосовних заходів, а також наявності, повноважень та процедур правоохоронних органів. Вона не охоплює вимоги щодо ефективності, які оцінюються окремо через компонент ефективності Методології.

Існують чотири рівні технічної відповідності: повна відповідність (без недоліків), переважна відповідність (незначні недоліки), часткова відповідність (помірні недоліки) та невідповідність (значні недоліки).

Ефективність є ключовою складовою оцінки відповідності країни міжнародним стандартам FATF. Оцінка ефективності має розглядатися поряд із технічною відповідністю. Вона спрямована на визначення того, наскільки національна система боротьби з відмиванням коштів і фінансуванням тероризму досягає цілей FATF та виявляє системні недоліки. Це дає змогу країнам фокусуватися на пріоритетних заходах для покращання своїх систем. У контексті Методології ефективність характеризується як «ступінь досягнення певних

результатів». У контексті протидії відмиванню коштів / фінансуванню тероризму (ПВК/ФТ) ефективність означає, наскільки фінансові системи та економіки здатні знижувати ризики та загрози відмивання коштів, фінансування тероризму та поширення зброї масового знищення.

Безпосередній результат 1 (R1. «Ризики відмивання коштів і фінансування тероризму усвідомлюються, і за необхідності здійснюється координація дій на національному рівні для ПВК/ФТ») демонструє ефективність ризик-орієнтованого підходу. Індикатор R1 відображає технічну відповідність вимогам FATF щодо використання цього підходу, тобто Рекомендації 1 «Оцінка ризиків та застосування підходу, заснованого на оцінці ризиків». Таким чином, ці два індикатори показують застосування ризик-орієнтованого підходу в країні з точки зору технічної відповідності та ефективності.

У жовтні 2020 року FATF оновила Рекомендацію 1 та пояснювальну записку до неї, в яких встановлено обов’язок для країн і суб'єктів приватного сектору виявляти, оцінювати, розуміти та управляти ризиками фінансування розповсюдження зброї масового знищення (ФРЗМЗ). Згідно з Рекомендацією 1 FATF, країни повинні виявляти, аналізувати та оцінювати внутрішні ризики щодо відмивання коштів і фінансування тероризму (ВК/ФТ), використовуючи ризик-орієнтований підхід (РОП). Це необхідно для того, щоб зіставити виявлені ризики з відповідними превентивними або пом’якшувальними заходами у сфері ПВК/ФТ.

Визначення, оцінка та розуміння ризиків ВК/ФТ є важливими складовими процесу побудови ефективної національної системи у сфері ПВК/ФТ. На рівні держави це забезпечується через розроблення відповідної політики та ухвалення обґрунтованих рішень, спрямованих на досягнення конкретних цілей. На рівні приватного сектору подібні цілі досягаються шляхом упровадження процедур належної перевірки клієнтів, моніторингу їхніх фінансових операцій та дотримання вимог чинного законодавства у сфері ПВК/ФТ для суб'єктів первинного фінансового моніторингу (СПФМ) і певних нефінансових установ.

У Керівництві FATF щодо застосування ризик-орієнтованого підходу у сфері ПВК/ФТ [179] наведено п’ять основних принципів:

1) Розуміння загроз і вразливостей, а також оцінка національних ризиків.

2) Наявність правової основи та регуляторних норм для впровадження підходу.

3) Розроблення основних механізмів нагляду за реалізацією ризик-орієнтованого підходу у середовищі СПФМ.

4) Ефективний розподіл обов’язків між органами моніторингу та забезпечення їх взаємодії.

5) Обмін інформацією між державним і приватним секторами щодо оцінки ризиків країни, типологій та методів протиправного використання фінансової системи особами, причетними до ВК/ФТ.

Аналіз документів FATF, зокрема настанов щодо оцінки ризиків ВК/ФТ на національному рівні та стратегій оцінки ризиків, дає змогу виокремити й сформулювати додаткові принципи Національної оцінки ризиків (НОР) у сфері ПВК/ФТ, які доповнюють зазначені п’ять принципів. Національна оцінка ризиків – системна діяльність, організована суб’єктами державного та первинного фінансового моніторингу, а також іншими державними органами, спрямована на виявлення і дослідження загроз, вразливостей, ризиків і наслідків у сфері ПВК/ФТ. Результатом оцінки є Звіт про характер і масштаби ВК/ФТ.

При цьому FATF надає країнам свободу у виборі методології для проведення НОР, з урахуванням їхніх особливостей, без нав’язування загальних підходів. Наведемо ключові визначення.

Загроза – особа або група осіб, діяльність яких може завдати потенційної шкоди державі, суспільству чи економіці. Йдеться, зокрема, про терористичні групи та їхніх прихильників, їхні фінансові ресурси, а також минулу, теперішню та майбутню діяльність у сфері ВК/ФТ.

Вразливістю вважаються сфери, де загроза може реалізуватися, або фактори, що сприяють цьому. Це можуть бути структурні елементи фінансової системи, механізми, послуги чи продукти, що використовуються для переміщення та зберігання фінансів. При оцінюванні вразливостей враховуються фактори, що створюють ризики у контрольно-наглядових заходах щодо ПВК/ФТ, а також особливості конкретних секторів, фінансових продуктів або послуг, які можуть бути привабливими для ВК/ФТ.

Наслідки – вплив злочинної діяльності, що може шкодити фінансовій системі, установам, економіці, населенню, бізнесу, національним і міжнародним інтересам, а також репутації й привабливості фінансового сектору країни для інвесторів.

Оцінка ризиків – аналіз загроз, вразливостей і наслідків, що базується на поєднанні кількісних (статистичних) та якісних (експертних) методів.

Оцінка ризиків на національному рівні тісно пов'язана з їхньою оцінкою на наднаціональному рівні, а також у конкретних секторах, галузях, видах економічної діяльності, продуктах, послугах та регіонах країни. Це забезпечує реалізацію принципу комплексності оцінки, який полягає в можливості узагальнення результатів окремих оцінок для створення цілісної картини національних ризиків.

Ризик-орієнтований підхід дає країнам можливість у межах вимог FATF використовувати гнучкіший набір заходів, щоб ефективніше розподіляти свої ресурси та застосовувати превентивні дії відповідно до характеру ризиків, зосереджуючи зусилля найбільш результативним способом.

Безумовною перевагою впровадження продуманого підходу до НОР у сфері ПВК/ФТ є сфокусованість на дисциплінованому та чітко регламентованому процесі збору, обробки й узагальнення необхідних даних для ухвалення обґрунтованих рішень у системі ПВК/ФТ на мікро- і макрорівнях.

Міжнародні стандарти ризик-менеджменту визначають ризик як функцію ймовірності виникнення негативних подій, що залежить від співіснування

загрози та вразливості до цієї загрози. Методологія МВФ визначає основні компоненти НОР і описує відповідні процеси та інструменти. Вона пропонує три ключові компоненти для оцінки ризиків ВК і ФТ: загрози, вразливості та наслідки. Іншими словами, ризикові події відбуваються, коли загроза реалізується через вразливість. Формально національний рівень ризику можна виразити як:

$$R = f[(T), (V)] * C \qquad (2.3),$$

де T – загроза; V – вразливість; C – наслідки прояву ризику ВК/ФТ. Відповідно, рівень ризику може бути пом’якшений шляхом зменшення загроз, вразливостей (слабких місць) або потенційних наслідків прояву ризику.

Рівень ризику ВК/ФТ (R) відображає чистий ризик, що враховує вплив управлінських контрольних заходів на зменшення загального невіддільного ризику, характерного для будь-якої діяльності. Іншими словами, контрольні механізми здатні знизити рівень загального ризику, але їх відсутність не призводить до збільшення звичайного ризику. Нагляд у сфері ВК/ФТ поділяється на дві категорії: загальні регуляторні вимоги для зменшення ризику та спеціалізований нагляд у сфері ВК/ФТ.

З точки зору оцінки ризику ВК загроза (T) великою мірою пов'язана із сутністю і обсягом потенційного попиту на операції з ВК, який формується суб'єктами, що володіють незаконно отриманими активами, які потребують легалізації. У випадку оцінки ризику ФТ загроза пов'язана із сутністю й обсягом коштів, призначених для фінансування тероризму, а також з юрисдикцією, через яку проходять відповідні кошти.

Отже, для належної оцінки ризиків ВК/ФТ необхідно зібрати дані за вказаними компонентами для формування індикаторів імовірності ВК/ФТ, які стануть невід'ємною частиною загальної НОР у сфері ПВК/ФТ. Створення цих індикаторів вимагатиме чіткого розуміння сутності, форм прояву та обсягів потенційних нелегальних доходів, що генеруються різними предикатними злочинами, а також чіткого уявлення про середовище ФТ у країні. Це дасть змогу

точно визначити рівень ризику ВК/ФТ, що буде вважатися суттєвим для вжиття всіх необхідних заходів у рамках національної системи запобігання та протидії ВК/ФТ.

Вразливість (*V*) в оцінці ризику ВК/ФТ пов'язана із сутнісними характеристиками продуктів, послуг, каналів їх розподілу, клієнтської бази, інституцій, систем, організаційних структур та юрисдикцій, включно зі слабкими місцями в національній системі ПВК/ФТ та механізмах регулювання і нагляду, які можуть використовуватися для ВК/ФТ. Головне завдання в оцінці вразливості — оцінити фактори, що сприяють успішному проведенню операцій ВК/ФТ щодо відповідних продуктів, послуг, категорій клієнтів, способів здійснення фінансових трансакцій тощо. Результатом такої оцінки повинне стати створення відповідних індикаторів вразливості. Останні можна групувати в такі категорії:

- географічне розташування;
- фінансові продукти і послуги;
- рівень тінізації відповідного сектору економіки;
- прогалини в системах ПВК/ФТ та адекватність механізмів регулювання і нагляду;
- рівень корупції в секторі економіки;
- ефективність правоохоронних органів і системи кримінального правосуддя;
- інші характеристики національної юрисдикції, що полегшують проведення операцій ВК/ФТ (рівень організованої злочинності).

Індикатори вразливості мають бути порівняні та об'єднані з індикаторами загроз для проведення всебічного аналізу ймовірності суттєвого й успішного ВК/ФТ.

Наслідки (*C*) стосуються результатів, які виникають унаслідок ризикових подій. Вони можуть мати вигляд завданих збитків, втрат активів, підриву репутації фінансової установи, втрати довіри клієнтів, а також втрат у доходах

бізнесу та держави загалом. Можна стверджувати, що процеси ВК/ФТ породжують наступні наслідки, які пов'язані безпосередньо з операціями ВК/ФТ та/або з використанням активів після їх легалізації.

Імовірність виникнення зазначених вище подій формує відповідні модулі аналізу ризику (МАР), що містять фактори, підфактори та їх індикатори. Кожен МАР виявляє унікальні ризикові фактори, пов'язані з конкретними загрозами та вразливостями, що впливають на ймовірність виникнення ризикових подій. Організацію та класифікацію подій, пов'язаних із ризиком ВК, а також аналітичні модулі, що використовуються для отримання непрямих (орієнтуючих) індикаторів імовірності ВК, наведено в табл. 2.2.

Таблиця 2.2.

Організація та класифікація подій, пов'язаних із ризиком ВК/ФТ

Чинники виникнення ризикових подій	**Загрози (T), вразливості (V), які збільшують ймовірність виникнення ризикової події (R):**		**Сфери аналізу (модулі факторів ризику)**	**Допоміжні фактори, (під-фактори) та індикатори**
1	2		3	4
Ризикова подія: 1) Здійснення операцій із ВК чи ФТ				
(1a) Внутрішні злочинні до ходи: створені або доступні	(t) Наявність внутрішніх доходів, одержаних злочинним шляхом (v) Неадекватне стримування внутрішніх предикатних злочинів		(A) Обсяг внутрішніх злочинних доходів: створених або доступних (1) (B1) Правоохоронні органи (стримування злочинності) (2)	Види злочинів, які генерують доходи: фіктивне підприємництво; ухилення від сплати податків; розтрата майна; зловживання службовим становищем та ін. Повноваження, ресурси, ефективність (3)
(1b) Закордонні злочинні доходи, які входять у національну юрисдикцію	(T) Наявність злочинних доходів іноземного походження (v) Існування транскордонних потоків товарів, послуг, активів, а також обставин, які можуть бути використаними для здійснення ВК у сфері зовнішньо-економічної діяльності. (v) Транскордонний контроль недостатній для стримування транскордонних операцій із ВК.		(C) Обсяг зовнішніх злочинних доходів, які входять у національну юрисдикцію (1) (D) Транскордонні продукти, послуги, активи і обставини (4) (E) Заходи транскордонного контролю (ретельної перевірки)	Юрисдикція походження злочинних доходів та фактори (види злочинів), які сприяють одержанню злочинних доходів у юрисдикції їх походження Специфічні транскордонні аспекти, які потребують всебічного аналізу (5) Переміщення валюти, фізичних активів, людей та здійснення фінансових транзакцій

Продовження таблиці 2.2

(1c) Зловживання продуктами, послугами, активами чи іншими обставинами даної юрисдикції для здійснення операцій із ВК	(v) Юрисдикція та її інституції, що генерують товари, послуги, активи та інші обставини, які можуть бути використані з метою ВК		(F) Характеристика загального середовища юрисдикції (G) Характеристика пропонованих продуктів, послуг, активів та наявних обставин їх використання (6)	Характеристика економіки, правової системи (верховенства права), бізнес клімату, якості регуляторної політики, політичного середовища, культури і доброчесності, зобов'язань у сфері ПВК/ФТ. Сектори, типи інституцій, масштаб, клієнтська база, канали збуту, загальні фактори стримування
1(d) Корупційні діяння, які полегшують ВК	(v) Корупція в системі правоохоронних		(H1) Корупція (7)	
Ризикова подія: 2) Суб'єкти ВК (включаючи партнерів-спільників і радників) не виявляються (не санкціонуються)				
(2a) Вчинені операції із ВД не виявляються відповідними суб'єктами взаємодії (СПФМ, СДФМ та правоохоронними органами)	(v) Правоохоронні органи не виявляють операції із ВК прямо (у процесі здійснення власних розслідувань) (v) Правоохоронні та інші уповноважені на виявлення	(v) Правоохоронні органи розслідують лише предикатні злочини (v) Правоохоронні органи не подають запитів до міжнародних ПФР чи не відповідають на запити міжнародних ПФР щодо ВК (v) Національний ПФР не одержує якісних повідомлень від СПФМ та СДФМ про операції із ВК через: (v) недостатність, неповноту, несвоєчасність та невідповідність повідомлень; (v) низьку якість повідомлень, включаючи надмірне (безпідставне) інформування; (v) неадекватний моніторинг транзакції; (v) неадекватну інформацію про клієнтів; (v) інституційна неспроможність СПФМ та СДФМ; (v) неадекватний регулятор-ний нагляд за СПФМ; (v) неефективний процес надання повідомлень до національного ПФР.	(B2) Правоохоронні органи (пряме виявлення ВК) (I) Система інформування про підозрілі фінансові операції (J) Моніторинг транзакцій та рахунків (K) Ідентифікація та профілювання клієнтів, подальші та посилені заходи обачності (L) Спроможність та компетенція інституцій (M) Регуляторний нагляд (N) ПФР	Ефективність стримування ВК та внутрішньої взаємодії Вимоги, кількісні та якісні ознаки, сектори, типи інституцій (СПФМ, СДФМ) (8) Вимоги, ефективність (9) Вимоги, ефективність Системи контролю, ресурси, методичне забезпечення Ефективність, особливо за умови виявлення недоліків Ефективність аналізу, надання інформації (Узагальнені матеріали/додаткові узагальнені матеріали)

Джерело: побудовано автором за матеріалами [179]

Модулі, зазначені в третій графі таблиці, називаються «Сфери аналізу» (модулі факторів ризику). Кожен із них визначає унікальні фактори ризику,

пов'язані із загрозами та вразливостями, які впливають на ймовірність настання ризикових подій протягом наступних 12 місяців, враховуючи ефективність наявних заходів контролю. Кожен фактор ризику має свій перелік індикаторів. Фактори ризику та їхні індикатори організовані у вигляді вкладеної ієрархії: на найвищому рівні перебувають ті фактори, що безпосередньо впливають на ймовірність виникнення ризику ВК або ФТ. На наступному рівні ієрархії розташовані підфактори, що впливають на фактори вищого рівня, і так далі. Остання графа таблиці 2.2 підсумовує основні індикатори найвищого рівня для кожного аналітичного модуля.

Аналітичні модулі оцінки ризику ВК використовують як кількісні, так і якісні індикатори, базуючись на інформації, отриманій з відкритих та приватних (комерційних) джерел (МВФ, Світовий банк, ООН, бази даних взаємної оцінки країн та опубліковані документи, непублічні дані з внутрішньої статистики органів влади).

У кожному аналітичному модулі кожен фактор ризику аналізується відповідно до його індикаторів, після чого цей фактор підлягає скоринговій оцінці (якісній оцінці в балах), що дає змогу визначити критерії прийняття рішень, пов'язаних із оцінкою ймовірності виникнення суттєвого ВК. Для кожного індикатора, пов'язаного з факторами ризику ВК, мають бути встановлені власні критерії прийняття рішень (групи бальних оцінок), що впливають на збільшення або зменшення такого ризику. Ці критерії повинні бути максимально стандартизованими для аналогічних типів індикаторів. Критерії прийняття рішень є описовими та базуються на якісній порядковій шкалі, що формується на основі скорингових оцінок факторів та індикаторів і складається із семи рівнів ризику (табл. 2.3).

Таблиця 2.3.

Оцінки рівня ризику

Оцінка рівня ризику	Опис рівня ризику	Пріоритет пом'якшення ризику
≤ 6-7	Дуже високий ризик	Дуже високий пріоритет
≤ 5-6	Значно вищий ризик	Значно вищий пріоритет
≤ 4-5	Вищий ризик	Вищий пріоритет
≤ 3-4	Середній ризик	Середній пріоритет
≤ 2-3	Нижчий ризик	Нижчий пріоритет
≤ 1-2	Значно нижчий ризик	Значно нижчий пріоритет
≤ 0-1	Дуже низький ризик	Дуже низький пріоритет

Джерело: складено автором

Отже, можна створити матрицю ризиків або графік, який відображатиме співвідношення між оцінкою ймовірності та оцінкою наслідків відповідної ризикової події (табл.2.4).

Таблиця 2.4.

Матриця рівня ризику ВК/ФТ

Дуже високий							Дуже високий
Значно вищий						Значно вищий	
Вищий					Вищий Ризик		
Середній				Середній			
Нижчий			Нижчий				
Значно нижчий		Значно нижчий					
Дуже низький	Дуже низький						
Рівень вразли-вості / Рівень наслідків	Дуже низький	Значно нижчий	Нижчий	Середній	Високий	Значно вищий	Дуже високий

Джерело: складено автором

Важливо враховувати, що наслідки можуть істотно відрізнятися залежно від того, чи розглядається національний або міжнародний контекст. Підхід до НОР, запропонований у Методології МВФ, дає змогу оцінювати окремі наслідки як в абсолютних величинах, так і відносно валового внутрішнього продукту країни.

Повний процес НОР за Методологією МВФ містить сім етапів і залежить від здатності органів влади збирати й надавати статистичні дані, здійснювати якісні експертні оцінки й використовувати інструменти збору даних із відкритих джерел в інтернеті. Процес є циклічним і базується на зворотному зв'язку від учасників робочих груп. Основні етапи та їхні завдання:

1) Попередній етап і аналіз загроз: узгоджуються цілі дослідження, створюється координаційний механізм НОР, досліджується середовище та індикатори загроз у сфері ПВК/ФТ, представниками органів влади заповнюються чотири опитувальники.

2) Загроза ВК/ФТ: фахівці МВФ проводять засідання з органами влади, погоджуючи оцінки національних і міжнародних загроз ВК/ФТ, зокрема щодо обсягів та характеру злочинних доходів.

3) Підготовка до оцінки вразливості: органи влади готують шаблони для збору даних, МВФ збирає загальнодоступну інформацію для аналізу ймовірності, включно із секторальним рівнем.

4) Оцінка вразливості ВК/ФТ та ймовірності: засідання з органами влади для узгодження вразливості та ймовірності подій ризику ВК/ФТ, а також секторальних ризиків.

5) Наслідки та підготовка загальної оцінки ризику: органи влади заповнюють опитувальники щодо наслідків ВК/ФТ, МВФ збирає дані та створює попередні теплові карти ризиків.

6) Аналіз наслідків та ризику ВК/ФТ: проводяться засідання з органами влади для погодження остаточних результатів, уточнюються теплові карти ризиків та визначаються пріоритети пом'якшення ризиків.

7) Завершальний етап: МВФ надає попередню оцінку ризику, яку органи влади переглядають і затверджують для публікації.

Методологія НОР надає стандартизовані висновки, включно з таблицями національних злочинних доходів, матрицею ризиків, тепловими картами ризикових подій і секторів, а також документ із детальним описом ризиків та рекомендацій для їх вирішення.

Група Світового банку теж розробила аналітичний інструмент для оцінки ризику, щоб допомогти країнам проводити національні оцінки ризику ВК/ФТ [133]. Цей інструмент, створений командою з цілісності фінансових ринків у 2007 р., ґрунтується на досвіді експертів і наданні допомоги в оцінці ризиків у багатьох країнах. Він містить кілька взаємопов'язаних модулів на табличній базі Microsoft Excel, які дають країнам можливість оцінювати загрози та вразливості у сфері ВК/ФТ. Під «загрозами» розуміють масштаби та характеристики доходів від злочинної діяльності чи фінансування тероризму. «Вразливості» означають слабкі місця або прогалини в захисті юрисдикції від ВК та ФТ. Ці фактори можуть мати як національний, так і секторальний рівень і разом формують загальний рівень ризику для країни.

Інструмент складається з дев’яти модулів, що допомагають оцінювати ризики ВК та ФТ. Основна увага приділяється семи модулям, які фокусуються на оцінці ризиків ВК. Крім того, інструмент включає один модуль для оцінки ризиків ФТ і один — для оцінки ризиків, пов'язаних із продуктами фінансових установ. Модуль національної вразливості (Модуль 2) та модулі для оцінки секторальної вразливості (Модулі 3–7) мають унікальну й доволі складну структуру, що використовує середньозважені значення, вбудовані припущення та формули. Проте модулі для оцінки ризиків ВК, ФТ та продуктів фінансових установ побудовані на відносно простих матричних схемах.

Для проведення НОР країна створює національну Робочу групу (РГ), яка проводить оцінку ризиків. Ця група поділяється на кілька команд, кожна з яких

працює над окремим модулем. У табл. 2.5 подано три основні частини інструменту та перелік модулів у кожній з них.

Сім модулів, що використовуються для оцінки національного ризику ВК, тісно пов’язані між собою. Визначення загального національного ризику ВК ґрунтується на оцінці двох ключових аспектів: (1) національної загрози ВК та (2) національної вразливості до ВК. Модуль оцінки загрози визначає «рівень загрози» ВК у межах від «низького» до «високого» за п’ятибальною шкалою. У рамках цього модуля РГ аналізує основні предикатні злочини, джерела та потоки злочинних доходів, а також методи та тенденції відмивання коштів у юрисдикції. Він також сприяє збору даних про транскордонні загрози ВК (див. табл. 2.5).

8) Попередній етап і аналіз загроз: узгоджуються цілі дослідження, створюється координаційний механізм НОР, досліджується середовище та індикатори загроз у сфері ПВК/ФТ, представниками органів влади заповнюються чотири опитувальники.

9) Загроза ВК/ФТ: фахівці МВФ проводять засідання з органами влади, погоджуючи оцінки національних і міжнародних загроз ВК/ФТ, зокрема щодо обсягів та характеру злочинних доходів.

10) Підготовка до оцінки вразливості: органи влади готують шаблони для збору даних, МВФ збирає загальнодоступну інформацію для аналізу ймовірності, включно із секторальним рівнем.

11) Оцінка вразливості ВК/ФТ та ймовірності: засідання з органами влади для узгодження вразливості та ймовірності подій ризику ВК/ФТ, а також секторальних ризиків.

12) Наслідки та підготовка загальної оцінки ризику: органи влади заповнюють опитувальники щодо наслідків ВК/ФТ, МВФ збирає дані та створює попередні теплові карти ризиків.

13) Аналіз наслідків та ризику ВК/ФТ: проводяться засідання з органами влади для погодження остаточних результатів, уточнюються теплові карти ризиків та визначаються пріоритети пом'якшення ризиків.

14) Завершальний етап: МВФ надає попередню оцінку ризику, яку органи влади переглядають і затверджують для публікації.

Методологія НОР надає стандартизовані висновки, включно з таблицями національних злочинних доходів, матрицею ризиків, тепловими картами ризикових подій і секторів, а також документ із детальним описом ризиків та рекомендацій для їх вирішення.

Група Світового банку теж розробила аналітичний інструмент для оцінки ризику, щоб допомогти країнам проводити національні оцінки ризику ВК/ФТ [180]. Цей інструмент, створений командою з цілісності фінансових ринків у 2007 р., ґрунтується на досвіді експертів і наданні допомоги в оцінці ризиків у багатьох країнах. Він містить кілька взаємопов'язаних модулів на табличній базі Microsoft Excel, які дають країнам можливість оцінювати загрози та вразливості у сфері ВК/ФТ. Під «загрозами» розуміють масштаби та характеристики доходів від злочинної діяльності чи фінансування тероризму. «Вразливості» означають слабкі місця або прогалини в захисті юрисдикції від ВК та ФТ. Ці фактори можуть мати як національний, так і секторальний рівень і разом формують загальний рівень ризику для країни.

Інструмент складається з дев’яти модулів, що допомагають оцінювати ризики ВК та ФТ. Основна увага приділяється семи модулям, які фокусуються на оцінці ризиків ВК. Крім того, інструмент включає один модуль для оцінки ризиків ФТ і один — для оцінки ризиків, пов'язаних із продуктами фінансових установ. Модуль національної вразливості (Модуль 2) та модулі для оцінки секторальної вразливості (Модулі 3–7) мають унікальну й доволі складну структуру, що використовує середньозважені значення, вбудовані припущення та формули. Проте модулі для оцінки ризиків ВК, ФТ та продуктів фінансових установ побудовані на відносно простих матричних схемах.

Для проведення НОР країна створює національну Робочу групу (РГ), яка проводить оцінку ризиків. Ця група поділяється на кілька команд, кожна з яких

працює над окремим модулем. У табл. 2.5 подано три основні частини інструменту та перелік модулів у кожній з них.

Сім модулів, що використовуються для оцінки національного ризику ВК, тісно пов'язані між собою. Визначення загального національного ризику ВК ґрунтується на оцінці двох ключових аспектів: (1) національної загрози ВК та (2) національної вразливості до ВК. Модуль оцінки загрози визначає «рівень загрози» ВК у межах від «низького» до «високого» за п'ятибальною шкалою. У рамках цього модуля РГ аналізує основні предикатні злочини, джерела та потоки злочинних доходів, а також методи та тенденції відмивання коштів у юрисдикції. Він також сприяє збору даних про транскордонні загрози ВК (див. табл. 2.5).

Таблиця 2.5.

Основні частини інструменту НОР

Оцінка ризику ВК	Оцінка ризику ФТ	Оцінка ризику фінансових продуктів
Модуль 1 - Оцінка загрози Модуль 2 - Національна вразливість Модуль 3 - Вразливість банківського сектору Модуль 4 - Вразливість сектору цінних паперів Модуль 5 - Вразливість сектору страхування Модуль 6 - Вразливість інших фін. установ Модуль 7 - Вразливість секторів ВНУП	Модуль 8 – Національні загроза та вразливість ФТ	Модуль 9 – Оцінка ризику фінансових продуктів

Джерело: складено автором

Вищий рівень загрози ВК свідчить про більший національний ризик. Оцінка національної вразливості водночас базується на здатності країни протидіяти ВК та вразливості різних секторів. Поєднуючи ці фактори з оцінкою слабких місць у системі запобігання ВК, модуль національної вразливості надає «оцінку вразливості» на шкалі від 0.0 до 1.0, яка відповідає одному з п'яти рівнів, від «низького» до «високого».

Загальний рівень ризику ВК визначається на перетині результатів оцінки загрози та вразливості. Наприклад, якщо загроза оцінена як «середня», а вразливість як «вища за середню», то ризик відмивання коштів буде «вище

середнього». Це означає, що, попри середній рівень загрози, загальний ризик ВК підвищується через вищу вразливість країни. На рис. 2.2 загальні рівні ризику зображені різними кольорами: найнижчі — зеленим, середні — жовтим, а високі — червоним.

ЗАГАЛЬНА ЗАГРОЗА	ЗАГАЛЬНИЙ РИЗИК ВК У ЮРИСДИКЦІЇ				
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H
	ЗАГАЛЬНА ВРАЗЛИВІСТЬ				

Довідково: L = low (низький); ML = medium-low (нище середнього); MH = medium-high (вище середнього); H = high (високий).

Рисунок 2.2. Загальний ризик ВК у юрисдикції

Джерело: побудовано автором за матеріалами [180]

Робоча група експертів Світового банку проводить оцінку вхідних змінних, використовуючи керівні інструкції, що надаються в складі пакету Інструменту НОР. Для кожного модуля передбачено окремий документ з інструкціями. Ці інструкції пояснюють мету оцінки кожної змінної, надають критерії для оцінювання та пропонують джерела інформації, які можуть допомогти обґрунтувати оцінку. Після аналізу критеріїв експерти повинні виставити оцінку в діапазоні від 0.0 до 1.0. Так, оцінка 0.3 відповідає низькому рівню. У табл. 1.8 наведено приклад керівної інструкції для оцінки ефективності внутрішньої співпраці в Модулі 2 — національна вразливість.

Після завершення оцінки кожної з 22 вхідних змінних і присвоєння їм відповідного рейтингу результати можна зазначити у файлі-таблиці Інструменту НОР. Кожен модуль має власну таблицю. Після введення рейтингів система

автоматично присвоїть кожному запису відповідний колір, щоб відобразити, як рейтинг впливає на національну вразливість до відмивання коштів. Високі оцінки, що відображають здатність до боротьби з ВК, позитивно впливають на вразливість і позначаються зеленим кольором (див. табл. 2.6).

Таблиця 2.6

Приклад керівної інструкції для оцінки ефективності внутрішньої співпраці учасників національної системи ПВК/ФТ

Оцінка										
Базуючись на критеріях оцінки та зібраній інформації/даних, було встановлено наступну оцінку для цієї змінної.										
Відмінна	Майже відмінна	Дуже висока	Висока	Вища середньої	Середня	Нища середньої	Низька	Дуже низька	Майже відсутня	Не існує
1.0	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0.0

Джерело: складено за матеріалами [180]

Оцінки вразливості для різних секторів (банківського, страхового, цінних паперів, криптоактивів, адвокатської діяльності) теж мають бути внесені до файлу-таблиці модуля національної вразливості. Варто зазначити, що чим вищий рівень вразливості сектору, тим негативніше це впливатиме на загальний результат національної вразливості. Експерти також призначають певний рівень значущості для кожного сектору, враховуючи його важливість для економіки країни, що додатково впливає на оцінку його вразливості.

Після введення рейтингів для всіх вхідних змінних інструмент автоматично розраховує рейтинги для проміжних змінних, таких як якість політики та стратегій у сфері протидії відмиванню коштів (ПВК), якість кримінальних розслідувань та кримінального переслідування, базуючись на оцінках вхідних змінних, мережевій структурі, зважених середніх і визначених умовах. Далі проводяться подібні розрахунки для визначення рівня національної спроможності до боротьби з ВК. Потім цей показник поєднується з результатами оцінки вразливості секторів для визначення загального рівня національної вразливості.

Інструмент НОР визначає пріоритети надання допомоги відповідним органам влади у встановленні першочергових заходів для зміцнення національних спроможностей у боротьбі з ВК і контролі у сфері ПВК/ФТ, що дає змогу цим органам вирішити, які кроки потрібно зробити насамперед для підвищення ефективності. Пріоритети не обов'язково відповідають оцінкам змінних, отриманим під час аналізу. Наприклад, змінна з кращим рейтингом може мати вищий пріоритет і потребувати більшої уваги. Це пов'язано з тим, що рейтинг, хоч і важливий, не є єдиним чинником, який визначає рівень національної вразливості й пріоритети. Інші фактори, такі як мережеві структури, що охоплюють первинні та похідні змінні, теж впливають на остаточний рівень вразливості й рейтинг пріоритетів. Робоча група експертів може враховувати ці чинники.

Модуль оцінки ризику фінансування тероризму (ФТ) використовує підхід, подібний до модулів оцінки ризику ВК, поєднуючи інтуїтивний і методичний аналіз. Він охоплює три основні аспекти:

1) оцінка рівня терористичної загрози для юрисдикції на основі кількісних і якісних даних, таких як інформація від правоохоронних органів, розвідувальних джерел і досліджень тероризму. Це важливо, оскільки рівень загрози тероризму впливає на ризик його фінансування, хоча цей аспект не є головним у модулі;

2) аналіз джерел фінансування тероризму, шляхів переміщення коштів і каналів їх постачання;

3) оцінка ефективності захисних механізмів юрисдикції для виявлення та протидії ФТ.

На основі цього аналізу експерти мають здійснити загальну оцінку ризику ФТ у юрисдикції, що проходить оцінку.

Модуль оцінки ризику продуктів фінансових установ призначений для того, щоб допомогти національним органам влади оцінювати ризики ВК та ФТ, пов'язані з продуктами фінансових установ, як наявними, так і новими чи такими,

що з'являються. Цей модуль теж може бути використаний регуляторами для розроблення фінансових продуктів або послуг із низьким ризиком ВК/ФТ чи для оцінки поточних продуктів щодо їхнього рівня ризику. Загальну структуру модуля показано на рис. 2.3.

Перший розділ модуля містить запитання для регуляторів, що стосуються особливостей фінансових продуктів. У другому розділі оцінюються загальні ризики ВК та ФТ у країні, зважаючи на можливі загрози і застосовувані заходи контролю за фінансовими продуктами. На основі відповідей на ці два блоки запитань третій розділ визначає початковий рівень ризику ВК/ФТ для кожної функції продукту. Далі інструмент пропонує додаткові запитання, що допомагають визначити, як можна зменшити будь-які виявлені високі ризики.

Процес оцінки ризику фінансових продуктів є не фіксованим, а скоріше динамічним. Він допомагає регулювати характеристики продукту та заходи з мінімізації ризиків залежно від результатів оцінки (див. рис. 2.3).

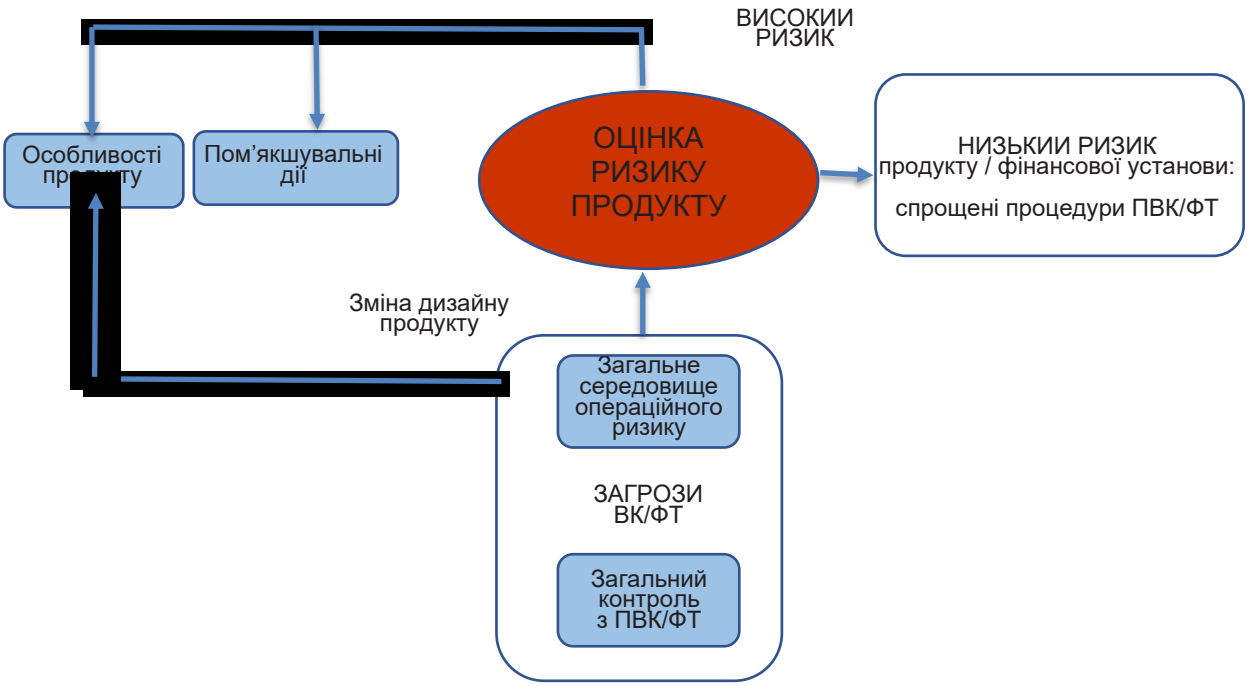


Рисунок 2.3. Модуль оцінки ризику продуктів фінансових установ

Джерело: складено автором за матеріалами [180]

Структура цього модуля відрізняється від інших модулів інструменту НОР. Тут оцінка спирається на висновки та результати інших модулів, а не постачає дані для НОР. Окрім того, фінансові продукти оцінюються окремо в секторальних модулях, щоб відобразити їхній вплив на загальну національну вразливість.

FATF рекомендує враховувати потенціал і досвід кожного сектору у сфері ПВК/ФТ під час НОР. Ризики ВК і ФТ повинні бути ідентифіковані, оцінені та зрозумілі, а також слід розробити заходи для їх попередження відповідно до виявлених загроз.

Відповідно до європейської методології оцінки ризиків [181], ризик ВК/ФТ у секторі, що аналізується, підпадає під наднаціональну оцінку, якщо компонент «загроза» відповідає компоненту «вразливість». Такий ризик впливає на внутрішній ринок ЄС, незалежно від кількості залучених країн-членів (навіть якщо йдеться лише про одну країну). Оцінка охоплює як відомі ризики, так і ті, що раніше не проявлялися.

Виходячи з цього, Директива (ЄС) 2015/849 «Про запобігання використанню фінансової системи для відмивання грошей та фінансування тероризму» визнає важливість наднаціонального підходу до ідентифікації ризиків. Вона покладає на Європейську комісію обов’язок оцінювати специфічні ризики, які можуть виникнути на європейському рівні й вплинути на внутрішній ринок (так звані наднаціональні ризики), і доручає їй проводити наднаціональну оцінку ризиків з ВК і ФТ (SNRA) [181]. Окрім наднаціонального рівня, кожна країна-член проводить національну оцінку ризиків для виявлення та зниження національних загроз. На третьому рівні оцінку ризиків здійснюють самі сектори, беручи до уваги фактори ризику, пов’язані з клієнтами, країнами, продуктами, послугами, операціями та каналами постачання.

Ці три рівні оцінки ризиків — наднаціональний, національний та секторальний — взаємодоповнюють один одного і мають однакову важливість у забезпеченні комплексного розуміння ризиків ВК/ФТ у ЄС.

Національні та секторальні оцінки ризиків можуть стати важливими елементами SNRA, але сама наднаціональна оцінка не є простою сукупністю цих оцінок. Проведення SNRA розглядається як окреме завдання, необхідне для виконання мандата, встановленого Директивою (ЄС) 2015/849 [181], оскільки Європейська комісія повинна надати рекомендації країнам-членам щодо заходів для боротьби з ризиками ВК/ФТ у Європі. Країни-члени теж мають брати до уваги висновки звіту SNRA під час проведення своїх НОР.

Пропонована методологія базується на таких послідовних діях:

1) Ідентифікація механізмів ВК та ФТ: визначаються механізми, які можуть становити ризики на рівні ЄС, незалежно від того, чи виникають вони в одній або кількох країнах-членах. Ці механізми повинні впливати на весь внутрішній ринок ЄС.

2) Оцінка рівня загроз: використовується чіткий підхід до оцінки загроз у різних секторах та сценаріях, що згадуються в статтях 2 та 4 Директиви (ЄС) 2015/849 [181]. Оцінка зосереджується на намірах і можливостях злочинців використовувати діючі або нові механізми для ВК та ФТ. Вона ґрунтується на думках експертів із країн-членів та інших зацікавлених сторін, а також на доступних розвідувальних даних (як якісних, так і кількісних) та затвердженому підході до оцінки загроз. Оціночна комісія затверджує результати обговорень SNRA, оцінює стратегічний рівень загрози таким чином:

- низький (1-й рівень);
- помірний (2-й рівень);
- істотний (3-й рівень);
- дуже істотний (4-й рівень).

3) Оцінка рівня вразливості: стосується механізмів ВК/ФТ у секторах. Вона зосереджується на заходах безпеки. Основою для оцінки є думки експертів країн-членів та інших зацікавлених сторін, які базуються на доступних розвідувальних даних (якісних і кількісних) та затвердженому підході до оцінки

вразливості. Оціночна комісія затверджує результати обговорень SNRA, оцінює стратегічний рівень вразливості за тими самими категоріями, що й загрози.

4) Визначення залишкового ризику: визначається як комбінація оцінених загроз і вразливостей для кожного механізму ВК/ФТ. Оцінка здійснюється з урахуванням ризик-орієнтованого секторального підходу. Для кожного сектору сукупність механізмів ВК/ФТ оцінюється за ризиком, що базується на визначеному рівні загроз та вразливостей.

У ході першого раунду SNRA компонент «вплив/наслідки» вважався постійно істотним, тому він не оцінювався окремо.

Таким чином, запропонована методологія враховує лише компоненти загроз і вразливостей. Попри те, що важливо розуміти наслідки діяльності ВК/ФТ, їх кількісне вимірювання є дуже складним. Тому в контексті оцінки ризиків вважається, що діяльність ВК/ФТ завдає постійної істотної шкоди прозорості, управлінню та підзвітності державних і приватних установ ЄС, а також негативно впливає на національну безпеку країн ЄС та економіку ЄС загалом. З методологічної точки зору, оскільки вплив/наслідки вважаються постійно негативно високими, для визначення залишкового ризику кожного сценарію буде використано комбінацію виявлених рівнів загроз і вразливостей. Процес можна узагальнити такими етапами (рис. 2.4.).

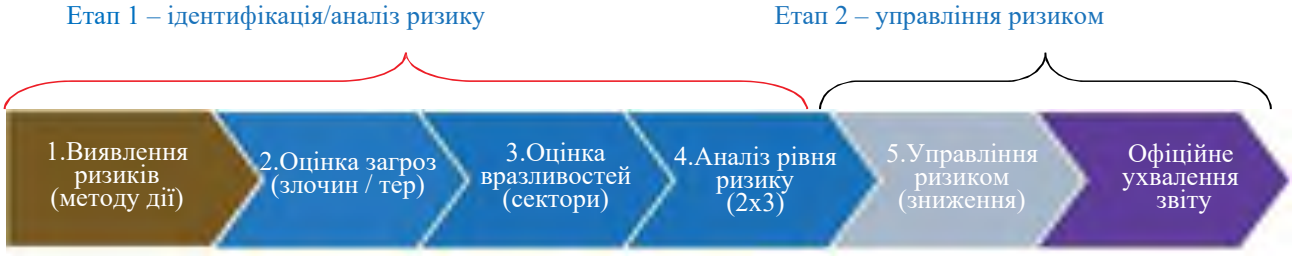


Рисунок 2.4. Послідовність етапів SNRA

Джерело: Складено автором за матеріалами [177]

Перший крок полягає у виявленні конкретних ризиків ВК/ФТ, які буде оцінено на наступних етапах процесу. У контексті SNRA, згідно з Директивою (ЄС) 2015/849, ідентифікація ризиків має на меті визначити відомі та потенційні

загрози ВК/ФТ, а також відповідні сектори, що використовуються злочинцями для вчинення своїх дій. Ризики ВК та ФТ можуть різнитися залежно від ситуації, тому слід застосовувати комплексний ризик-орієнтований підхід. Хоча процес ідентифікації буде здебільшого спиратися на відомі загрози, важливо також враховувати нові загрози, пов'язані з інноваціями, для яких може не бути належного захисту. На цьому етапі мета полягає у виявленні природи ризикових сценаріїв та визначенні тих, які є найактуальнішими, без оцінки їхнього рівня.

Другий крок передбачає оцінку рівня загрози (низький (1), помірний (2), істотний (3), дуже істотний (4)) для кожного сценарію, визначеного на першому етапі. Оцінка ґрунтується на комбінованій оцінці намірів та можливостей злочинців у здійсненні незаконних операцій. Результати оцінки рівня загрози для кожного ризику утворюють загальний рівень оцінки загрози для ЄС. Тому пропонується оцінити стратегічний рівень загрози для кожного ризику згідно з методом узгодження оцінки загрози, затвердженим Єврокомісією. Компонент «наміри» загрози базується на відомих успішних або зірваних намірах та привабливості певних механізмів для ВК/ФТ. Тоді як загальні наміри ВК/ФТ оцінюються як постійно високі, використання конкретних методів дії (механізмів) може змінюватися залежно від їхньої привабливості та наявності заходів безпеки. Компонент «можливості» загрози стосується здатності злочинців успішно обмінювати або переказувати злочинні доходи в рамках ВК та ФТ. Оцінка цього компонента буде враховувати легкість застосування конкретних методів (технічні вимоги та підтримка), доступність і витрати на їх використання.

Третій крок полягає в оцінці рівня вразливості (низький (1–1,5), помірний (1,6–2,5), істотний (2,6–3,5), дуже істотний (3,5–4)) для кожного сценарію, виявленого на першому етапі. Оцінка вразливості зосереджується на наявності й ефективності запобіжних заходів: чим більше ефективних заходів, тим нижчі вразливість і ризик. Оцінка вразливості буде проводитися для сфер, пов'язаних із механізмами ВК/ФТ, що були визначені на першому кроці, які потребують

застосування законодавства з ПВК/ФТ. У рамках SNRA оцінка вразливості теж повинна враховувати національне та міжнародне законодавство, а також законодавство ЄС і ефективність його імплементації на національному рівні. Оскільки SNRA охоплює широкий спектр ризиків ВК/ФТ, важливо звернути увагу на інші критерії, такі як ефективність обміну інформацією між фінансовими розвідками, координація з іншими органами влади з ПВК та міжнародна співпраця, включно зі співпрацею між наглядовими органами (рис. 2.5).

ЗАГРОЗА					
	Дуже істотна	2,2	2,8	3,4	4
	Істотна	1,8	2,4	3	3,6
	Помірна	1,4	2	2,6	3,2
	Низька	1	1,6	2,2	2,8
		Низька	Помірна	Істотна	Дуже істотна
	ВРАЗЛИВІСТЬ				

Рисунок 2.5. Оцінка вразливості системи до ВК/ФТ

Джерело: складено автором

Оцінка вразливості системи до ВК/ФТ у цілому ґрунтуватиметься на даних, зібраних і проаналізованих відповідними наглядовими органами, фінансовими розвідками та національними органами влади. Результати кроків 2A/B (оцінка загрози ВК/ФТ) та 3A/B (оцінка вразливості ВК/ФТ) визначать рівень ризику для кожного виявленого ризику (крок 1A/B) через матричний підхід, що поєднує оцінки загрози та вразливості.

Матриця ризику визначає його рівень, виходячи з вагових коефіцієнтів 40% (загроза) / 60% (вразливість), враховуючи, що вразливість має більшу вагу у визначенні рівня ризику. Передбачається, що рівень вразливості може підвищити привабливість певних методів дії, що, у свою чергу, вплине на рівень загрози.

Комісія експертів з оцінки проводить консультації з приватним сектором і громадськістю протягом процесу НОР. Для цього вона організовує спеціальні семінари з чотирма основними групами зацікавлених сторін у приватному секторі: фінансовими установами, юристами, іншими підзвітними суб'єктами та недержавними організаціями. Ці семінари проводяться на основі вже виявлених ризиків і зібраних відгуків щодо них, обговоренні результатів оцінки ризиків та можливих заходів для їх пом'якшення. На підставі доступної інформації та розвідувальних даних Комісія ініціювала подальші раунди оцінки ризиків для перегляду ситуації із загрозами, що виникають або розвиваються.

Наслідки відмивання коштів можуть проявлятися в короткострокових викривленнях попиту на різні продукти, послуги та активи як у реальному, так і у фінансовому секторах економіки. Використання успішно відмитих активів має значно більш широкий і довгостроковий негативний вплив на соціальну, економічну та політичну сфери, що торкається громадян, бізнесу, національних і міжнародних інтересів, включно зі сприянням подальшій злочинній діяльності та збільшенням обсягів доходів, які відмиваються. На сьогодні внаслідок аналізу спеціальної літератури та світової практики широкий спектр наслідків ВК класифіковано на 24 категорії [182].

Всі 24 наслідки ВК не завжди миттєво (короткостроково) впливають і можуть проявлятися з певним часовим лагом (у довгостроковій перспективі). Тому доцільно зосередитися на поступовому і детальному аналізі коротко- та довгострокових наслідків відмивання коштів для економіки, суспільства та політичної сфери. Що стосується наслідків фінансування тероризму, то вони варіюються залежно від юрисдикцій і найбільшу негативно впливають у країнах, що піддаються терористичним атакам.

В контексті економічних наслідків ВК негативно впливає на реальний сектор (виробництво та споживання), ділову активність, відносні ціни, заощадження, продуктивність, зайнятість і економічне зростання. Фінансовий сектор також зазнає негативного впливу, що стосується ліквідності, репутації,

цілісності та стабільності. Державний сектор відчуває наслідки ВК через недоотримані податки, а також через загрози, пов'язані з нелегальними приватизаційними процесами. Монетарний сектор може постраждати від значних і неконтрольованих потоків капіталу, а також від підвищення волатильності процентних ставок і валютних курсів.

Управління ризиками та їх зменшення здебільшого включають комплексне поєднання рішень і процесів для охоплення різних бізнес-активностей та профілів ризику. Існує багато інструментів для боротьби з ВК, найкращі з яких автоматизують оцінку ризиків для нових клієнтів і нових трансакцій у режимі реального часу.

Основні технології протидії відмиванню грошей поділяються на дві ключові категорії: ідентифікація та верифікація клієнтів; моніторинг діяльності.

Важливу роль у розробленні цих технологій і загальної системи боротьби з відмиванням коштів, отриманих злочинним шляхом, відіграв Базельський комітет з банківського нагляду. На основі його заяви про принципи, спрямованої на боротьбу з незаконним використанням банківських систем для легалізації доходів, отриманих злочинним шляхом, визначено такі принципи діяльності банківських установ:

- ідентифікація клієнтів;
- дотримання законодавства;
- підтримка високих етичних стандартів, відповідність місцевим законам і нормам;
- активна співпраця з правоохоронними органами в межах конфіденційності клієнтів;
- навчання персоналу;
- ведення обліку та проведення аудиту.

Ці принципи, що передували законодавчим актам щодо боротьби з відмиванням коштів, сприяли наданню правоохоронним органам інформації про

клієнтів і забезпечили банкам правовий захист у випадках порушення конфіденційності клієнтів [183].

Документ Базельського комітету «Основні принципи ефективного банківського нагляду» (далі – Основні принципи) став ключовим керівництвом для діяльності регуляторних органів у всьому світі. У керівництві зазначалося, що наглядові органи повинні забезпечити впровадження банками відповідних політик, практик і процедур, включно з жорстким правилом «Знай свого клієнта» (ЗСК; англ. know your customer, KYC), щоб підтримувати високі етичні й професійні стандарти у фінансовому секторі та запобігати використанню банків злочинними елементами. Також комітет закликав країни прийняти та імплементувати 40 рекомендацій FATF.

Базельський комітет зосередив увагу на політиці ЗСК, яка передбачає ретельну перевірку клієнтів з метою зменшення ризиків прийняття небажаних клієнтів. Якщо банк не проводить належну перевірку, він ризикує втратити репутацію, а також наражається на операційні, юридичні та концентраційні ризики, що може спричинити серйозні фінансові збитки. Надійна політика та процедури ЗСК з чотирма основними її елементами – ідентифікація клієнтів, управління ризиками, відбір клієнтів і моніторинг – є ключовими для збереження безпеки банків і стабільності банківських систем.

Аналіз наукової літератури свідчить, що поява технології блокчейн і швидкий розвиток криптоактивів стали значним викликом для науковців і практиків. Висока волатильність доходів криптоактивів і поширеність кібератак, спрямованих на цю технологію є одними із основних ризиків крипторинку, на яких зосереджена увага дослідників. Серед існуючої дослідницької літератури є низка досліджень, присвячених ризикам крипто-ринку та напрямам вирішення технологічних вразливостей (Бонно та ін., 2015 [184]; Стюарт та ін., 2018 [185]; Ма та ін., 2018 [186]; Гофар, 2019 [187]; Чень та ін., 2020 [188]; Дрлевіч та ін., 2019 [189]; Патель, 2020 р. [190], Саад та ін., 2019 р. [191]; Нгуєн Пхук Кань та ін., 2019 [192]; Лем’є, 2016 [193]; Газалі та ін., 2018 [194]; Лу, 2019 [195]).

Зауважимо, що переважна увага дослідників ризиків крипторинку зосереджує увагу на моделюванні ціноутворення. Дослідники доводять, що криптоактиви демонструють відсутність кореляції з традиційними активами, а також незалежність від глобальних макроекономічних факторів (Дірберг, 2016 р. [196]; Бурі та ін., 2017 [197]; Дас і Каннадхасан, 2018 [198]). Деякі дослідники виявили, що фактори волатильності, ліквідності є важливими для прогнозування дохідності криптовалют (Ван та ін., 2021 [199]). Фактори ризику операцій з криптовалютами, які можуть бути передбачені, розглядає низка дослідників (Кутмос, 2018 [200]; Б'є та ін., 2019 [201], 2020 [202]; Сокін і Сюн, 2020 [203]; Лю, 2019 [204]; Конг та ін., 2020 р. [205]; Момтаз, 2019 [206]; Рутледж і Зетлін-Джонс, 2022 [207]; Паньотта, 2022 р. [208]; Лю та ін., 2022 [209]).

Незважаючи на значну кількість робіт, спрямованих на моделювання цін і ризиків криптовалют, дослідження, присвячені ризик-орієнтованому підходу до регулювання ринку цифрових активів, залишаються обмеженими. Наше дослідження є одним із перших у цьому напрямі.

Ризик-орієнтований підхід до регулювання ринку цифрових активів передбачає акцент на оцінці та управлінні ризиками, замість застосування застарілих методів контролю або заборон. Основна мета — забезпечити інноваційний розвиток, створивши безпечне та надійне середовище для учасників ринку. Це передбачає ідентифікацію ризиків, пов'язаних із використанням цифрових активів, таких як криптовалюти та токени, і ефективне управління ними.

Ключовим елементом цього підходу є вивчення технічних, правових та регуляторних ризиків, а також створення стандартів безпеки і моніторингу ринку. Це дозволить розвивати інновації у сфері цифрових активів, одночасно забезпечуючи їхню стабільність.

Підсумовуючи, авторське визначення сутності ризик-орієнтованого підходу до регулювання обігу цифрових активів в сфері ПВК/ФТ полягає в забезпеченні систематичного здійснення оцінки ризиків використання цифрових

активів у легалізаційних операціях та операціях маніпулювання віртуальними активами уповноваженими державними органами й учасниками обігу цифрових активів і особами, які обслуговують операції з цифровими активами, а також застосування широкої сукупності методів фінансового контролю за обігом цифрових активів з метою виявлення операцій щодо легалізації (відмивання) доходів, ухилення від сплати податків, корупційної діяльності, фінансування тероризму, обходження санкцій, шахрайства для забезпечення фінансової цілісності та резильєнтності економічної системи.

Таким чином, ризик-орієнтований підхід сприяє створенню стабільного і довірчого середовища на ринку цифрових активів, збалансовуючи інновації та безпеку.

В умовах зростання цифрової економіки рішення для цифрової верифікації та підтвердження особи постійно вдосконалюються. Ці технології можуть визначити, чи є особа справжньою, і чи людина, яка її представляє, є законним власником. Вони також можуть оцінювати ризики або репутацію цієї особи на основі попередньої діяльності та продовжувати моніторинг ризиків, допомагаючи бізнесу краще знати своїх клієнтів.

Процес моніторингу трансакцій клієнта, таких як перекази, депозити та виведення (зняття) коштів, називається моніторингом трансакцій. Рішення для моніторингу трансакцій розроблені для зменшення ризику відмивання грошей, контролюючи цифрові трансакції у всіх бізнес-каналах для виявлення підозрілої поведінки, що може вказувати на відмивання грошей, та запобігання цьому до того, як це відбудеться.

Все частіше блокчейн-технології використовують для моніторингу трансакцій не тільки з криптоактивами, а й у фінансових операціях з фіатними грошима. Фіатні гроші (фіат) — це узаконений платіжний засіб, цінність якого встановлюється урядом. Але і цифрові валюти центральних банків можуть бути емітовані на блокчейн-платформі. Наприклад, е-гривня Національного банку України розроблена на блокчейн-платформі Stellar.

Завдяки децентралізованій природі блокчейну, запуск нових продуктів і мереж стає простішим. Блокчейн дозволяє створювати чіткі та стандартизовані правила для трансакцій, які легко відстежувати та виконувати без посередників. Інформація про кожну трансакцію назавжди зберігається в блокчейні і не може бути змінена, що забезпечує прозорість та відповідність регуляторним вимогам, зокрема в рамках політики ПВК/ФТ.

Починаючи з 2019 року, згідно з оновленою 15 Рекомендацією FATF [223], держави почали розробляти та впроваджувати державну регуляцію ринку віртуальних активів, зокрема ліцензування та реєстрацію професійних операторів, які проводять операції з віртуальними активами.

40 Рекомендацій FATF [178] взаємопов'язані, і тому всі вимоги політики ПВК/ФТ для фінансових установ повинні застосовуватися також до операторів крипторинку. Зокрема, за 1 Рекомендацією FATF, необхідно впроваджувати ризик-орієнтований підхід у діяльність ринку віртуальних активів.

Розвитку систем оцінки та управління ризиками, пов'язаними з ВК/ФТ, присвячені дослідження таких науковців, як Ж. О. Андрійченко [210], С. О. Дмитров, О. В. Меренкова, Т. А. Медвідь, О. М. Ващенко [211], Т. І. Єфименко, С. С. Гасанов, О. Є. Користін [212], Я. Х. Занг (Y.-H. Zhang), Я. В. Ксу (Y.-W. Xue) [213], В. М. Каднічанська, Т. О. Ромась [214], Л. Л. Лазебник [215], М. І. Худокормова [216], О. В. Черевко [217] та інші.

Ж. О. Андрійченко [210] досліджувала роль ПВК/ФТ у системі управління ризиками на ринку фінансових послуг, застосовуючи системний підхід. У монографії [211] запропоновано методику експрес-оцінки внутрішньобанківських ризиків, пов'язаних із використанням банківських послуг для ВК/ФТ. Колектив авторів [211] розробив підхід до оцінювання ризиків у сфері ПВК/ФТ. Дослідження [212] присвячене оцінці рівнів ризиків клієнтів у контексті реалізації ризик-орієнтованого підходу. О. В. Черевко [217] обґрунтував критерії оцінки ризику використання банку для ВК, а також заходи щодо його зменшення. Л. Л. Лазебник [215] визначив напрями розвитку бізнес-

процесів банку з точки зору комплаєнс-ризиків. В. М. Каднічанська та Т. О. Ромась [214] розширили класифікацію ризиків у сфері ПВК/ФТ.

В сфері обороту віртуальних активів, де будь-яка діяльність криптоіндустрії та її взаємодія з фінансовими ринками протягом п’ятнадцяти років віднесена до високого ризику впровадження ризик-орієнтованого підходу до регулювання такого обороту стало негайним. В наукових працях Міщенка В.І., Науменкової С.В., Міщенко С.В. [218] обґрунтовано, що використання цифрових грошей центральних банків сприятиме трансформації механізмів реалізації бюджетної та податкової політики, системи ПВК/ФТ, дії каналів монетарного трансмісійного механізму, суттєвим змінам у структурі та функціях комерційних і центральних банків, а також посилить роль фінтехкомпаній у функціонуванні платіжних систем і фінансових та крипто ринків. Розвиваючи впровадження ризик-орієнтованого підходу в діяльності банківських і платіжних установ в умовах цифровізації економіки такі науковці, як Гулей А.І., Гулей С.А., Коваленко Ю.Л., Рябокінь М.В. [219,220 наголошують про необхідність систематизувати зарубіжний досвід управління ризиками та узагальнити основні зміни міжнародних стандартів FATF. Такий підхід сприяє ефективніше розподіляти ресурси, посилюючи контроль у сферах підвищеного ризику та застосовуючи спрощені процедури там, де ризики є мінімальними.

У наукових працях Долінського Л.Б. [221,222] розглянуто питання управління ефективністю та ризиками підприємницької діяльності в умовах цифрової трансформації економіки. Запропоновано економетричні методи оцінки ризиків, що можуть стати основою для розробки програм ПВК/ФТ для суб’єктів фінансового моніторингу з урахуванням їхнього застосування у відповідному програмному забезпеченні.

Крім того, проаналізовано теоретико-методологічні, концептуальні та практичні аспекти цифрової трансформації промислового менеджменту, визначено вплив Четвертої промислової революції на цифрову стратегію управління підприємствами та їхню адаптацію до концепції INDUSTRY 5.0.

Розкрито значення цифрових змін для управління людськими ресурсами, фінансами, ризиками, інноваційно-інвестиційною діяльністю, маркетингом, а також для запобігання рейдерським захопленням у системах управлінського обліку та контролю. Окрему увагу приділено використанню цифрових технологій як у бізнес-процесах, так і в злочинній діяльності.

Всі операції в блокчейн-мережах можна переглянути за допомогою блокчейн-експлорерів — інструментів, що надають детальну інформацію про трансакції, блоки та стан блокчейну. Однак, проводять оцінку ризику учасників і їхніх операцій з маркуванням рівня ризику подібно до теплової карти блокчейн-аналітичні програми.

Блокчейн-аналітика дає змогу відстежувати трансакції та виявляти незаконну діяльність, роблячи криптоактиви прозорішими порівняно з традиційними грошима. Вона допомагає криптовалютним бізнесам та фінансовим установам управляти ризиками і захищати свою репутацію та клієнтів від незаконних дій.

Завдяки аналітиці в блокчейні можна виявляти шахрайські операції, що дає змогу своєчасно реагувати на ризики. Крім того, компанії в криптовалютному секторі використовують ці технології для запобігання відмиванню грошей, що є важливою частиною дотримання міжнародних стандартів боротьби з фінансовими злочинами.

В основу розроблення блокчейн-аналітичних програм покладено методики ризик-орієнтованого підходу з алгоритмами оцінки ризику за зазначеними вище методологіями, наприклад, тепловими картами оцінки ризику учасників операції (рис. 2.6.)

Блокчейн-аналітичні компанії повинні збалансувати зменшення ризиків з досвідом клієнта під час впровадження технологій протидії відмиванню грошей, гнучко адаптуючи контроль залежно від рівня ризику, який представляє конкретний клієнт або трансакція для бізнесу. Швидкість та зручність мають таке ж значення, як і безпека, для послуг, що викликають довіру. Не кожен

процес клієнта потребує найвищого рівня безпеки, і надмірне ускладнення, що призводить до відмови клієнтів або припинення трансакцій, слід зменшувати.



Рисунок 2.6. Приклад встановлення рівнів ризику інструментів крипторинку на платформі блокчейн-аналітичної компанії Chanalysis

Джерело: складено автором за матеріалами [250]

Однак, вартість таких рішень для бізнесу є важливим фактором, але її потрібно порівняти з потенційними втратами від шахрайської діяльності, штрафами та репутаційними збитками. Тому для оптимізації витрат як у приватному бізнесі, так і в державному секторі все більше використовують програмні продукти по оцінці ризику, особливо ризику ВК/ФТ.

2.2. Кластерно-порівняльний аналіз ризиків використання цифрових активів в злочинній діяльності

Віртуальні активи та пов’язані з ними послуги мають потенціал для стимулювання фінансових інновацій та підвищення ефективності, однак їхні особливі риси теж створюють нові можливості для ВК/ФТ та інших злочинів. Здатність швидко проводити трансакції через кордони не тільки дає змогу злочинцям у цифровій формі отримувати, переміщувати та зберігати активи часто поза межами регульованої фінансової системи, а й приховувати джерело або призначення коштів, що ускладнює своєчасне виявлення підозрілих дій підзвітними установами. Ці фактори створюють додаткові труднощі для виявлення та розслідування злочинної діяльності національними правоохоронними органами влади.

Організовані злочинні групи (ОЗГ) можуть використовувати псевдонімний та децентралізований характер криптоактивів для ВК та вчинення інших злочинів. Злочинці здатні обходити офіційну банківську систему, застосовуючи криптоактиви для переказу великих сум грошей, що знижує ймовірність виявлення цього явища правоохоронними органами чи фінансовими установами, що зобов'язані звітувати про підозрілі трансакції.

Однак державні законодавчі та регуляторні органи влади можуть значно сприяти зменшенню ризиків незаконного використання криптоактивів шляхом координації розроблення та впровадження законодавчих і нормативних актів, підвищення обізнаності населення про ризики, пов’язані з криптоактивами, та зміцнення можливостей правоохоронних органів для протидії злочинним мережам.

Криптовалюти є одним із видів криптоактивів, що базуються на технології блокчейн і мають трикомпонентну структуру, описану винахідником Сатоші Накамото як «однорангова електронна система готівки». Ця система містить універсальний засіб обміну, інфраструктуру для емісії та аудиту, а також правила, що регулюють грошову пропозицію та процеси трансакцій. Незважаючи на децентралізовану організацію, правила заздалегідь визначені та реалізовані через алгоритм із відкритим кодом [220].

Чу Рене визначає криптовалюту як «віртуальний засіб обміну, який існує лише в електронному вигляді; він не має фізичного аналога, як монета чи банкнота, і не був підтриманий грошовим резервом на момент свого створення» [227].

Криптоактиви використовують алгоритми шифрування для створення та функціонування, виступаючи одночасно як валюта і віртуальна система обліку. Трансакції з криптоактивами відбуваються за допомогою шифрувальних алгоритмів та криптографічних методів, що перевіряються всіма користувачами системи для забезпечення безпеки [228]. Це означає, що введені дані є незмінними й не можуть бути скасовані. Така властивість блокчейну забезпечує постійний і загальнодоступний запис трансакцій. Крім того, це означає, що помилкові або шахрайські транзакції також неможливо анулювати, оскільки відсутній центральний орган, який би забезпечував скасування або відкликання інформації про здійснені операції з віртуальними активами.

Оскільки криптоактиви функціонують незалежно від центральних банків, вони обходять традиційну банківську систему. У користувачів немає криптовалютних рахунків у звичному розумінні. Кожна одиниця криптоактиву контролюється через набір ключів доступу, що ідентифікує кожну окрему монету. Власник монети має закритий (приватний) ключ [229], який підтверджує його право власності на актив, а трансакції анонімно фіксуються в блокчейні [230].

Хоча користувачам не потрібно розкривати особисту інформацію під час операцій із криптоактивами, псевдонімний ідентифікаційний номер їхнього криптогаманця часто є публічно доступним. Крім того, більшість блокчейнів відкриті для користувачів інтернету, що дає можливість відстежувати трансакції з криптоактивами. Тому, як стверджує Маріо Оттлер, хоча криптоактиви можуть забезпечувати певний рівень псевдонімності, публічний характер блокчейну й можливість відстеження означають, що вони не є повністю анонімними [231].

Крім використання криптоактивів для передачі незаконних коштів, вони

також можуть стати об’єктом крадіжок через зловмисне програмне забезпечення. Позиція Європолу збігається із санкціями США, накладеними на осіб і криптовалютні біржі, котрі допомагали північнокорейським хакерам відмивати викрадені кошти за допомогою криптовалют [232]. У цьому випадку злочинці використовували псевдонімність криптоактивів для сприяння незаконній діяльності, але технологія блокчейн і публічність даних зрештою дали змогу правоохоронцям відстежити трансакції.

Утім, різні сервіси й стратегії можуть підвищити анонімність і ускладнити роботу правоохоронних органів. Наприклад, для обміну до 1000 євро готівкою в деяких криптобанкоматах (АТМ) ідентифікація не потрібна. Можливе проведення кількох обмінних трансакцій протягом певного часу або використання різних криптобанкоматів [233] (Додаток А. Типологічне дослідження А.5).

Криптобанкомати відіграють зростаючу роль у сфері криптоактивів, забезпечуючи зручний спосіб швидкого обміну криптовалюти на фіатні гроші або навпаки. Вони спрощують процес передачі готівки від одного користувача до іншого, навіть якщо ті перебувають у різних місцях. Прихильники криптовалютного ринку вважають, що ці пристрої сприяють фінансовій інтеграції та поширенню криптоактивів.

Станом на листопад 2024 р. у світі працювало понад 4115 криптобанкоматів [234], багато з яких підтримували обмін різноманітних альткоїнів, таких як Ether, Litecoin, Dash, Zcash, Monero (Додаток Б). Проте в багатьох країнах ці пристрої залишаються нерегульованими або мають неоднозначний правовий статус, що робить їх привабливими для злочинців. Зловмисники використовують криптобанкомати для конвертації великих сум готівки у криптовалюту через простоту використання. Вони вивчають, як конвертувати нелегальні кошти в криптовалюту або навпаки та переказати ці активи іншим членам злочинної мережі. Це можна робити як у межах країни, так і на міжнародному рівні, уникаючи контактів із офіційною фінансовою системою

на певних етапах процесу ВК.

Поряд із орієнтацією на стандартні біржі криптоактивів злочинці можуть покладатися на так званих грошових мулів (осіб, котрі отримують на свій поточний рахунок гроші від інших людей (злочинців), перераховують ці кошти на інший рахунок або знімають готівку та передають злочинцю, за що отримують винагороду), щоб переказувати незаконні кошти через мережі криптобанкоматів. Використання значно поширених та складних мереж грошових мулів може створити додаткові проблеми у виявленні та запобіганні для операторів криптобанкоматів, особливо там, де використовується неправдива або вкрадена ідентифікаційна інформація.

У публічних звітах блокчейн-аналітичних компаній, таких як Chainanalysis, Crystal, Elliptic, CipherTrace, Global Ledger [413-416] (Додаток В), зазначено, що в криптобанкоматах зростає кількість шахрайських операцій з криптоактивами. Жертв обманюють, стимулюючи вносити фіатні кошти для подальшого переказу криптоактивів на відповідні криптогаманці, що належать злочинцям. У подальшому злочинці відмивають кошти через біржі або інші послуги з конвертації.

Термін «onramps» у криптовалютному середовищі означає процес конвертації традиційної валюти в криптовалюту, що дає змогу увійти на криптовалютний ринок. Це можна зробити різними способами, зокрема через купівлю криптоактивів за допомогою кредитної картки або банківського переказу, з використанням криптовалютного банкомата або отримання криптовалюти через надання послуг із майнінгу чи стейкінгу. Стейкінг (від англ. staking) — це механізм, за допомогою якого власники криптовалют блокують свої монети в мережі блокчейну для підтримки її роботи та отримують за це винагороду. Водночас «offramps» означає процес зворотної конвертації криптовалюти у фіатну валюту, що дає користувачам можливість вийти з крипторинку. Це може бути здійснено шляхом продажу криптоактивів за фіатну валюту на криптобіржі, зняття коштів у криптобанкоматі або через одноранговий

ринок криптовалют.

Така екосистема створює потенційні ризики відмивання грошей, оскільки забезпечує вільний доступ до крипторинку й вихід із нього, а також сприяє переливу коштів між традиційними фінансовими системами та крипторинком [235]. Важливим аспектом для виявлення злочинної діяльності, пов'язаної з криптоактивами, є здатність пов'язати псевдонімні ідентифікатори гаманців і трансакції з реальними особами. Саме тому криптобіржі, яким часто потрібно підтверджувати особу користувачів, є важливим джерелом інформації для правоохоронних органів. Однак злочинці знають про ці вимоги та нерідко намагаються використовувати підроблені документи під час реєстрації на криптобіржах. Коли біржі не проводять належної перевірки, незаконні кошти можуть бути перетворені на «чисту» криптовалюту [236].

Децентралізована структура криптоактивів ускладнює контроль за ними та залучення до судового процесу. Вони можуть становити загрозу для стабільності фіатних валют і сприяти формуванню сегмента економіки, що функціонує поза прямим контролем і регулюванням з боку держави [237]. Це спонукало окремі країни, у тому числі Індію та Китай, запровадити суворі обмеження на використання криптовалют. Водночас інші держави, такі як Японія, ухвалили законодавчі акти, що офіційно визнають криптоактиви як законний фінансовий інструмент. Однак більшість урядів лише нещодавно розпочали активні дискусії щодо регулювання криптоактивів [238].

Криптоактиви дають змогу майже миттєво здійснювати перекази коштів через кордони, надаючи злочинним організаціям зручні засоби для переміщення капіталу, обходячи транскордонні обмеження і збільшуючи ризики ВК/ФТ, пов'язані з криптовалютою [26; 27]. Незаконні кошти можуть бути спрямовані до інших фінансових юрисдикцій, де діють злочинні угруповання, для захисту активів від конфіскації під час ВК [37].

Тоді як традиційна банківська система використовує центральні органи для перевірки трансакцій, децентралізована природа криптоактивів дає змогу

здійснювати перевірку трансакцій у багатьох країнах, оминаючи звичайні регулюючі органи [32].

Наше дослідження показує, що злочинці дедалі більше уникають регульованих біржових платформ і віддають перевагу біржам, які не вимагають проходження процедур ЗСК. Як показано на рис. 2.7, після прийняття міжнародних стандартів FATF щодо криптоактивів у червні 2019 р. обсяги незаконних переказів біткоїнів на великі регульовані платформи ВА помітно знизилися, тоді як на біржах без вимог політики ЗСК вони зросли.

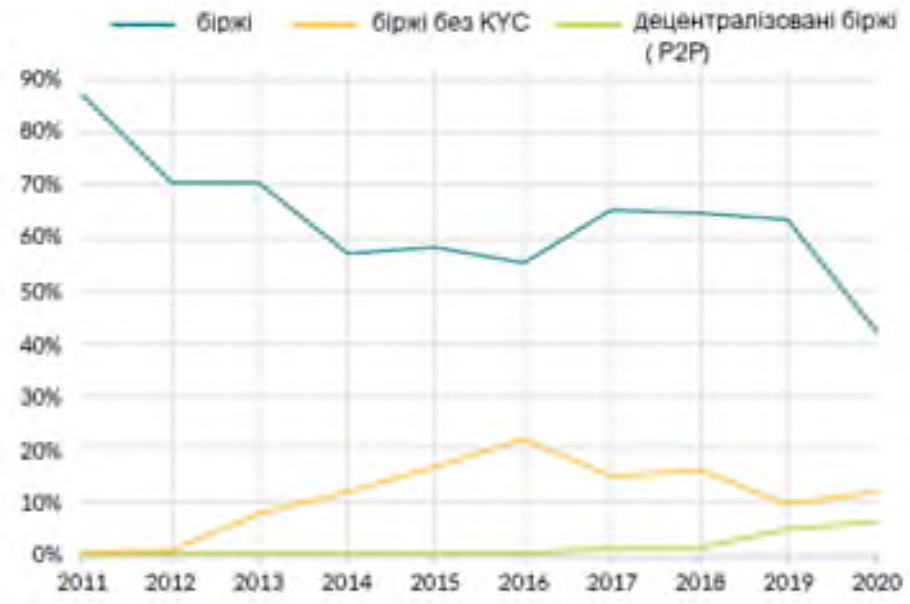


Рис. 2.7. Використання крипто бірж в процесі ВК/ФТ

Джерело: за матеріалами [233]

Криптобіржі забезпечують необхідну ліквідність ринкам криптовалют, виступаючи ключовими шлюзами між реальним світом і цифровими екосистемами. Як результат, вони часто відіграють значну роль у відмиванні коштів, пов'язаних із криптоактивами.

Злочинці цілеспрямовано шукають біржі, які, на їхню думку, дають змогу легко переміщувати кошти між фіатною валютою та криптоактивами або між самими криптоактивами, не створюючи особливих перешкод. Через відсутність ліцензування такі біржі зазвичай не вимагають від користувачів надання інформації для перевірки особи або належної перевірки клієнта для проведення

трансакцій. Біржі, що не впроваджують комплаєнс-процедур, і неліцензовані платформи створюють значні системні ризики для екосистеми криптоактивів, оскільки надають можливість різним незаконним суб'єктам брати участь у масштабному ВК (Додаток А. Типологічні дослідження А.5, А.6, А.7).

Зловмисники часто звертаються до криптобірж, розташованих у юрисдикціях підвищеного ризику, коли мають намір відмивати криптовалютні активи. Ця категорія може охоплювати країни та регіони, що в інших контекстах можуть не вважатися високоризиковими, але їх слід розглядати як такі для цілей відмивання криптоактивів.

Вони орієнтуються як на неліцензовані біржі, так і на ліцензовані та регульовані біржі, які дотримуються вимог ПВК/ФТ і вживають суворі заходи для зменшення ризику. Використання регульованих бірж може допомогти злочинцям надавати легітимність своїй незаконній діяльності. Легальні платформи можуть створювати для них ефект «змішування» трансакцій, що ускладнює виявлення злочинної активності.

Залежно від юрисдикції, платформи Peer-to-peer (P2P) можуть не підпадати під регулювання, і часто користувачам не потрібно надавати особисту ідентифікаційну інформацію. Платформи P2P, що функціонують окремо від великих централізованих бірж і активно обробляють значні клієнтські замовлення, слугують координаційними майданчиками для прямої взаємодії користувачів криптовалют при обміні на фіатні гроші та інші криптоактиви. Це включає прямі грошові перекази між користувачами. Такі платформи відіграють важливу роль у криптовалютній екосистемі, надаючи користувачам можливість обмінюватися активами без участі великих централізованих посередників.

Основні платформи P2P, такі як LocalBitcoins та Paxful, мають ефективні системи дотримання вимог ПВК/ФТ, але багато інших платформ цього не роблять. Злочинці використовують таких неліцензованих P2P-продавців для відмивання незаконно отриманих коштів (Додаток А. Типологічне дослідження А.8).

Крім того, у країнах, де правоохоронні органи не мають необхідної спроможності чи ресурсів для подолання псевдонімності системи, використання криптовалют може слугувати ефективним засобом маскування незаконних трансакцій і, отже, є привабливим для злочинців [240].

На відміну від простих платформ P2P, що є основними вебсайтами для взаємодії користувачів криптоактивів, децентралізовані біржі (DEX), побудовані на базі блокчейн-платформі Ethereum, використовують смарт-контракти для забезпечення реального часу обміну криптоактивами між користувачами.

Децентралізовані фінанси (DeFi) стали однією з найцікавіших сфер інвестиційного зростання криптоактивів у 2020 р. Завдяки мережі Ethereum новатори запустили платформи DeFi для послуг кредитування, прогнозування ринків, децентралізованих послуг обміну (DEX).

Окремі експерти вважають DEX кращими від централізованих бірж, оскільки DEX менше схильні до крадіжок і втрат, не потребують зовнішнього управління [241].

У 2020 р. обсяги торгів на DEX зросли, досягнувши понад 30 млрд дол. США на місяць. Основні DEX, такі як Uniswap, вже конкурують із великими централізованими біржами за обсягами торгів. Зростання ліквідності на DEX зробило їх більш вразливими для використання відмивачами грошей, котрі можуть переміщати значні обсяги коштів через ці активні платформи. Наприклад, на 2 жовтня 2020 р. через DEX було переміщено викрадені токени Ethereum на суму, еквівалентну 19,5 млн дол. США з KuCoin (Додаток А. Типологічне дослідження А.9).

Послуги азартних ігор із криптоактивами, такі як Satoshi Dice, стали одними з перших, найуспішніших і найбільш популярних програм у цій сфері. Сьогодні існують численні ігрові сайти та онлайн-казино, що приймають криптовалюти від своїх клієнтів. Крім того, нові онлайн-біржі дозволяють користувачам обмінювати криптовалюти на ігрові валюти, такі як Linden Dollars і World of Warcraft Gold, створюючи дедалі складнішу екосистему азартних ігор.

Хоча ці платформи підтримують ігрову інфраструктуру, вони також можуть бути використані для відмивання грошей. Багато онлайн-азартних послуг не вимагають надання інформації за вимогами комплаєнс-процедур. Дослідження Elliptic показало, що азартні сайти обробляли близько 20% біткоїнів, отриманих через «темний» вебринок Alphabay у 2015–2016 рр. [239]. Водночас, як показано на рис. 2.8, азартні ігри стали менш популярними серед методів відмивання з використанням біткоїнів.

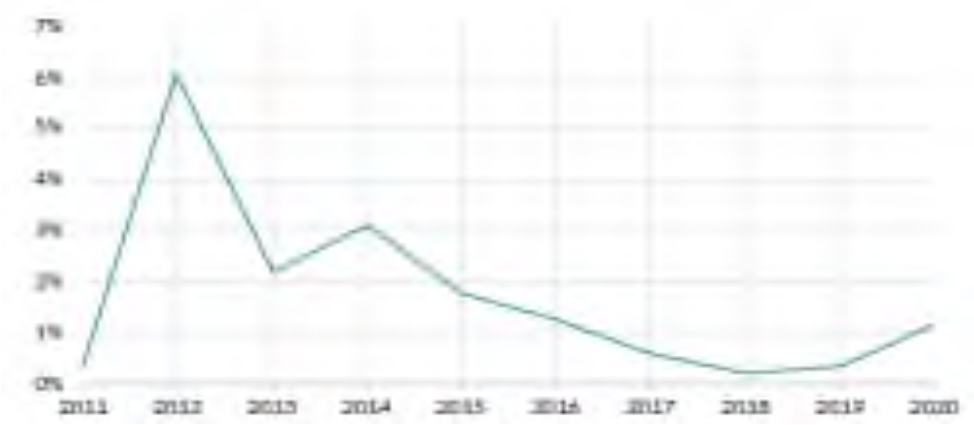


Рис.2.8. Обсяги надходжень у азартні крипто валютні ігри та інші ігрові послуги, пов'язані з криптоактивами

Джерело: за матеріалами [239]

Проте у 2020 році було зафіксовано підвищення обсягів ВК через азартні ігри, зокрема, за допомогою біткойнів, порівняно з попередніми двома роками.

Два основні методи, які злочинці використовують для ВК через азартні ігри з використанням криптовалют, такі:

1. Використання Інтернет-казино для ВК.

Інтернет-казино, які працюють тільки з криптовалютами або приймають як фіатні гроші, так і криптовалюти, є популярним інструментом для легалізації незаконних коштів. Ці методи нагадують традиційні способи відмивання грошей, якими злочинці користуються в казино вже десятиліттями. Зловмисники купують фішки або роблять ставки, використовуючи брудні гроші, а потім виводять виграш (або компенсують збитки як частину процесу відмивання). Вони отримують нові кошти та квитанцію від казино, що маскує джерело коштів.

2. Обмін криптовалют на ігрові валюти.

Ігрові валюти, такі як Linden Dollars та World of Warcraft Gold, все частіше доступні на онлайн-біржах, таких як VirWox [239]. Обмін криптовалют через ці платформи надає злочинцям вигідний спосіб розподіляти незаконні доходи через різноманітні онлайн-екосистеми, що дозволяє їм переривати ланцюг трансакцій в кіберпросторі. Цей метод допомагає відмивати незаконні криптовалюти або приховувати брудну готівку.

З точки зору суспільного розвитку, вплив криптовалют є досить суперечливим. Прихильники вважають, що вони сприяють інклюзивному розвитку, пропонуючи децентралізовані, безпечні та прозорі способи здійснення фінансових операцій. Наприклад, криптоактиви можуть спростити міжнародні платежі та грошові перекази, розширюючи доступ до фінансових послуг для людей, які не мають доступу до банківських послуг або мають обмежений доступ, а також надаючи підприємцям і малому бізнесу можливість отримувати капітал із альтернативних джерел [242].

З іншого боку, критики звертають увагу на можливий негативний вплив криптовалют на економічний розвиток. Головною проблемою є висока волатильність і часті коливання їхньої вартості, що створює труднощі для компаній та окремих осіб у довгостроковому плануванні та інвестуванні [243].

Криптоактиви також привабили інвесторів, які шукають «швидкого збагачення», а зростання ринкових цін значною мірою було обумовлене залученням нових інвесторів. Подібні спекулятивні вкладення можуть створити фінансову бульбашку, яка в разі різкого падіння вартості віртуальних активів призведе до значних збитків для інвесторів. Наприклад, у листопаді 2021 року біткойн досяг ціни 70 000 доларів США, але до листопада 2022 року впав майже на 75%, що завдало великих втрат багатьом звичайним інвесторам, зокрема, у країнах із низьким і середнім рівнем доходів [244].

Малгожата Кутера відзначає, що децентралізована, розподілена і захищена структура криптовалют суттєво сприяла перетворенню їх на глобальну

торговельну платформу [245]. Проте ці ж самі риси зробили криптоактиви привабливими для кримінальних елементів [246]. Різке зростання цієї галузі, імовірно, призведе до збільшення злочинної діяльності, пов'язаної з криптовалютами, та відмивання грошей із використанням ВА [247]. Справді, у недавньому звіті Європолу йдеться, що використання криптоактивів для нелегальних цілей і приховування незаконних доходів значно зросло за обсягом і складністю за останні роки [230].

Згідно зі звітом Європолу про криптоактиви та кримінальні фінанси за 2022 рік, зростання популярності цифрових валют сприяло їхньому активному використанню організованими злочинними групами. Європол відзначає, що «кримінальне використання криптоактивів більше не обмежується кіберзлочинністю, а охоплює всі види злочинів, де є потреба у передачі вартості». Звіт також підкреслює роль криптовалют у злочинах, пов’язаних із корупцією, та їхню загальнішу функцію у сприянні організованій злочинності, зокрема як інструмент ВК. Нині операції з ВК займають найбільшу частку в незаконних операціях із криптовалютами, перевершуючи навіть шахрайство [230].

Криптоактиви можуть допомагати зловмисникам, які скоїли фінансові злочини, приховувати джерело злочинних доходів для кожного типу правопорушень. Наприклад, незважаючи на те, що процес майнінгу, що вимагає застосування потужних комп'ютерних систем для розв’язання складних математичних задач і підтвердження трансакцій у блокчейні, сам по собі не є протиправним, його можна організувати з використанням злочинних активів.

Злочинці можуть вкладати доходи від незаконної діяльності, як-от торгівля наркотиками чи рекет, у фінансування майнінгу криптовалют, створюючи нові цифрові монети, які не мають явного зв’язку з правопорушеннями. Після цього ці монети можуть бути продані за фіатну валюту, що забезпечує ефективний спосіб ВК [249].

Також існують постачальники кримінальних послуг, які сприяють

переказу злочинних доходів через криптоактиви. Виявлення нелегального походження активів, що зберігаються в криптовалюті або відмиваються через криптоактиви, є складним завданням. Таким чином, важко визначити масштаби використання криптовалют для ВК, отриманих у результаті традиційних офлайн-злочинів [239].

Це пов’язано з тим, що в таких випадках криптовалюта не проходить через адреси, раніше пов’язані зі злочинами. Натомість кошти у фіатній валюті спершу конвертуються у криптоактиви (наприклад, через біржі або згадані вище сервіси майнінгу), і блокчейн не містить прямих ознак незаконного походження [250].

Таким чином, нелегальне використання криптоактивів уже не обмежується лише «ланцюговими» злочинами, як-от шантаж чи атаки програм-вимагачів, де кіберзлочинці вимагають оплату в криптовалюті. Окрім того, що криптоактиви служать засобом передачі незаконних доходів, вони також можуть ставати об’єктом крадіжок за допомогою різного шкідливого програмного забезпечення, яке націлене як на біткоїни, так і на NFT та активи в Метавсесвіті [239].

ВА зараз застосовуються для здійснення різних правопорушень, що передбачають обмін грошових цінностей, зокрема для придбання незаконних товарів і послуг, пов'язаних із «позаланцюговими» злочинами, як-от торгівля наркотиками, замовні вбивства та матеріали, що стосуються сексуальної експлуатації дітей [250, 251].

Капіталізація крипторинку за даними Звіту про криптозлочинність у 2024 році блокчейн-аналітичної компанії Chainanalysis знову суттєво знизилася до 24,2 мільярда доларів США [252].

У 2023 році відбулось зростання цін на криптовалюти, оскільки індустрія відновилась після скандалів, злетів і падіння цін у 2022 році. Протягом 2023 року оборот криптоактивів відновлювався, а ринкова активність зростала, однак це не впливало на показники обсягів криптозлочинності, деякі показники навіть за обсягами зменшились [253] (рис. 2.9).

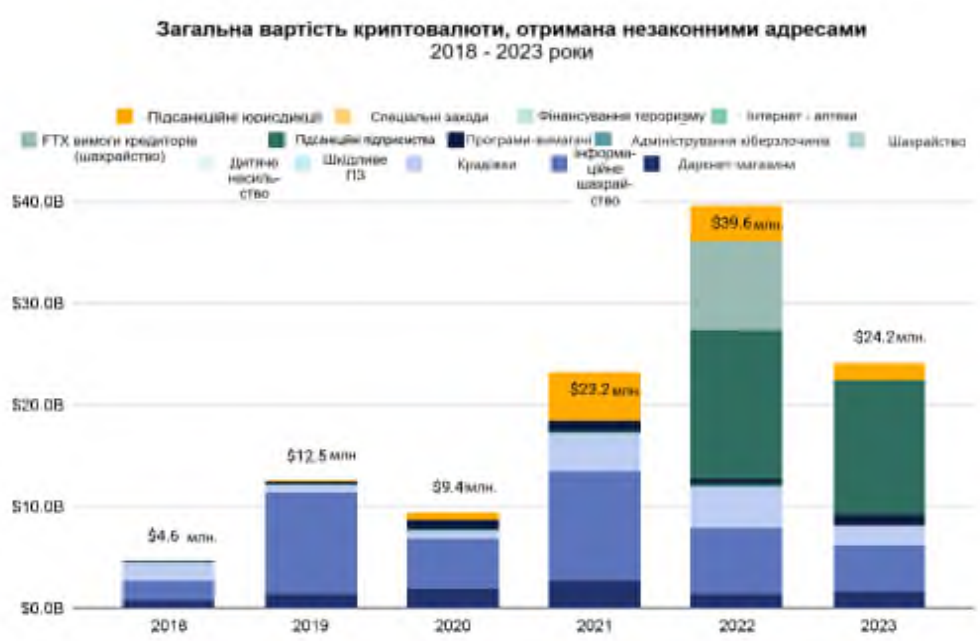


Рис.2.9. Розподіл злочинних надходжень у ВА за типами злочинної діяльності

Джерело: за матеріалами [252].

Як завжди, варто зазначити, що наведені цифри є мінімальними оцінками, базованими на надходженнях на виявлені незаконні адреси на сьогодні. Через рік ці показники будуть вищими, оскільки з часом ідентифікується більше незаконних адрес і в статистиці враховується їхня історична активність в оцінках, що призводить до необхідності коригувати цифри попередніх звітів Chainanalysis.

Наприклад, коли опублікували звіт про криптовалютні злочини за 2022 р., обсяг незаконних трансакцій було зафіксовано на суму 20,6 млрд дол. США [252]. Через рік оновлена оцінка за 2022 р. становила 39,6 млрд дол. США, що ми можемо побачити з аналогічного звіту за 2023 р. [253]. Значна частина цього зростання пов’язана з ідентифікацією раніше невідомих, надзвичайно активних адрес, які використовуються санкційними сервісами, а також із додаванням обсягів трансакцій, пов’язаних із сервісами в юрисдикціях під санкціями, до загальної суми незаконних операцій.

Іншою важливою причиною, чому нова загальна сума є настільки вищою, крім виявлення нових незаконних адрес, є врахування аналітиками компанії 8,7 млрд дол. США в претензіях кредиторів проти криптобіржі FTX відносно показників за 2022 р. унаслідок судового визнання винним у шахрайстві колишнього генерального директора FTX (Додаток А. Топологічне дослідження А 11).

Всі інші підрахунки не включають доходи від не пов'язаних з криптовалютою злочинів, таких як звичайна торгівля наркотиками, де криптовалюта використовується як засіб платежу. Такі трансакції практично не відрізняються від законних трансакцій у даних блокчейну. Проте правоохоронні органи з позаланцюговим контекстом все ще можуть розслідувати ці потоки за допомогою рішень Chainalysis.

Наразі, за відсутності офіційної статистики про діяльність ринку ВА у деяких країнах, які ще працюють над упровадженням оновленої 15-ї та адаптованої до криптотрансакцій 16-ї Рекомендацій FATF, дані звітів Chainalysis широко використовуються для власних досліджень і звітів не лише правоохоронними органами та урядами, а й міжнародними організаціями. Chainalysis послуговується методологією збору даних, базованою на обсягах криптовалютних трансакцій у різних сервісах і протоколах на основі вебтрафіку цих платформ. Використання вебтрафіку означає, що застосування віртуальних приватних мереж (VPN, англ. virtual private network) та інтернет-засобів для приховування активності користувачів може впливати на показники. Проте, з огляду на те, що дані Chainalysis охоплюють сотні мільйонів трансакцій, VPN має використовуватися в надзвичайно масових масштабах, щоб суттєво спотворити дані.

Експерти міжнародних організацій загалом погоджуються, що статистика відповідає їхнім уявленням про ринки, з якими вони працюють, що підвищує довіру до методології Chainalysis. Як зазначено у першому розділі цього

дослідження, методологія та статистика Chainalysis також використовуються для розрахунку Глобального індексу сприйняття криптоактивів [171].

У першому розділі дисертаційного дослідження ми торкались питання впливу використання ВА в злочинній діяльності на необхідність легалізації ринку ВА або заборони обігу ВА на національному рівні. Також зазначали, що як наступний крок після оновлення Рекомендації 15 FATF, Пояснювальної записки до неї [223] та Керівництва щодо ризик-орієнтованого підходу щодо обігу ВА та діяльності ППВА [30] FATF підготувала звіт про індикатори «червоних прапорців» для ВК/ФТ, пов’язаних із ВА. Звіт мав допомогти підзвітним суб'єктам у виявленні та інформуванні про потенційну діяльність ВК/ФТ з використанням ВА, включно з аспектами звітності щодо підозрілих трансакцій (StR, англ. suspicion transactions).

Нагадаємо: “червоні прапорці” (англ. Red flag indicators) – це ознаки підвищеного ризику ВК/ФТ, що вказують на можливе використання інструментів ринку ВА фінансовими установами та учасниками цього ринку для ВК/ФТ, шахрайства та кіберзлочинності. Окремі з “червоних прапорців” та підходів, що часто використовуються злочинними організаціями, можуть стосуватися різних пріоритетів. Виявлення таких ознак стає легшим, коли ці підходи та показники (тригери) повторюються у певних ризикових ситуаціях. Часте запитання від фінансових організацій стосується розпізнавання та розуміння сутності таких злочинів і їхнього впливу на фінансові операції та операції з ВА [38].

Різноманітність злочинної діяльності із залученням ВА не дає змоги створити універсальний набір «червоних прапорців» для всієї злочинної діяльності з ВА, тому для кожного типу злочину розроблено окремі індикатори ризиків. У деяких випадках індикатори можуть збігатися, але для певних злочинів, пов'язаних із особливостями технології, наприклад, у кіберзлочинності, ризики мають унікальний характер. Проте у випадках ВК, незалежно від предикатного злочину, «червоні прапорці» перестають бути

унікальними, оскільки за методологією ВК етапи цього злочинного процесу однакові, єдине, чим вони можуть відрізнятись – це використання фінансового, нефінансового чи цифрового інструментарію [254, с. 117].

Тому для розуміння технології використання ВА в злочинній діяльності потрібно застосувати кластерно-порівняльний аналіз, де тип злочинної діяльності розглядається як кластер. Для порівняння кластерів виберемо способи використання ВА:

- як платіжного засобу (торгівля незаконними товарами, вимагання, фінансування тероризму, уникнення санкцій, корупція, нелегальна діяльність);
- як цифрового інструменту з використанням відповідних йому характеристик (шахрайство через маніпулювання ринком віртуальних активів, випуск нових монет (ICO, IDO), схеми Понці, розмивання бази оподаткування, нелегальна діяльність).

На практиці ці злочинні способи використання криптоактивів часто змішують для ускладнення їхнього розслідування. Однак на початку визначимо технологічні інструменти для першого класу використання ВА у злочинній діяльності з відповідними типологічними оглядами.

Варто зазначити, що у випадках використання ВА як платіжного засобу в злочинній діяльності найчастіше використовують першу криптовалюту – біткоїн (BTC), незважаючи на її високу волатильність. Так, за статистичними даними блокчейн-аналітичної компанії Crystal, біткоїн залишається найбільш використовуваною валютою серед суб’єктів мережі Даркнет (англ. DarkNet) (рис. 2.10).

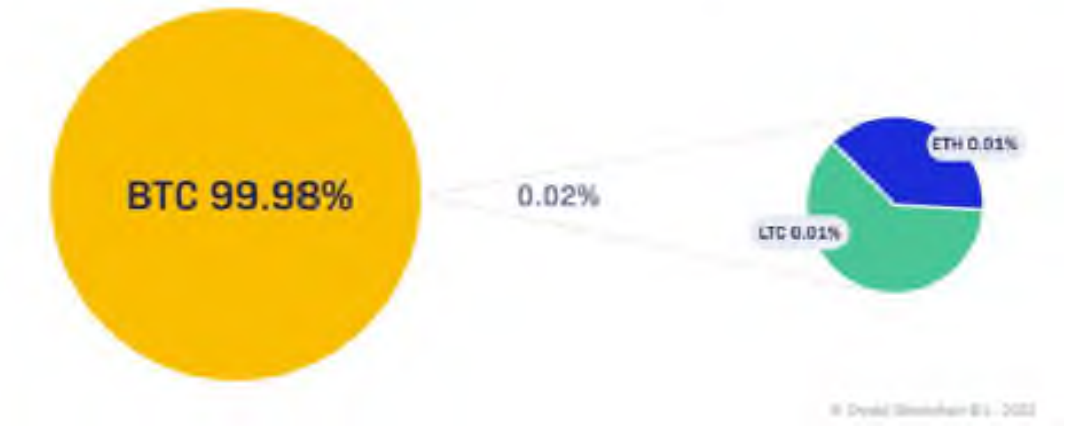


Рисунок 2.10. Обсяги переказів криптовалют BTC, ETH та LTC в Даркнет в 2022 році

Джерело: за матеріалами [255]

Даркнет (також відомий як «Прихована мережа», «Темний інтернет», «Темна мережа», «Тіньова мережа», «Темний веб») — це прихована мережа, де з'єднання встановлюються тільки між довіреними вузлами, із застосуванням нестандартних транспортних протоколів та портів. Інакше кажучи, ресурси, не проіндексовані пошуковими системами (HTML-сторінки, зображення, файли, медіа-потоки або інші дані), можуть бути доступні користувачу через пряме мережеве з’єднання [255]. Даркнет є повністю анонімною, нерегульованою і нікому не підконтрольною частиною інтернет-мережі. Він не доступний для звичайних користувачів. Доступ до нього можна отримати тільки за допомогою спеціальних програм, найвідоміша з яких Tor Browser [256].

TOR (скорочено від англ. The Onion Router) – найвідоміша і популярна анонімна мережа Даркнету. Це система проксі-серверів, що підтримують “цибулеву маршрутизацію” – технологію анонімного обміну інформацією через комп'ютерну мережу. Tor дає можливість зберігати анонімність в інтернеті та захищає трафік користувача від аналізу.

Даркнетом активно користуються злочинці, продавці заборонених товарів (насамперед персональних даних та наркотиків), дитячої порнографії, всіляких кримінальних послуг [247].

Майже 100 % отриманих і надісланих сум суб'єктами Даркнету були зроблені в біткоїнах. З цієї причини аналіз купівлі-продажу недозволених товарів Даркнету зосереджено на обсягах переказу біткоїнів. Найбільш значна частина грошей, що надсилаються організаціям Даркнету, є їхніми власними активами [247].

Зі злочинною метою Даркнетом користуються для забезпечення анонімності учасників та їхньої діяльності. Тобто в злочинних трансакціях з ВА як платіжним інструментом головною вимогою є анонімність. Користувачі Даркнету уникають взаємодії із зареєстрованими (легальними) ППВА, щоб не розголошувати чи не заморожувати їхні кошти через їх походження. Користувачі Даркнету прагнуть використовувати міксери для виведення грошей. За результатами спостережень сума трансакцій зросла протягом усього аналізованого періоду, за винятком 2022 р. На початку 2022 р. від суб'єктів Даркнету до міксерів було надіслано більше коштів, ніж рік тому. Однак після січня 2022 р. спостерігається падіння перерахованих сум.

Даркнет, як зазначалося вище, не єдиний інструмент забезпечення анонімності. Розглянемо технологічні рішення для підвищення анонімності в операціях з ВА, що найчастіше використовують для приховування джерел походження коштів.

У сфері як фіатних, так і віртуальних активів для приховування джерел походження коштів, отриманих від учинення злочинів або набутих злочинним шляхом, використовують інструменти підвищення анонімності учасників трансакцій.

Зокрема, ІТ-фахівцями розроблено віртуальні монети з підвищеною анонімністю. За підсумками минулого року до десятки найанонімніших монет віднесено Monero (XMR), Zcash (ZEC), PIVX (PVX), Komodo (KMD), Verge (XVG), ZCoin, GRIN, Navcoin (NAV) [258;259] (Додаток Б). Водночас використання цих монет під час проведення трансакцій з віртуальними активами, декларування останніх наражають власника на додаткові питання з

боку наглядових і правоохоронних органів щодо їх вибору. Тому для приховування джерел походження криптоактивів найпоширенішими наразі є спеціально розроблені програми, що сплутують ланцюги трансакцій, а саме міксери, тумблери та децентралізовані протоколи, котрі працюють без людського втручання.

Криптоміксери завжди мали жорсткі відносини з правоохоронними органами та компаніями у сфері Blockchain Intelligence. Змішувач (міксер, тумблер, смарт-контракт) – це послуга з високим ризиком для користувача незалежно від того, за яким протоколом він побудований; клієнти надсилають кошти організації в надії, що їх буде повернуто. Змішувач потребує достатньо коштів, аби зробити заміну через поставку нових активів замість попередніх. Серед згаданих структур переважає думка, що змішувачі працюють лише в кримінальних цілях, хоча варто нагадати, що подібні аргументи висувалися стосовно шифрування даних під час передачі на початку існування інтернету. Всі вони мають дві ключові характеристики: довіра та ліквідність.

Таким чином, користувач віддає кошти, сподіваючись на їх повернення, – ненадійний сценарій, котрим часто послуговуються шахраї. Завдяки блокчейну Ethereum та його здатності запускати смарт-контракти існують некастодіальні послуги, коли користувач просто вносить кошти в контракт міксера та вказує адресу для отримання коштів після змішування.

Як приклад наведемо таку ситуацію. Управління США з контролю за іноземними активами (Office of Foreign Assets Control, OFAC) оголосило про застосування санкцій до Tornado Cash, популярного сервісу змішування криптовалют. Це другий випадок, коли OFAC використовує фінансові санкції проти послуг із криптомікшування (перший – ситуація з Blender.io у травні 2022 р.) [260]. Подібні зусилля переважно спрямовані на забезпечення контролю діяльності найпотужніших глобальних злочинних угруповань, терористичних організацій чи навіть національних держав і характеризуються як прояв “жорсткої сили”.

Tornado Cash (tornado.cash) описує себе як “повністю децентралізований протокол для приватних трансакцій на Ethereum”. Він стверджує, що “покращує конфіденційність трансакцій, розриваючи зв’язок onchain (тобто всередині мережі) між адресами джерела та призначення” [261]. Tornado здобув сумну популярність, оскільки фактично став місцем призначення вкрадених коштів, зокрема тих, які забрала північнокорейська хакерська група, відома як Lazarus, після зламу мосту 1 Ronin у березні 2022 р. Дослідження Crystal Blockchain показало, що 95 % усіх публічних коштів, пов’язаних із Lazarus, були відправлені в Tornado Cash. Це становило понад 4 % усіх коштів, отриманих сервісом [260]. Lazarus була не єдиною групою, яка покладалася на Tornado Cash, аби приховати джерело коштів; їхні послуги використовувалися в інших великомасштабних крадіжках, а також шахрайствах. З цієї та інших причин багато представників правоохоронних органів вважають доцільною заборону цього криптоміксеру. Після застосування певних попередніх публічних санкцій представники Tornado заявили, що дотримуватимуться їх, і вжили заходів для реалізації рішення. Попри ці зусилля, однак, не можна говорити про його високу ефективність.

Як і більшість подій та рішень, котрі стосуються криптовалюти, наслідки накладання санкцій на Tornado Cash, імовірно, відчуються негайно. Попри те, що сервіс усе ще може працювати (зрештою, це програмний код (смарт-контракт)), санкції OFAC означають, що будь-який бізнес, котрий підпадає під регуляторний вплив Сполучених Штатів і пропонує послуги підприємствам, громадянам, не може приймати кошти від Tornado Cash. Іншими словами, будь-яке майно або інтереси Tornado Cash, розміщені в США, теж повинні бути заблоковані й про них має бути повідомлено OFAC. Пропозицією щодо ВК може також стати перехід до діяльності на основі міжланцюгових мостових протоколів, таких як renBTC [262]. Аналітичну програму Crystal Blockchain було оновлено протягом 30 хв після публікації заяви OFAC, тобто клієнти відповідної аналітичної компанії змогли негайно скоригувати свій профіль ризику та ризики з

упроваджених санкцій. Інші подібні аналітичні програми теж розмітили власні й клієнтські криптогаманці та трансакції з ВА, дотичні до діяльності Tornado Cash.

Перейдемо до другого класу кластерів злочинної діяльності, пов'язаної з ВА, в яких використовують заявлену та відсутню ліквідність ВА або фіктивно підвищують ліквідність токенів у DeFi, ініціюють залучення інвесторів у нові, часто нічим не забезпечені монети та проєкти з ними, маніпулювання цінами на ВА, тобто в суті злочинів яких є шахрайство.

Подібно до інструментів фінансового та фондового ринків у блокчейні та децентралізованих фінансах (DeFi) створюють інструменти з удаваною ліквідністю, подібні до технічних ("сміттєвих") цінних паперів, а також запускають проєкти випуску нових монет та їхнього первинного розміщення без фінансового і технічного (IT-перевірки) аудиту [264].

24 % нових токенів, запущених у 2022 р., відповідають характеристикам схеми Pump & Dump, яка є досить поширеною на криптовалютному ринку, оскільки для її реалізації потрібна значно менша ліквідність, ніж на фондовому чи валютному ринках, де маніпулювати цінами активів істотно складніше [265].

За визначенням експертів-розробників кастодіальних та некастодіальних криптогаманців Trustee Plus, «Pump & Dump (памп і дамп) – це схема маніпулятивного підвищення ціни шляхом купівлі, а потім продажу активів на великі суми: цінних паперів, дорогоцінних металів або криптовалют. Термін Pump (накачування) означає, що трейдер штучно завищуватиме курс з метою підвищення попиту на криптовалюту. Dump (скидання) називають ціновим обвалом після стрімкого зростання, коли трейдер фіксує прибуток» [266].

Вперше схема Pump & Dump була застосована ще у XVII ст. у Великій Британії: Компанія South Sea Bubble штучно підняла курс своїх акцій, обіцяючи інвесторам великий прибуток, що призвело до створення фінансової бульбашки. Шахраї почали використовувати такі схеми на фондовому, а згодом і на криптовалютному ринку. Вони орієнтуються на «сміттєві» акції, криптовалюти та токени. Такі «сміттєві» активи — це цінні папери чи криптовалюти з низькою

капіталізацією, курс яких легко змінити на власну користь. Ці активи також називають «шиткоїнами».

Це явище стосується і великих криптовалют: першим масштабним прикладом став дамп біткоїна у 2017 р., коли в криптовалюту вкладалися недосвідчені інвестори, котрі недостатньо розуміли і сам біткоїн, і особливості крипторинку загалом. Падіння ціни біткоїна потягнуло за собою і курси альткоїнів, деякі з них втратили понад 90 % своєї вартості за кілька місяців.

Щоб розпізнати памп криптовалюти, варто звернути увагу на графік, де курс матиме форму гори або трикутника, як показано на наведеному нижче скриншоті. Pump & Dump зазвичай відбувається після лістингу на біржі, коли інтерес до криптовалюти різко зростає (рис. 2.11). Шахраї організовують короткострокові пампи, прагнучи отримати швидкий прибуток. Натомість довгострокові пампи можуть виникати природним чином, наприклад, коли в медіа з’являється новина про значну інвестицію у криптовалюту з боку великого інвестиційного або хедж-фонду.

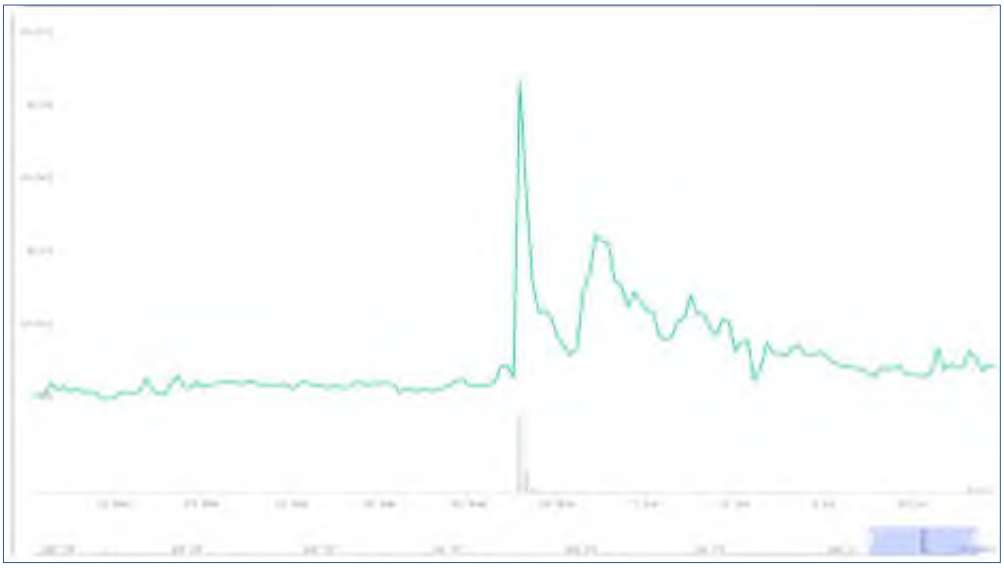


Рис. 2.11. Pamp&Damp пари криптовалюти Dogecoin з фіатною валютою USDollar. Криптобіржа Binance. TradindView.

Джерело: за матеріалами [271]

Навіть твіт відомої особистості може спричинити різкий короткостроковий памп. Це винятковий випадок, адже користувачі помилково сприймають

подібний твіт як інвестиційну пораду. Наприклад, після публікацій Ілона Маска різко зростала вартість великих криптовалют, таких як Bitcoin і Dogecoin.

Ще одним прикладом маніпулювання ринком є штучне збільшення нових криптомонет. За рахунок відсутності вимог до реєстрації емісії криптомонет випуск таких ВА є нескладною діяльністю на рівні ІТ-розробки смарт-контракту на децентралізованій платформі. У подальшому, за рахунок власних ліквідних або широковідомих та котированих на криптобіржах криптоактивів, формується та штучно підвищується вартість нової монети шляхом великої кількості операцій для подальшого лістингу її на криптобіржі. Так створюється «технічний» інструмент поза параметром державних регуляторних вимог до емісії криптоактивів.

Подібні маніпулювання криптоактивами здійснюються і за рахунок шахрайських «схем Понці» із залученням інвесторів до нових криптопроєктів (Додаток А. Типологічне дослідження 9)

У березні 2020 р. FATF опублікувала керівництво щодо цифрового ідентифікатора [267], щоб допомогти ідентифікувати клієнтів у цифровому вигляді. У Керівництві переглянуто міжнародні стандарти ПВК/ФТ, які застосовуються до стейблкоїнів.

Як і у випадку з ППВА, важливо, щоб були проаналізовані ризики ВК/ФТ щодо стейблкоїнів, особливо тих, які мають потенціал масового використання та які можна використовувати для P2P-трансакцій на постійній та перспективній основах. Під час розроблення нових продуктів постачальники послуг із віртуальних активів та інші зобов’язані суб’єкти повинні оцінити ризики ВК/ФТ перед тим, як вивести їх на ринок, та вжити заходів щодо зменшення їхнього впливу перед запуском. Потенційні заходи зменшення можуть включати, наприклад:

- обмеження можливостей користувачів здійснювати анонімні операції;
- контроль того, хто може отримати доступ до угоди;

– контроль того, чи/як запобіжні заходи ПВК/ФТ вбудовані в угоду та/або забезпечення того, щоб ці вимоги до зобов'язаних осіб виконувалися в рамках угоди, наприклад, за допомогою програмного забезпечення для моніторингу трансакцій та виявлення підозрілої активності.

Стейблкоїни є важливою частиною екосистеми криптовалют, і попит на них буде зростати, бо вони є неволатильними активами, які забезпечують глобальний трансфер грошей на крипторинку. На 1 квітня 2021 р. загальна ринкова капіталізація стейблкоїнів становила 64,5 млрд дол. США, що у 12 разів більше порівняно з 2020 р. [37].

USDT (раніше відома як RealCoin) – централізований стейблкоїн, який уперше було представлено на біржі Bitfinex у 2015 р. Враховуючи те, що це перший стейблкоїн на ринку, він і тепер має велику перевагу за обсягами емісії та послідовно зберігає позиції лідера ринку стейблкоїнів. На квітень 2021 р. ринкова капіталізація USDT становила 40 млрд дол. США, або 66 % загального обсягу ринку стейблкоїнів [37].

USDT підтримує прив’язку до долара США через систему забезпечення за принципом «один до одного». Оскільки цей стейблкоїн еквівалентний USDT, його резервним забезпеченням виступають готівка та інші активи. Це певною мірою нагадує історичну практику, коли долар США був забезпечений золотом. Однак проблема полягає в непрозорості процесу випуску стейблкоїна Tether (USDT). Оскільки його емісія має централізований характер і спирається на резервний фонд, у криптоспільноті до нього ставляться зі скептицизмом. У березні 2019 р. ці побоювання частково підтвердилися, коли Tether змінив свою стратегію, використавши USDT для забезпечення кредитів своїм дочірнім компаніям.

Протягом багатьох років Tether перебував під розслідуванням різних державних правоохоронних органів. У лютому 2021 р. генеральний прокурор штату Нью-Йорк розслідував внутрішні фінансові операції Bitfinex і Tether. Хоч офіційних звинувачень не висували, компанії було призначено колективний

штраф у розмірі 18,5 млн дол. США за звинуваченням у змішуванні клієнтських і корпоративних активів.

Ситуація навколо Tether залишається відкритою і навряд чи буде врегульована найближчим часом. Водночас такі події, як лістинг USDT на Coinbase, сприяють зміцненню його легітимності. Крім того, технічний директор Bitfinex підтвердив, що Tether зареєстрований і регулюється FinCEN.

Maker є одним із перших DeFi-проєктів, що виконує функції децентралізованого «центрального банку». Як протокол кредитування він випускає DAI як похідний продукт попиту на позики, тоді як застава (зазвичай у формі ETH) депонується у сховищі Maker. Ці сховища суттєво забезпечені (зазвичай 150 % і вище, крім стейблкоїнів), що допомагає захиститися від «чорного лебедя», коли вартість забезпечувальних активів значно падає. «Чорний лебідь» — теорія, що розглядає важкопрогнозовані та рідкісні події, котрі мають значні наслідки (англ. TBS, The Black Swan) [259].

Maker допомагає регулювати кількість DAI, контролюючи процентні ставки за кредитами, щоб впливати на попит і пропозицію.

Проблема з цим стейблкоїном полягає в тому, що надмірне забезпечення обмежує ефективність використання капіталу, що ускладнює масштабування відповідно до попиту. Арбітражна техніка використовується для зниження ціни DAI шляхом викупу цього стейблкоїна за ринковою ціною, якщо вона вища за прив’язану вартість (1 DAI ≈ 1 USD), і подальшого його погашення (redeem) через механізми системи MakerDAO.

Цей процес передбачає збільшення обсягу DAI, що викуповується та погашається, що, своєю чергою, потребує залучення більшого капіталу. Основна ідея – зменшити загальну кількість DAI в обігу, що сприяє його дефіциту та коригуванню ціни вниз до цільового рівня.

Наприклад, основне сховище ETH, коефіцієнт забезпечення якого становить 150 %, вимагатиме від позичальника сплатити 1,5 дол. США за 1 DAI. Це призводить до сценаріїв, таких як сумнозвісний «Чорний четвер» і запуску

майнінгу ліквідності Compound, коли ціна DAI перевищила позначку в один долар, оскільки вона не могла задовольнити попит.

Усі стейблкоїни мають власні недоліки, що не обмежуються недоліками Tether або DAI. В основі проблеми перебуває балансування принципів децентралізації DeFi проти створення валюти, яка може надійно підтримувати свою прив'язку.

З одного боку, централізовані стейблкоїни ефективні, їхнє використання вимагає довіри, відповідно, до центральної організації та пов'язане з тими самими системними ризиками, що загрожують традиційним фінансам. З другого боку, хоча DAI і децентралізована, вона все ще неефективна з погляду капіталу і може задовольнити поточний ринковий попит.

З моменту створення Tether та DAI з'явилося кілька децентралізованих протоколів стейблкоїнів, спрямованих на підвищення децентралізації, стабільності цін та ефективності використання капіталу. Ми називаємо ці протоколи алгоритмічними стейблкоїнами.

Поряд із запуском проєктів DeFi та швидким упровадженням інновацій у наявні проєкти спостерігається збільшення кількості зломів та експлойтів, що призводять до значних втрат. Розвиток DeFi неминуче зупиниться, якщо екосистема буде розрахована лише на тих, хто сприймає високі ризики. Наявність надійної системи страхування є важливим заходом для зниження ризиків, які користувачі беруть на себе при взаємодії з програмами DeFi, тим самим привертаючи до цього простору увагу більшої кількості користувачів.

За рахунок заявленої забезпеченості стейблкоїнів резервами у фіатній валюті такі віртуальні активи низьковолатильні, що підвищує на них попит для переміщення активів як усередині однієї країни, так і для транскордонних переказів. За рахунок таких властивостей у злочинній діяльності стейблкоїни, особливо USDT блокчейн-платформи Tron, використовують для ухилення від санкцій (транскордонні перекази за допомогою неліцензованих ППВА), кіберзлочинності та в корупційних злочинах – хабарництві й розкраданні.

Нещодавні консультації FATF з криптогалуззю підкреслюють цінність інформаційно-роз'яснювальної роботи з державним сектором та навчання з цього питання, а також конкретних інструментів і методів, таких як моніторинг і блокування GeoIP (VPN) та аналіз шаблонів за допомогою аналітичних інструментів блокчейну, щоб допомогти у перевірці санкцій на трансакції у ВА. У майбутньому швидке впровадження Правила подорожей Рекомендації 16 FATF стає життєво важливим компонентом для підтримки ефективної ідентифікації контрагентів та належної перевірки санкцій.

Крім того, FATF визнає можливе зловживання ВА для ухилення від санкцій. Нещодавній діалог FATF показує, що ухилення від санкцій за допомогою ВА не відбувається у великому масштабі через обмеження ліквідності, з чим ми можемо посперечатись із доказовою базою аналітичного дослідження про виведення активів громадянами рф на початку неспровокованої російської агресії в Україні. Цьому дослідженню ми присвятимо окремий розділ нашого дослідження.

Водночас, з огляду на можливість зміни цієї загрози та у світлі недавньої глобальної уваги до санкцій, багато юрисдикцій FATF нещодавно вжили заходів, щоб підтвердити своєму приватному сектору, що вимоги цільових фінансових санкцій (TFS, англ. Targeted financial sanctions) застосовуються до ВА та ППВА.

Подібним чином FATF реагує на постійну і зростаючу загрозу злочинного використання ВА для отримання та відмивання незаконних доходів від атак програм-вимагачів. Діалог FATF із галуззю з цього питання у квітні 2022 р. підкреслює, що злочинці продовжують покладатися на невелику групу ППВА, які не відповідають вимогам, а іноді є співучасниками, щоб відмити свої доходи від атак програм-вимагачів, хоча вони часто використовують централізовані, сумісні ППВА на останніх стадіях ВК, щоб переказати в фіатну валюту.

Кіберзлочинці, які використовують програми-вимагачі, дедалі частіше використовують міксери, тумблери та конфіденційні монети для отримання й відмивання своїх незаконних доходів, хоча галузеві діалоги свідчать про те, що

біткоїн залишається найпоширенішим віртуальним активом для цієї мети (Додаток А. Типологічні дослідження А 10).

Щоб боротися з цими загрозами, як юрисдикції, так і галузь під час останніх консультацій визнали можливості аналітики блокчейнів, щоб допомогти відстежити відмивання грошей, пов'язане з програмами-вимагачами. Інструменти блокчейну підтримували та інформували про успішні випадки правозастосування, цільові фінансові санкції та інші дії для припинення фінансування програм-вимагачів. Однак індустрія визнала, що деякі проблеми залишаються, зокрема через використання конфіденційних монет, зміни блокчейнів через незареєстровані ППВА та нехостингові гаманці. Для усунення цих загроз у майбутньому важливо, щоб як юрисдикції, так і приватний сектор застосовували стандарти FATF щодо ВА та ППВА, включно з Правилом подорожей, щоб дозволити приватному сектору виявляти незаконних осіб і підозрілі трансакції.

З функціональної точки зору протоколи DeFi – це місця для торгівлі криптовалютними токенами та похідними інструментами або передачі їх у кредит. Але на відміну від традиційних криптобірж на кшталт Coinbase чи Kraken протоколи DeFi існують у вигляді безлічі вузлів, що перевіряють і координують, а не у формі єдиного порталу і механізму зіставлення, керованого зареєстрованою юридичною особою. І, теоретично, протокол DeFi може існувати без формального керівництва, з яким зазвичай взаємодіють регулятори. Це особлива проблема для державних наглядових органів, оскільки багато наявних систем DeFi розроблено без будь-яких вимог до користувачів до розкриття своєї особистості.

Знову-таки, це створює помітний контраст із такими організаціями, як централізовані криптобіржі Coinbase і Kraken, що мають рішення політик ЗСК. Це важливо, адже DeFi є потенційним вектором для всіх трьох ключових ризиків, які фінансові регулятори повинні контролювати:

– злочинна діяльність, включно з ВК/ФТ та ухиленням від сплати податків;

– шахрайство, яке широко використовувалося в серії підроблених або шахрайських продажів токенів під час буму первинних пропозицій монет (ICO) у 2017 р., чому сприяли ранні версії DeFi;

– системний ризик (DeFi та криптовалюта, ймовірно, все ще недостатньо великі або впливові, щоб викликати ширше фінансове "зараження" серед населення у разі великого краху ринку або збою системи, і тому більше не потрібно брати участь у спекуляціях, щоб передбачити такий рівень впливу в майбутньому).

Наглядові органи повинні шукати заходи зменшення ризиків до надання реєстрації/ліцензування та на постійній основі. Знизити ризики цих продуктів після їх запуску буде складніше.

Традиційно регулюючі органи значною мірою покладаються на осіб, які керують торговими послугами, щоб контролювати ці ризики, відстежуючи клієнтів та підозрілі активності на своїх платформах. Самі лідери традиційних фінансових послуг іноді стають стрижнем правозастосування, який національні та міжнародні регуляторні й правоохоронні органи активно використовують.

Особливої уваги в контексті врегулювання й визначення ризиків потребує взаємодія криптобізнесу із секторами реальної економіки, так звані шлюзи обміну ВА на фінансові інструменти, цінні папери, нерухомість, майнові права. Важливо забезпечити гармонійну співпрацю наглядових органів реального сектору економіки з наглядовим органом ринку ВА, наявність якого рекомендована міжнародними стандартами [258].

Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) оприлюднила перший набір пріоритетів з ПВК/ФТ. Згідно із заявою FinCEN від 30.06.2021, пріоритети спрямовані на найсерйозніші загрози ВК/ФТ, з якими стикаються США [268].

Треба розуміти, що фінансові установи не зобов'язані коригувати свої комплаєнс-програми, допоки остаточні положення не набудуть чинності. Однак їм настійно рекомендується розпочати процес розгляду цих пріоритетів, таким чином визначаючи необхідні коригування на основі ризиків.

Крім того, вказані пріоритети переглядатимуться принаймні раз на чотири роки й узгоджуватимуться з появою нових та поточних загроз для критично важливої фінансової інфраструктури. Оскільки фінансові організації застосовують ці пріоритети до своїх бізнес-моделей, клієнтів, продуктів, послуг, включно з іншими банківськими каналами та платформами, географічними регіонами, вони помітять, що істотно розширені типології перетинатимуть кілька пріоритетів.

Станом на 2024 р. злочин ВК посідає третє місце серед «індустрій» світу, із щорічним обсягом у близько 2 трлн дол. США [272]. Ця величезна сума підживлює глобальну злочинність і становить значну загрозу світовій економіці. Щоб протидіяти цьому, регулятори запровадили суворі заходи для фінансових установ, які перебувають на передовій боротьби з фінансовими злочинами.

Хоча ПВК/ФТ є відповідальністю компаній, на команду з дотримання норм (compliance team) припадає значна частина цього тягаря. Вони повинні вчасно виявляти ознаки ВК та перші прояви фінансових злочинів для ефективного втручання.

Ознаки ВК вказують на можливі відповідні дії. Сьогодні злочинці використовують складні схеми, тому фінансовим установам важливо відстежувати нові тенденції та ознаки, які можуть свідчити про злочинну діяльність. У своїх рекомендаціях FATF надає уявлення про стратегії, які злочинці використовують для ВК. Це часто здійснюється через традиційні фінансові установи та ППВА, наприклад:

- використання корпоративних рахунків легальних бізнесів для проведення особистих трансакцій;
- придбання цінних активів за допомогою незаконних коштів;

- створення фіктивних компаній для приховування власності на активи чи здійснення операцій із відмитими грошима;
- використання фальшивих особистостей для управління незаконними коштами з приховуванням справжніх учасників;
- надання позик із відмитих коштів злочинцям, що надає угоді легального вигляду.

Наведемо ключові ознаки відмивання грошей на ринку віртуальних активів, на які слід звертати увагу відповідно до рекомендацій FATF у 2024 р.:

1. *Підозрілі або незрозумілі джерела коштів.* Незрозумілі джерела коштів є однією з найбільших ознак ВК. Наприклад, надходження великих сум на біржові/банківські рахунки чи криптогаманці без чіткого пояснення джерела коштів можуть свідчити про спробу легалізувати кошти, отримані незаконно. Також викликають занепокоєння трансакції, пов'язані з адресами чи рахунками, які фігурують у відомих злочинних схемах.

2. *Незвичні трансакції та шаблони.* Великі готівкові депозити та виведення коштів у готівку, часті операції через різні банківські рахунки, особливо в різних юрисдикціях, є серйозними сигналами про можливе ВК.

3. Неповна або недостовірна інформація. Якщо клієнт не надає повної інформації щодо вимог комплаєнсу (процедур ЗСК) або вказує фальшиві дані, це може свідчити про спробу приховати свою особу чи джерело коштів.

4. Швидке зняття готівки. Швидкі зняття готівки після депозитів можуть свідчити про ВК шляхом «заплутування» з метою маскування джерел походження коштів.

5. *Часті придбання віртуальних активів.* Складність відстеження операцій із ВА робить їх привабливими для ВК. Установи мають звертати увагу на клієнтів, котрі одразу конвертують великі суми у ВА.

6. *Трансакції з особами чи певними локаціями з показником високого ризику.* Співпраця з особами зі списків санкцій або з високоризикованих регіонів потребує додаткового розслідування.

7. *Трансакції у високоризикових індустріях*. Операції у сферах онлайн-азартних ігор, недозволених товарів в Даркнеті, торгівлі зброєю, наркотиками, людьми, мистецтва та індустрії для дорослих мають бути під особливим моніторингом.

8. *Кримінальне фінансове минуле.* Клієнти з попередніми правопорушеннями, пов'язаними з фінансовими злочинами, становлять підвищений ризик рецидиву.

9. *Негативне висвітлення в медіа*. Клієнти, про яких пишуть у негативному контексті, становлять підвищений ризик для фінансових установ і потребують частих перевірок.

10. *Присутність у списках санкцій.* Наявність клієнта в санкційних списках вказує на високий ризик ВК.

З огляду на попередньо викладені матеріали цього дослідження ми додамо ще три ознаки злочину ВК:

11. Різкі зміни ціни на ВА, які не відповідають загальному ринковому тренду (котируванням на криптобіржах).

12. Короткострокова активність на криптогаманцях із нульовим залишковим балансом та взаємодія між криптогаманцями з такою ознакою

13. Постійне користування анонімізаторами – міксерами, монетами з підвищеною анонімністю та іншими способами приховування інформації про адреси криптогаманців і криптотрансакції.

Саме ці ознаки ми застосуємо в розрахунках ризиків використання ВА в злочині ВК/ФТ у наступному розділі. Однак ми не зазначили в цьому розділі ризиків обороту цифрових валют центральних банків, щоб охопити кластерно-порівняльним аналізом всі типи цифрових активів.

Цифрові валюти центральних банків (CBDC) та інша публічна інфраструктура здатні сприяти розмаїттю фінансової екосистеми, що підтримує інновації в інтересах суспільства. На міжнародному рівні центральні банки можуть об'єднувати свої оптові CBDC безпосередньо через грошові резерви в

кількох валютах. Це можливо завдяки використанню дозволеного розподіленого реєстру, що дає змогу банкам і платіжним постачальникам застосовувати технологію getranger — 10 центральних банків демонструють, що такі механізми можуть забезпечити швидші, дешевші та прозоріші транскордонні платежі [273].

Дизайн CBDC може мати різні варіанти — від централізованих баз даних до розподілених реєстрів та систем, що працюють на основі токенів. Проте основними ризиками для будь-якого дизайну CBDC є кібербезпека та конфіденційність.

Перш ніж робити висновки про ризики кібербезпеки та конфіденційності, важливо проаналізувати кожен варіант дизайну. Також слід порівняти ці конструкції з наявною фінансовою системою, щоб визначити, чи здатні нові технології забезпечити безпечніші варіанти.

1) Централізоване збирання даних.

Деякі запропоновані варіанти дизайну CBDC (особливо для роздрібних CBDC) передбачають централізований збір даних про трансакції, що може призвести до значних ризиків конфіденційності та безпеки.

2) Прозорість і конфіденційність.

Проєкти, що прагнуть зберегти конфіденційність (включно з тими, що використовують спеціалізовані криптографічні методи), часто стикаються з питанням зниження прозорості для регуляторів. Регуляторні органи зазвичай потребують певного рівня доступу до даних для виявлення підозрілих трансакцій, що дає їм змогу запобігати ВК/ФТ та іншим незаконним діям.

Останнім часом стало зрозуміло, що деякі центральні банки вважають цифрові валюти (CBDC) надто ризикованими з точки зору кібербезпеки та захисту даних. Водночас уряди мають широкий вибір варіантів їхньої реалізації, включно з новими підходами, які ще не пройшли достатніх тестувань у пілотних проєктах. Кожен із цих варіантів має переваги та недоліки, зокрема щодо продуктивності, рівня безпеки та конфіденційності.

Фрагментований підхід до створення CBDC на міжнародному рівні може призвести до проблем із сумісністю та транскордонними кіберризиками. Очевидно, що країни зосереджені на внутрішньому застосуванні, не приділяючи достатньої уваги транскордонному регулюванню, сумісності та стандартизації.

Країни повинні обирати дизайн CBDC, виходячи з національних потреб та пріоритетів політики. З огляду на аналіз цих компромісів CBDC не є автоматично безпечнішими або небезпечнішими за наявні системи. З огляду на важливість кібербезпеки при їх проєктуванні це не повинно перешкоджати розгляду можливості створення та тестування CBDC.

2.2. Математична модель оцінки ризику використання цифрових активів в легалізаційних та кримінальних операціях

У відповідь на нагальну потребу країн упровадити ефективні заходи для запобігання злочинному та терористичному використанню криптосектору FATF запровадила глобальні стандарти для ВА та ППВА. Зокрема, FATF зазначила, що швидкий розвиток, зростання функціональності, розширення використання та глобальний, транскордонний характер ВА роблять невідкладними дії з боку країн щодо зниження ризиків ВК/ФТ, пов'язаних із діяльністю ВА та ППВА, пріоритетним завданням. Останні висновки FATF свідчать, що країни продовжують зазнавати труднощів у виконанні основних вимог, таких як проведення оцінки ризиків, прийняття законодавства для регулювання ППВА та здійснення наглядових перевірок.

Для зниження потенційно значних ризиків ВК/ФТ, які виникають у секторі ВА, важливо, щоб країни запровадили ефективний нагляд за ризиками у сфері

ПВК/ФТ, орієнтуючись на ризики в цьому секторі. У багатьох випадках наглядові оцінки ризику ВК/ФТ ще не були проведені й бракує можливостей для розроблення відповідних наглядових інструментів для цих оцінок.

Нові ризики виникли на додаток до зручностей, які принесли швидкі досягнення в галузі інформації та технологій. Зловмисники змінили свою мету, методи та тип атак завдяки швидкій адаптації до нових технологій [252; 253]. Для протидії цим ризикам необхідне нове покоління процедур безпеки для державних організацій і установ, комерційних компаній та звичайних користувачів інтернету. Набір процедур та алгоритмів, відомий як методи класифікації, застосовується для групування даних у визначені класи або категорії [274]. Кожен елемент у вибірці даних класифікується за допомогою класифікації в один із наперед визначених класів або груп. Для передбачення категоріальних міток створюється модель, або класифікатор, для виконання завдання аналізу даних класифікації.

Мета класифікації — точно передбачити клас для кожного прикладу у вибірці даних. Початковою точкою для завдання класифікації є збір даних, що містять відомі класи. Наприклад, використовуючи спостережувані дані щодо кількох позичальників із часом, можна створити модель класифікації, яка прогнозуватиме кредитні ризики [274]. Дискретні класифікації не мають порядку. Для прогнозних моделей із числовими цілями замість класифікації використовується регресійний аналіз.

Криптовалюти зазвичай класифікуються відповідно до їхніх відносних розмірів на ринку, з використанням ринкової капіталізації, яка визначається шляхом множення їхньої поточної ціни на циркулюючу пропозицію. Зміни в циркуляційній пропозиції та коливання цін можуть спричиняти волатильність у рейтингах ринкової капіталізації. Регресійний аналіз визначає, чи є змінні статистично важливими для пояснення варіацій залежної змінної, аналізуючи коефіцієнти незалежних змінних. Це потужна та гнучка технологія, що застосовується у багатьох різних галузях. Він пропонує систематичний підхід до

прогнозування результатів, розуміння та аналізу взаємодій між змінними, а також сприяє прийняттю рішень.

Незважаючи на те, що дані про криптовалюти, зокрема біткоїн, доступні для всіх, анонімність цих даних ускладнює можливість пов’язати ярлики шахрайських або незаконних трансакцій з мережами. Техніки класифікації — різновид керованого машинного навчання, що використовується для категоризації даних у заздалегідь визначені класи або мітки. Ці техніки часто застосовуються для таких завдань, як розпізнавання зображень, виявлення спаму в електронних листах, аналіз настроїв і виявлення шахрайства. Р. М. Азіз та ін. [275], використовуючи метод Light Gradient Boosting Machine (LGBM) для ефективного виявлення шахрайських трансакцій, порівнюють свої вимірювання з методом LGBM. Техніки екстремального градієнтного бустингу (XGBoost) і LGBM демонструють найвищу точність, причому LGBM працює дещо краще, досягаючи 98,60 % для наданого набору даних. Завдяки подальшому налаштуванню гіперпараметрів LGBM досягається точність 99,03 %. А. Дутта та ін. [276] прагнуть знайти докази шахрайства та обману в трансакціях Ethereum. Використовуючи узагальнені карти Люрота, штучна нейронна мережа ChaosNet дає змогу досягти цієї функціональності. Завдяки високим рівням хаотичної активності серед нейронів, ChaosNet застосовує деякі з найкращих характеристик біологічних нейронних мереж для виконання складних завдань класифікації, що перевершують традиційні нейронні мережі (CNN). Вона вимагає значно меншої кількості навчальних даних.

З метою виявлення шахрайства в блокчейні Нрусінгха Тріпаті та ін. [277] використовували різні методи класифікації, такі як логістична регресія (LR), класифікатор випадкових лісів (RF), метод найближчих сусідів (KNN), адаптивний бустинг (AdaBoost) та екстремальний градієнтний бустинг (XGBoost). Використаний ними набір даних містить рядки з відомими шахрайськими трансакціями, а також трансакціями, здійсненими за допомогою криптовалюти Ethereum. Важлива модель «XGBoost» виявляє варіації, які

можуть привернути увагу та запобігти проблемам. Вони застосували різні підходи до класифікації щодо виявлення і запобігання шахрайству з криптовалютами.

Шахрайство з криптоактивами, за оцінками OFAC, є одним із п'яти найбільших за обсягами напрямів злочинної діяльності [278].

Дослідженню шахрайства з криптоактивами присвячено багато міжнародних наукових досліджень, оскільки здебільшого вони надихаються офлайновими моделями, такими як схема Понці, яка є 150-річною аферою, що імітує програми з високим доходом, дозволяючи користувачам вивести гроші лише за умови, що вони приведуть достатню кількість нових учасників, аби покрити прибуток схеми. Відповідно, раніше залучені інвестори отримують прибуток за рахунок банкрутства пізніших. Ці шахрайства шкодять репутації всій екосистемі криптовалют.

Часто способи шахрайства з криптоактивами поєднують для більшої плутанини та схожості на реальні проєкти стартапів, спекулюючи відсутністю знань з фінансової, цифрової інклюзії та інвестування пересічних інвесторів.

Наприклад, організатори платформи «Platincoin» після реєстрації інвестора в системі платформи відкривали йому особистий кабінет із криптогаманцем. Далі в цьому додатку в розділі «Торгівля» була надана можливість купити на криптобіржі стейблкоїн USDT та інші валюти. При купівлі USDT при виборі способу оплати було дозволено купити USDT у великої кількості вже зареєстрованих раніше інвесторів. На куплені та перераховані USDT до Ultimafarm.com, здійснювалась оплата ліцензії на навчання та купівлю монети Platincoin (PLC). Більше того, кожному учаснику платформи було запропоновано залучити нових вкладників та отримати бонус у вигляді 20 % вкладеної суми останнього, бонуси за залучення нараховувались у вигляді монет PLC, для зняття яких інвестори за переказом на біржу «Coincbit» мали можливість обміняти монети PLC на USDT за курсом монети (Додаток А. Типологічне дослідження А 10).

Особливістю розслідування, проведеного правоохоронними органами в співпраці з блокчейн-аналітичною компанією Global Ledger, були моніторинг і аналіз швидкого зростання та падіння ціни (волатильність) монети PLC, короткотерміновість користування криптогаманцями для операцій зі стейблкоїном USDT та зупинення активності на криптогаманцях.

Такі явища з «новими» монетами, дослідження й оцінка кредитного ризику через волатильність таких монет до стану їхньої «смерті», тобто банкрутства криптопроєкту, досліджували протягом п’яти років науковці під головуванням Діна Франзіні. Науковці проаналізували набір даних із понад 2000 криптоактивів [280].

На відміну від традиційних моделей низькочастотної волатильності, які враховують лише ціни закриття, щоденний діапазон використовує всю інформацію з традиційних щоденних наборів даних, включно з цінами відкриття, максимуму, мінімуму та закриття (OHLC, англ. Open-High-Low-Close) для кожного активу. Було проведено оцінку точності ймовірності ліквідації, розрахованої за допомогою щоденного діапазону, порівняно з різними моделями прогнозування, такими як моделі кредитного скорингу, машинного навчання та на основі часових рядів. У дослідженні розглядалися різні визначення «мертвих монет» і різні горизонти прогнозування. Результати показали, що моделі кредитного скорингу та методи машинного навчання, які враховують затримані обсяги торгів і онлайн-пошуки, були найефективнішими для короткострокових горизонтів до 30 днів. Натомість, моделі часових рядів, що використовують щоденний діапазон, виявилися більш релевантними для довгострокових прогнозів, до одного року. Додатково аналіз показав, що моделі, які використовують щоденний діапазон, заздалегідь сигналізували про ослаблення кредитної позиції платформи торгівлі криптодеривативами FTX, що подала заяву про банкрутство за Главою 11 Кодексу США про банкрутство 11 листопада 2022 р. (Додаток А. Типологічне дослідження 11)

Варто зазначити, що Семюель Бенкман-Фрід, колишній генеральний директор FTX, визнав, що приділення більшої уваги управлінню ризиками могло би потенційно запобігти краху компанії, про що він заявив 30 листопада 2022 р. [281].

На жаль, питання управління кредитними ризиками для криптоактивів не викликає великого інтересу, що відображено в обмеженій кількості академічної фінансової літератури на цю тему. Це можна пояснити двома основними чинниками: відсутністю достатніх фінансових та бухгалтерських даних і необхідністю використання іншого визначення кредитного ризику. У цьому контексті було запропоновано нове визначення кредитного ризику для криптоактивів, яке ґрунтується на їхній «смерті», що відбувається, коли ціна суттєво падає і вони стають неліквідними [282]. Варто підкреслити, що як у професійній, так і в академічній літературі немає єдиного визначення «мертвого» активу. Більше того, навіть коли криптоактив вважається «мертвим», він може все ще демонструвати незначні обсяги торгівлі (як відбувалося з токеном FTX на кінець грудня 2022 р.) або через можливість часткового повернення початкових інвестицій, або через спекуляцію на його ймовірному відновленні. Також варто зазначити, що стан «смерті» криптоактиву може бути тимчасовим, а не постійним: як показали Ніл Гендал, Дж. Т. Хемрік, Тайлер Мур і Марі Васек, деякі монети були покинуті, а потім «відроджені» до п’яти разів протягом кількох років [283].

Дослідження науковців залишають низку питань для подальших досліджень: обчислювальні труднощі, що виникли в його ході, вказують на можливість використання Баєсових методів для згладжування шумових даних та покращання обчислень моделі у випадку коротких часових рядів. Крім того, кілька випадків у їхньому емпіричному аналізі підкреслили можливість покращання прогнозів шляхом комбінування оцінок імовірності дефолту, отриманих різними методами. Усі ці питання залишаються перспективними напрямами для майбутніх досліджень.

Розглянувши науково-методологічні підходи науковців для оцінки і управління ризиками використання ВА в нелегальній діяльності ми повернулись до оцінки ризику використання ВА саме в злочині ВК, використовуючи метод експертних оцінок за методикою SEER (System for Evolutions and Review) [284, с. 43]. Зазначений метод передбачає обробку висновків експертів, отриманих через їхнє опитування. Залучення експертів як джерел інформації про майбутній розвиток об'єкта дослідження (у цьому випадку ризиків) базується на припущенні, що окремі провідні спеціалісти ринку ВА та фінансового ринку мають достатні знання для вирішення досліджуваних питань, використовуючи форсайт-підхід до прогнозування через анкетне опитування.

Варто згадати, що для розроблення Стратегії розвитку ринку віртуальних активів в Україні також було використано форсайт-підхід. Форсайт «Віртуальні активи в Україні 2030» [285] — дослідження галузі (екосистеми) ВА в Україні, її місця та перспектив у вітчизняній економіці та на світовому ринку. Він проводився в березні – травні 2021 р. й об’єднав широке коло експертів, серед яких підприємці, народні депутати, представників правоохоронних органів та органів виконавчої влади, зокрема регуляторів, Міністерства цифрової трансформації України тощо.

Також доцільним було застосувати при проведенні експертних оцінок, а саме в опитувальниках для експертів, методи класифікації, враховуючи, що в нашому дослідженні в першому розділі ми класифікували цифрові активи, а в другому розділі – види злочинної діяльності, які в значних обсягах використовують ВА, що і було запропоновано.

На додаток до оцінки інструментарію ринку ВА нас зацікавило оцінювання ризиків кількісними методами (квантифікація) із застосуванням Баєсових мереж для оцінки ризику учасників операцій з ВА відповідно до вимог політики ЗСК. Фінансова платоспроможність самих учасників операцій з ВА сприяє зниженню ризику ВК відповідно до методики проведення оцінки ризиків Світового банку, описаної в першому розділі нашого дослідження.

Баєсові мережі призначені для встановлення та аналізу причинно-наслідкових зв’язків між змінними ознаками об’єкта. Вони не потребують спеціальної обробки та тестування даних, оскільки апріорна інформація про них вдало поєднується з розвинутими методами аналізу [286].

Як метод оцінки ризиків, баєсівські методи базуються на теоремі Баєса, що обчислює ймовірність істинності гіпотези за умов обмеженої інформації про подію, відомої зі спостережень. Баєсівський підхід як альтернатива класичному статистичному підходу дає змогу точніше та повніше оцінювати моделі, надаючи належні результати у випадках, коли класичні статистичні методи мають обмежені можливості.

Класичний підхід до аналізу даних акцентує увагу на розробленні ефективних алгоритмів оцінки та дослідженні їхні асимптотичних властивостей для формування статистичного висновку на основі великих обсягів даних. Однак при роботі з короткими вибірками асимптотичні результати стають недостатньо обґрунтованими. Баєсівські методи ґрунтуються на інших теоретичних передумовах і мають інший підхід до інтерпретації істинних параметрів моделі.

Таким чином, баєсівський підхід відкриває нові широкі можливості для застосування методів математичного моделювання, а розроблені обчислювальні алгоритми на основі генерування випадкових чисел дають змогу розв’язувати поставлені задачі за допомогою сучасних обчислювальних процедур [287].

Застосування баєсівського підходу є оптимальним для аналізу ризиків використання ВА у ВК з огляду на відсутність загальнодержавних статистичних даних про операції з ВА. Водночас для оцінки фінансових показників учасників обігу ВА потрібна стандартна фінансова звітність, якої наразі теж немає в Україні за відсутності ліцензованих ППВА як офіційних джерел інформації про операції з ВА та державного регулювання ринку ВА. Тому цей метод є доцільним для експертизи операцій з ВА на предмет їхнього використання у ВК/ФТ, але за умов легалізації крипторинку.

Тому за наявності критеріїв використання ВА в злочинах ВК та експертного середовища з представників блокчейн-аналітичних компаній AMLbot, Crystal, Global Ledger, Purefi [287–290], наукової спільноти, сферою досліджень якої є ВА та ризики, пов'язані з їх обігом та правоохоронних органів, що розслідують злочини, пов'язані з використанням ВА та легалізацією доходів, отриманих злочинним шляхом.

Для точної та надійної оцінки ризику використання ВА необхідно розробити методику, яка враховуватиме коефіцієнти значущості складових ризику ВА. Це включає значущість ризиків, пов'язаних із наявністю або відсутністю ознак використання у схемах відмивання злочинних доходів, інформацію про географічне розташування учасників операцій, належність до санкційних списків, а також тип злочину, що передував відмиванню коштів.

Міжнародно-правове визначення предикатного злочину викладене в Конвенції Ради Європи про захист прав людини і основоположних свобод [297], де він описується як будь-який злочин, унаслідок якого виникають доходи, що можуть бути використані для відмивання.

У дослідженні представлено методику оцінки ризику використання ВА на основі коефіцієнтів значущості ризику [291,с. 85;294]. Відповідно до цієї методології, розрахунок ризику використання ВА здійснюється за такою формулою:

$$Rc = \sum_{n=1}^{8} Kio \times R \qquad (2.4)$$

де Rc – ризик за певними компонентами використання ВА у ВК;

Kio – коефіцієнт значущості критеріїв ризику за певними компонентами використання ВА в ВК;

R – кількість ризиків за певними компонентами використання ВА у ВК.

Для оцінки ризику використання ВА у ВК наведемо перелік ризиків, які будуть застосовані в запропонованій методиці SEER (System for Evolutions and Review) [290, с. 43]:

1. Постійне користування анонімізаторами (міксери, монети з підвищеною анонімністю та інші способи приховування інформації про адреси криптогаманців та криптотрансакції).

2. Трансакції у високоризикових індустріях (онлайн-азартні ігри, недозволені товари в Даркнеті, торгівля зброєю, наркотиками, людьми, мистецтва та індустрії для дорослих тощо).

3. Присутність у списках санкцій окремих країн та міжнародних організацій.

4. Швидке зняття готівки після серії депозитних операцій.

5. Часті придбання ВА на великі суми.

6. Різкі зміни ціни на ВА, які не відповідають загальному ринковому тренду (котируванням на криптобіржах).

7. Трансакції з особами чи певними локаціями з показником високого ризику.

8. Негативне висвітлення клієнтів у медіа.

9. Незвичні трансакції та типології використання ВА у ВК.

10. Короткострокова активність на криптогаманцях із нульовим залишковим балансом та взаємодія між криптогаманцями з такою ознакою.

11. Підозрілі або незрозумілі джерела коштів.

12. Неповна або недостовірна інформація про клієнта.

13. Кримінальне фінансове минуле клієнтів.

Для визначення критеріїв важливості кожного показника застосовується методика оцінювання порівняльної значущості окремих чинників (параметрів). Для цього було проведено опитування експертів, у якому вони оцінювали відносну важливість чинників, присвоюючи їм бали в межах від 1 до 100 (Додаток Г. Метод експертних оцінок).

Під час обробки експертних оцінок, що відображають відносну вагу окремих чинників, поряд із балами використовуються ранги. На основі матриці балів здійснено ранжування чинників, а результати відображено в матриці

рангів. Виходячи з матриці рангів, визначено стандартизований ранг. Оцінки показників стандартизованого рангу подано в табл. 2.7.

Таблиця 2.7

Матриця рангів критеріїв оцінки ризику

за ознаками використання ВА у ВК

Показник	Критерії												
	1	2	3	4	5	6	7	8	9	10	11	12	13
Бальна оцінка	100	100	90	60	70	30	90	20	80	10	70	40	50
Рейтингова оцінка	1-2	1-2	3-4	8	6-7	11	3-4	12	5	13	6-7	10	9
Стандартизований ранг	1,5	1,5	3,5	8	6,5	11	3,5	12	5	13	6,5	10	9

Джерело: Складено автором

Для визначення коефіцієнтів значущості слід оцінити відносну вагу критеріїв за допомогою індивідуального нормування та показників порівняльної важливості критеріїв. Ця вага визначається за формулою:

$$W\ \text{j} = \frac{\sum_{j=1}^{m} Wi}{\sum_{j=1}^{n}\sum_{i=1}^{m} \text{Wij}} \qquad (2.5),$$

j – вага (нормована оцінка), надана і-тим експертом j-му чиннику;

$W\ j$ – загальна вага, надана експертами j- му чиннику;

n – кількість чинників.

Зважаючи на те, що кожен експерт оцінив усі критерії, а сума відносних значень, які він призначив усім чинникам, становить 1, ця сума дорівнює загальній кількості експертів, залучених до оцінювання.

Для визначення коефіцієнтів значущості слід проаналізувати показники порівняльної важливості критеріїв за такими параметрами:

1. Сума рангів.

2. Середній ранг.

3. Середнє значення в балах.

4. Середня вага (нормована оцінка).

5. Частота максимально можливих оцінок.

6. Коефіцієнт активності експертів.

7. Амплітуда.

Сума рангів, призначених експертами *j*-му чиннику, визначається за формулою:

$$Sj = \sum_{i=1}^{m} Rij \qquad (2.6),$$

де Rij – ранг оцінки вартості відносної ваги (в балах), наданої *i*-м експертом *j*-му чиннику.

Сума рангів обчислюється для всіх критеріїв, причому зі зниженням важливості певного критерію ця сума зростає. Таким чином, менша сума рангів свідчить про більшу важливість відповідного критерію.

Середній ранг кожного критерію визначається за формулою:

$$\overline{Sj} = \frac{\sum_{i=1}^{m} Rij}{m} = \frac{Sj}{m} \qquad (2.7),$$

де Rij– ранг оцінки вартості відносної ваги (в балах), наданої *i*-м експертом j-му чиннику;

m – кількість експертів.

Порівнюючи відносну важливість критеріїв, найвищу важливість слід надати тому критерію, який має найменше значення середнього рангу. Паралельно зі значеннями середніх рангів для кожної досліджуваної складової обчислюється середнє значення в балах:

$$\overline{M}_j = \frac{\sum_{i=1}^{m} \mathrm{C}_{ij}}{\mathrm{m}_j} \qquad (2.8),$$

де C_{ij} – оцінка вартості відносної ваги (в балах), наданої і-м експертом j-му чиннику;

m_j – кількість експертів, що оцінили j-й чинник.

Показник частоти максимально можливих оцінок розраховується за формулою:

$$K_{100j} = \frac{m_{100j}}{mj} \quad (2.9),$$

де m_{100j} – показник частоти максимально можливих оцінок (100 балів), отриманих кожним чинником;

m_j – кількість експертів, які оцінили *j*-й чинник.

Активність експертів по кожному напряму визначається за допомогою коефіцієнта активності, який обчислюється за такою формулою:

$$K_{aoj} = \frac{m_j}{m} \quad (2.10),$$

де m_j – кількість експертів, які оцінили j-й чинник;

m – загальна кількість експертів.

Оскільки оцінки, надані кожним експертом для окремого критерію, зазвичай різняться, потрібно визначити амплітуду оцінок, який обчислюється за такою формулою:

$$L_j = C_{jmax} - C_{jmin} \quad (2.11),$$

де C_{jmax} та C_{jmin} – відповідно максимальна та мінімальна оцінки, поставлені експертом m_j-му чинники.

Результати оцінювання показників порівняльної важливості критеріїв наведено в табл. 2.8.

Таблиця 2.8

Оцінювання показників порівняльної важливості критеріїв

Показник		Сума рангів	Середній ранг	Середнє значення в балах	Частота максимально можливих оцінок	Середня вага (нормована оцінка)	Коефіцієнт активності експертів	Розмах
КРИТЕР ІЇ	1	595.0	17.5	88.235	0.3236	0.029	1	30
	2	595.0	17.5	96.765	0.6765	0.032	1	10
	3	596.0	17.52	90.882	0.3530	0.030	1	30
	4	589.5	17.33	48.529	0	0.016	1	50
	5	610.8	17.96	67.941	0	0.023	1	30
	6	582.0	17.11	37.647	0	0.013	1	30
	7	595.0	17.5	90.588	0.2353	0.030	1	20

Продовження таблиці 2.8

	8	535.5	15.75	25.882	0	0.009	1	30
	9	620.0	18.23	81.765	0	0.027	1	20
	10	425.0	12.5	16.765	0	0.006	1	20
	11	598.5	17.60	64.706	0	0.022	1	50
	12	595.0	17.5	54.412	0	0.018	1	40
	13	572.0	16.82	50.882	0	0.017	1	50

Джерело: Складено автором

Для оцінки достовірності обраної методології було проведено аналіз ступеня узгодженості думок експертів та їхньої кореляції, оскільки прийняття остаточного рішення щодо важливості чинників можливе лише за умови достатнього рівня узгодженості думок серед експертів. Ступінь узгодженості оцінок експертів визначався за допомогою коефіцієнта конкордації Кендала [295, с. 78]. З урахуванням того, що в матриці рангів присутні стандартизовані ранги, коефіцієнт конкордації обчислюється за формулою:

$$\begin{cases} K_{\text{кон}} = \dfrac{12\sum_{j=1}^{n} d_j^2}{m^2(n^3-n)-m\sum_{i=1}^{m} T_i} = 0{,}852 \\ d_j = S_j - \dfrac{\sum_{j=1}^{n} S_j}{n} \\ S_j = \sum_{i=1}^{m} R_{ij} \\ T_j = \sum_{l=1}^{L}(t_l^3 - t_l) \end{cases} \quad (2.12),$$

де l – кількість груп зв'язаних рангів;

t_l – кількість зв'язаних рангів у кожній групі.

Результати розрахунку компонентів коефіцієнта конкордації наведено в табл. 2.9.

Коефіцієнт конкордації змінюється в межах від 0 до 1. Чим більше значення має коефіцієнт конкордації, тим вищий ступінь узгодженості думок експертів (табл. 2.9).

Таблиця 2.9.

Розрахунок компонентів коефіцієнта конкордації

Показник	Критерії												
	1	2	3	4	5	6	7	8	9	10	11	12	13
S_j	595.0	595.0	595.0	595.0	595.0	595.0	595.0	595.0	595.0	595.0	595.0	595.0	595.0
d_j	4.1	4.1	5.1	-1.4	19.9	-33.4	4.1	4.1	4.1	17.3	-34.7	4.1	2.8
d_j^2	16.87	16.87	25.67	1.94	359.09	1115.1	16.87	16.87	16.87	299.59	1203.61	16.87	6.69

Джерело: Складено автором

Статистичну значущість коефіцієнта конкордації було перевірено за допомогою критерію Пірсона:

$$\chi_p^2 = \frac{12\sum_{j=1}^{n} d^2}{\left[mn(n+1) - \frac{1}{n-1}\sum_{i-1}^{m} T_j\right]} = 347{,}65 \qquad (2.13)$$

Критерій узгодженості Пірсона — один із найвідоміших критеріїв, що використовується для перевірки гіпотези про закон розподілу. Ґрунтується на групованих даних. Будь-яка випадкова величина задається своїм розподілом імовірностей. Якщо χ є випадковою величиною, його розподіл ставить у відповідність відрізкам [a, b] імовірність Pr[a ≤ χ ≤ b], тобто ймовірність, що випадкова величина χ набуде значення з інтервалу [a, b]. Розподіл імовірностей величини χ може бути описаний своєю функцією розподілу ймовірностей F(x), що визначається, як $F(x) = Pr[\chi \leq x]$, для усіх *x* з *R*, [290; 291].

У нашому випадку, розрахункове значення χ_p^2 та χ_t^2 для *n-1*, тобто 12 ступенів свободи та будь-якої довірчої ймовірності (P = 0,95 та P = 0,99), є меншим за отриману величину, $P = 0{,}95 - \chi_t^2$, де $\chi_p^2 \chi_t^2$, що підтверджує правильність гіпотези про узгодженість позицій експертів щодо ранжування критеріїв 1–13. Це свідчить про значущість коефіцієнта конкордації та підтверджує достовірність методології розрахунку коефіцієнтів значущості ризику.

Запропонований методичний підхід до оцінки ризику за ознаками використання ВА у ВК забезпечує об'єктивну оцінку рівня ризику з урахуванням коефіцієнта його значущості. Система управління ризиками легалізації (відмивання) доходів, отриманих незаконним шляхом, розроблена на основі цієї методології, дасть змогу ефективно управляти зазначеними ризиками та зменшувати їх до мінімуму. Загалом, що ефективнішими та досконалішими є методи дослідження оцінки ризиків, то якіснішою буде система ПВК/ФТ та меншою ймовірність залучення учасників ринку ВА до процесів легалізації (відмивання) незаконно отриманих доходів.

Для виявлення і припинення потоків незаконних коштів через різні канали необхідно впроваджувати заходи протидії фінансуванню злочинних угруповань не лише всередині країни, а й за її межами. Відмивання нелегальних коштів, «тінізація» економіки та фінансування тероризму негативно впливають на економічну безпеку держави, спричиняють соціальний дисбаланс. У світовій економічній науковій літературі вчені та дослідники приділяють увагу кількісному виміру процесів і дій, пов'язаних із відмиванням незаконних коштів. Однак через прихований та непомітний характер цих процесів оцінка ефективності, достатності, результативності та адекватності таких моделей є складним і проблемним завданням.

Для вивчення глобальних процесів відмивання коштів і доходів, отриманих від операцій транснаціональної злочинності, які циркулюють через світову фінансово-економічну систему, а також для оцінки впливу операцій з ВА на стійкість фінансової системи ефективність економічної безпеки та розрахунок ризиків у ППВА та фінансових установах було розроблено відповідні моделі.

Найбільш відомими та широко використовуваними є економетричні моделі оцінки ризиків (методи експертних оцінок), стрес-тестування ліквідності (оцінка кредитного ризику) [276; 277] та структуроване моделювання (методи класифікації) [278].

Особливу увагу науковці приділяють гравітаційному моделюванню, шо, як зазначають дослідники [296; 297; 298], популярне в багатьох країнах. Воно використовується в соціальних і економічних науках для прогнозування та опису специфічних форм поведінки на основі закону гравітації Ісаака Ньютона. Гравітаційні моделі дають змогу оцінювати потоки між різними місцями, вказуючи на аномалії в рівнях потоків.

Модель *Walker Gravity Model* [299] стала першою глобальною моделлю оцінки процесів ВК, базованою на гравітаційній концепції, популярній у торгівлі. Ця модель оцінює світові потоки нелегальних коштів та визначає географію їхнього походження для маскування законного джерела.

Інша модель, *Isis Economic Model* [300], ґрунтується на концепції територіального управління та здатна забезпечувати фінансово-економічну самодостатність і різноманітність ресурсів, де основою є капітал країни, що становить джерело фінансування внутрішніх і зовнішніх процесів, зберігаючи стабільну цінність фінансових ресурсів у будь-який час.

Для проведення дослідження було сформовано набір даних щодо діяльності 65 глобальних криптобірж (ППВА) за 2024 р. [301]. Цей набір є статистичною інформацією, отриманою з відкритих джерел та з використанням блокчейн-аналітичного програмного забезпечення компаній AMLbot, Crystal, Global Ledger, Purefi [287–290]. Було обрано 6 показників: К1 — частка операцій з ВА, розмічених за ознаками високоризикових операцій (шахрайські азартні ігри; вимагання; санкції; шахрайство; експлуатація дітей; ринки та сервіси Даркнету; фінансування тероризму; крадіжки; виконавчі дії правоохоронних та судових органів влади); К2 — частка операцій ВА, розмічених за ознаками уникнення санкцій; К3 — частка операцій ВА, розмічених за ознаками злочину відмивання коштів (ВК); К4 — криптовалютні нелегальні послуги; К5 — частка операцій з інструментами анонімізації від загальної суми надходжень (міксери, тумблери та інші сервіси змішування трансакцій з ВА); К6 — частка операцій з

інструментами анонімізації від загальної суми видатків (міксери, тумблери та інші сервіси змішування трансакцій з ВА).

Розглянемо методику розрахунку кожного з числових показників діяльності криптобірж:

– К1 — частка операцій з ВА, розмічених за ознаками високоризикових операцій, обчислюється за формулою:

$$К1 = \frac{ВРО}{ЗКО}, \qquad (2.14),$$

де ВРО — кількість операцій з ВА, розмічених за ознаками високоризикових операції; ЗКО — загальна кількість зареєстрованих операцій з ВА.

Цей показник дає змогу оцінити якість розмітки операцій із ВА за ознакою високоризиковості (ВРО), який є менш формальним до ризику злочину ВК, ніж розмічені операції за критерієм ВК, і, відповідно, є більш ризиковим для криптобіржі;

– К2 — кількість операцій з ВА, розмічених за ознаками обходу санкцій;

– К3 — кількість операцій з ВА, розмічених за ознаками злочину ВК;

– К4 — кількість наданих криптовалютних нелегальних послуг;

– К5 — частка операцій з інструментами анонімізації від загальної суми надходжень (міксери, тумблери та інші сервіси змішування трансакцій з ВА);

– К6 — частка операцій з інструментами анонімізації від загальної суми видатків (міксери, тумблери та інші сервіси змішування трансакцій з ВА).

Показники К1–К4 взято з блокчейн-аналітичного програмного забезпечення компаній Crystal за двома криптоактивами – біткоїн (BTC) як високоволатильна криптовалюта та доларовий стейблкоїн на блокчейн-платформі як найбільш застосовуваний у цифровій економіці забезпечений фіатними резервними валютами віртуальний актив. Показник К5 дає змогу

оцінити обсяги криптоактивів, джерела походження яких свідомо були приховані. Показник К6 допомагає оцінити обсяг криптоактивів, відправлених з криптоадрес осіб, котрі прийняли рішення використати інструменти анонімізації. Цей показник є базовим індикатором ризику можливого залучення криптобіржі до «конвертаційної» схеми з метою ВК.

Для оцінки ризику ВК пропонується методика, що базується на гравітаційному моделюванні.

Перший етап передбачає нормалізацію даних для другого, третього та четвертого показників, оскільки вони мають різні одиниці вимірювання. Їх слід привести до значень у діапазоні від 0 до 1. Важливо також урахувати, що показники по-різному впливають на ризик ВК. Зокрема, збільшення значення стимуляторів сприяє покращанню ситуації, тобто зниженню рівня ризику, і навпаки. Коли збільшення показника погіршує ситуацію та підвищує ризик, ідеться про дестимулятори. Для нормалізації використовується рівняння абсолютної нормалізації (2.15), яке підходить для обробки як стимуляторів, так і дестимуляторів [286].

$$Xij^{+} = \frac{Xij}{Xmaxj},\ Xij^{-} = \frac{Xminj}{Xij} \qquad (2.15),$$

де X_{ij}^{+} та X_{ij}^{-} – нормалізоване значення *j*-го показника характеристики рівня ризику ВК, як для стимуляторів (+), так і для дестимуляторів (–) та *i*-го показника розглянутої криптобіржі;

X_{ij} – емпіричне значення *j*-го показника рівня ризику легалізації для *i*-ї криптобіржі;

$X_{\min j}$ – мінімальне значення *j*-го показника рівня ризику легалізації серед усіх криптобірж, що досліджуються;

$X_{\max j}$ – максимальне значення *j*-го показника рівня ризику легалізації серед усіх криптобірж, що досліджуються.

На другому етапі реалізації методики за допомогою методу головних компонент визначаються вагові коефіцієнти для обраних показників. Послідовність виконання етапу така:

1) за допомогою програмного пакета Statistica 13.0 (Statistica, Multivariate Exploratory Techniques, Principal Components & Classification Analysis)[1] [302] побудувати *графік кам'янистого осипу*, таблицю власних значень та таблицю факторних навантажень;

2) на основі *графіка кам'янистого осипу* визначити релевантні фактори, сумарна дисперсія яких становить не менше 70%;

3) обчислити суму добутків факторних навантажень на дисперсію відповідних факторів (графа 4 табл. 2.4);

4) визначити вагові коефіцієнти пріоритетності показників ризику ВК з використанням ВА криптобіржами за формулою (2.15) (графа 5 табл. 2.10).

Таблиця 2.10

Проміжні розрахунки обчислення вагових коефіцієнтів показників оцінювання рівня ризику ВК

	Фактор 1	…	Фактор М	Сума добутків факторних навантажень на дисперсію впливу відповідних факторів	Ваги показників
	1	2	3	4	5
X_1	f_{11}	…	f_{1m}	$\sum_{k=1}^{m} {f_1}^k {\sigma_1}^2$	$\frac{\sum_{k=1}^{m} {f_1}^k {\sigma_1}^2}{\sum_{j=1}^{n} {f_1}^k {\sigma_1}^2 \sum_{k=1}^{m} {f_1}^k {\sigma_1}^2}$
…	…	…	…	…	
Xn	f_{1n}	…	f_{mn}	$\sum_{k=1}^{m} {f_m}^k {\sigma_1}^2$	$\frac{\sum_{k=1}^{m} {f_n}^k {\sigma_1}^2}{\sum_{j=1}^{n} {f_1}^k {\sigma_1}^2 \sum_{k=1}^{m} {f_n}^k {\sigma_1}^2}$
…	…	…	…	…	

[1]Пакет STATISTICA – це універсальний пакет статистичного аналізу, в якому реалізовані основні математичні методи аналізу даних. Розробником пакета є фірма StatSoft, Inc (США). У 2014 р. її поглинула корпорація Dell, яка включила пакет STATISTICA до складу власної лінійки програмного забезпечення проблематики великих даних. STATISTICA дає змогу проводити різні процедури (модулі) оброблення статистичних даних (у термінології програми – аналізи): 1. Розрахунок описових статистик; 2. Аналіз динамічних рядів і прогнозування; 3. Множинна регресія; 4. Дискримінантний аналіз; 5. Аналіз відповідностей; 6. Кластерний аналіз; 7. Факторний аналіз; 8. Дисперсійний аналіз і та ін.)

Продовження таблиці 2.10

Xj	f_{1j}	…	f_{mj}	$\sum_{k=1}^{m} {f_n}^k {\sigma_1}^2$	$\frac{\sum_{k=1}^{m} {f_j}^k {\sigma_1}^2}{\sum_{j=1}^{n} {f_1}^k {\sigma_1}^2 \sum_{k=1}^{m} {f_j}^k {\sigma_1}^2}$
Дисперсія впливу факторів	$\sigma_1{}^2$	…	$\sigma_m{}^2$		

Джерело: Складено автором

Отже, формула для розрахунку вагових коефіцієнтів пріоритетності показників оцінки ризику ВК з використанням ВА криптобіржами має такий вигляд:

$$\omega_j = \frac{\sum_{k=1}^{m} f_{jk} {\sigma_k}^2}{\sum_{j=1}^{n} \sum_{k=1}^{m} f_{jk} {\sigma_k}^2} \ , \qquad (2.16) \ ,$$

де ω_j – ваговий коефіцієнт пріоритетності j-го показника оцінювання ризику ВК з використанням ВА криптобіржами;

f_{jk} – значення факторного навантаження k-го фактору в розрізі j-го показника;

$\sigma_k{}^2$ – дисперсія впливу k-го фактора.

Після визначення вагових коефіцієнтів на третьому етапі розраховується інтегральний показник кількісної оцінки рейтингу криптоіндустрії щодо рівня ризику ВК за допомогою метрики Мінковського (формула (2.17)) [303], яка дає змогу враховувати вплив факторів – як стимуляторів, так і дестимуляторів:

$$\mathrm{IRA}_i = 1 + \sqrt{\sum_{j=1}^{k} \omega_j |1 - {x_{ij}}^+|^2} \sum_{j=k+1}^{n} \omega_j |1 - {x_{ij}}^-|^2, \qquad (2.17),$$

де IRA_i – інтегральний рейтинговий показник рівня ризику для i-ї криптобіржі;

ω_j – вагові коефіцієнти для j-го показника.

Зважаючи на те, що для оцінки ризику ВК і ФТ було обрано шість показників, формула інтегрального показника набуде такого вигляду:

$$\mathrm{IRAx}_i = 1 + \sqrt{\omega_1(1-x_1^{+})^{2} + \omega_2(1-x_2^{+})^{2} + \omega_3(1-x_3^{+})^{2} + \omega_4(1-x_4^{+})^{2} + \omega_5(1-x_5^{+})^{2} + \omega_6(1-x_6^{+})^{2}} \quad (2.18),$$

де x_1^{+}– фактичне значення операцій з ВА, розмічених за ознаками високоризикових операцій як стимулятор;

x_2^{+}– нормалізоване значення показника операцій з ВА, розмічених за ознаками обходу санкцій як стимулятор;

x_3^{+}– нормалізоване значення показника операцій з ВА, розмічених за ознаками злочину ВК як стимулятор;

x_4^{+}– нормалізоване значення показника наданих криптовалютних нелегальних послуг як стимулятор;

x_5^{+}– фактичне значення частки операцій з інструментами анонімізації від загальної суми надходжень (міксери, тумблери та інші сервіси змішування трансакцій з ВА) як стимулятор;

x_6^{+}– фактичне значення частки операцій з інструментами анонімізації від загальної суми видатків (міксери, тумблери та інші сервіси змішування трансакцій з ВА) як стимулятор.

Отримане значення інтегрального показника перебуватиме в межах від 0 до 1.

Четвертим етапом буде розроблення гравітаційної моделі ризику легалізації. Для цього буде використано рівняння закону гравітації в суспільних явищах, тобто формулу:

$$M_{ij} = k\frac{p_i p_j}{{d_{ij}}^{2}}, \quad (2.19),$$

де M_{ij} – показник взаємодії між об'єктами i та j;

k – коефіцієнт відповідності;

p – значимість об'єкта;

d_{ij}^{2} – відстань між об'єктами.

Такий підхід було розглянуто у праці Волтера Айзарда «Location Theory and Trade Theory: Short-Run Analysis» (1954) для моделювання міжнародної торгівлі в економіці [304].

Ризик легалізації визначається так: окремий банк «притягує» ризикові операції із силою, прямо пропорційною рейтинговій оцінці ризику ВК з використання ВА як цієї криптобіржі, так і «нормативної» криптобіржі, і обернено пропорційною квадрату «відстані» між ними (різниці між криптобіржами в процесі здійснення ризикових операцій) за формулою:

$$SVA_r = \frac{IRA_k IRA_r}{d_{kr}{}^2}, \qquad (2.20),$$

де SVA_r – кількісна оцінка сили взаємодії між розглянутою криптобіржею та *k*-ю «нормативною» криптобіржею за ризиком ВК з ВА;

IRA_k – рейтингова оцінка ризику ВК з ВА для *k*-ї криптобіржі;

IRA_r – рейтингова оцінка ризику ВК з ВА для *r*-ї криптобіржі;

d_{kr} – нормалізована різниця між «нормативною» криптобіржею *k* та криптобіржею *r*.

У рамках цього дослідження формула (20) перетворюється таким чином:

– варіант 1 (формули (2.21) та (2.22)), де як «нормативна» криптобіржа беруться показники максимально можливого значення інтегральної рейтингової оцінки рівня ризику ВК з використанням ВА, розраховані за метрикою Мінковського;

– варіант 2 (формули (2.23) та (2.24)), де як «нормативна» криптобіржа розглядаються показники середнього значення інтегральної рейтингової оцінки рівня ризику ВК з використанням ВА за метрикою Мінковського.

Для оцінки ризику ВК з використанням ВА в першому варіанті використовується формула (21):

$$SVA_r = \frac{IRA_i max IRA_{i\,i}}{d_r{}^2}, \qquad (2.21),$$

де знаменник обчислюється за допомогою формули (2.22):

$$d_r = \left| \frac{VK_r}{maxVK_r\, r} - \left(\frac{VK_r}{maxVK_r\, r}\right) \right|, \qquad (2.22),$$

де VK_r – значення власного капіталу криптобіржі k,

$\left(\frac{VK_r}{maxVK_r\, r}\right)$ – середньоквадратичне відхилення нормалізованого показника власного капіталу криптобіржі r .

Для оцінки ризику ВК з використанням ВА в другому варіанті застосовується формула:

$$SVA_r = \frac{\frac{IRA_i \sum_i IRA_i}{65}}{{d_r}^2}, \qquad (2.23),$$

де знаменник визначається за формулою (2.21):

$$d_r = \left| \frac{\sum_i r \frac{VK_r}{maxVK_r}}{62} - \frac{VK_r}{maxVK_r} - \sigma\left(\frac{VK_r}{maxVK_r}\right) \right|, \qquad (2.24),$$

де $\sum_i r \frac{VK_r}{maxVK_r}$ – середнє значення нормалізованого відносним методом (для показника стимулятора) значення власного капіталу для криптобіржі r.

У процесі створення цієї матриці результати потребують додаткової нормалізації для досягнення значень від 0 до 1. Для цього застосовується рівняння нормалізації Харрінгтона:

$$SVA_r{}' = exp\,(-exp\,exp\,(-SVA_r\,)), \qquad (2.25),$$

Отримане значення буде в межах від 0 до 1: значення, близькі до 0, свідчать про високу привабливість криптобіржі для ВК, а близькі до 1, – про низьку привабливість.

На завершальному етапі оцінки ризику легалізації кримінальних доходів через i-ту криптобіржу виникає потреба в обчисленні узагальненої характеристики ризику на основі двох розрахункових варіантів. Це здійснюється шляхом обчислення середньої арифметичної оцінки:

$$SVA_i{}^* = \frac{SVA_{1i}{}' + SVA_{2i}{}'}{2}, \qquad (2.26),$$

де SVA_i^* — узагальнена оцінка ризику використання i-ї криптобіржі для легалізації кримінальних доходів;

$SVA_{1i}{}'$ — оцінка ризику для i-ї криптобіржі за першим варіантом, заснованим на максимальних значеннях метрики Мінковського;

$SVA_{2i}{}'$— оцінка ризику для i-ї криптобіржі за другим варіантом, що ґрунтується на середніх значеннях метрики Мінковського.

Обчислення виконувалося за допомогою MS Excel на основі даних 65 глобальних криптобірж на 30 серпня 2024 р. (табл. 2.11).

Таблиця 2.11

Вхідна статистична база дослідження ризику використання банків для легалізації кримінальних доходів

Нумерація криптобірж	К1 — частка операцій з ВА, розмічених за ознаками високо-ризикових операції	К2 — кількість операцій з ВА, розмічених за ознаками обходу санкцій	К3 — кількість операцій з ВА, розмічених за ознаками злочину відмивання коштів (ВК)	К4 — кількість наданих крипто-валютних нелегальних послуг	К5 — частка операцій з інструментами анонімізації від загальної суми	К6 — частка операцій з інструментами анонімізації від загальної суми видатків
1	0,0760	20	48	0	0,6305	0,1815
2	0,2013	100	100	34	0,5588	1,0000
3	0,0798	25	29	6	0,7306	0,2668
4	0,1107	38	86	7	0,5571	0,2163
5	0,1376	7	0	0	0,7043	0,2532
6	0,1239	0	0	0	0,7919	0,3932
7	0,0525	1	0	0	0,8879	0,4456
8	0,1739	0	29	3	0,7715	0,4377
9	0,0514	6	97	27	0,9017	0,4259
10	0,0260	0	37	100	0,8243	0,4176
…	…	…	…	…	…	…
56	0,0557	0	0	0	0,9748	0,4518
57	0,1591	0	0	0	0,7433	0,2615
58	0,4023	0	0	1	0,9921	0,3738

Продовження таблиці 2.11

59	0,2313	0	0	0	0,8924	0,4091
60	0,0000	0	0	0	0,6902	0,7707
61	0,0506	0	0	0	0,8704	0,3992
62	0,0096	2	0	0	0,9421	0,2653
63	0,0000	0	0	0	0,8368	0,2434
64	0,1231	0	0	0	0,9675	0,4132
65	0,0000	7	0	0	0,0000	0,0632

Джерело: Складено автором

На першому етапі методики проведено нормалізацію факторів-стимуляторів для другого, третього та четвертого показників (табл. 2.12).

Таблиця 2.12

Нормалізовані значення показників оцінювання ризику використання криптобірж для легалізації кримінальних доходів

Нумерація криптобірж	**К1 — частка операцій з ВА, розмічених за ознаками високо-ризикових операції**	**К2 — кількість операцій з ВА, розмічених за ознаками обходу санкцій**	**К3 — кількість операцій з ВА, розмічених за ознаками злочину відмивання коштів (ВК)**	**К4 — кількість наданих крипто-валютних нелегальних послуг**	**К5 — частка операцій з інструментами анонімізації від загальної суми надходжень**	**К6 — частка операцій з інструментами анонімізації від загальної суми видатків**
1	0,0760	0,2	0,48	0	0,6305	0,1815
2	0,2013	1	1	0,34	0,5588	1,0000
3	0,0798	0,25	0,29	0,06	0,7306	0,2668
4	0,1107	0,38	0,86	0,07	0,5571	0,2163
5	0,1376	0,07	0	0	0,7043	0,2532
6	0,1239	0	0	0	0,7919	0,3932
7	0,0525	0,01	0	0	0,8879	0,4456
8	0,1739	0	0,29	0,03	0,7715	0,4377
9	0,0514	0,06	0,97	0,27	0,9017	0,4259
10	0,0260	0	0,37	1	0,8243	0,4176

Продовження таблиці 2.12

…	…	…	…	…	…	…
56	0,0557	0	0	0	0,9748	0,4518
57	0,1591	0	0	0	0,7433	0,2615
58	0,4023	0	0	0,01	0,9921	0,3738
59	0,2313	0	0	0	0,8924	0,4091
60	0,0000	0	0	0	0,6902	0,7707
61	0,0506	0	0	0	0,8704	0,3992
62	0,0096	0,02	0	0	0,9421	0,2653
63	0,0000	0	0	0	0,8368	0,2434
64	0,1231	0	0	0	0,9675	0,4132
65	0,0000	0,06	0	0	0,0000	0,0632

Джерело: Складено автором

На другому етапі було визначено значущість факторів. Аналіз графіка “кам'янистого осипу” (рис. 2.12) та матриці власних значень (табл. 2.13) показав, що для подальшого розрахунку вагових коефіцієнтів показників ризику легалізації кримінальних доходів необхідно врахувати три перші головні компоненти. Саме вони забезпечують рівень дисперсії впливу не менше 70 %.

Таблиця 2.13

Варіативність	Змінні внески, засновані на кореляції					
	Фактор 1	Фактор 2	Фактор 3	Фактор 4	Фактор 5	Фактор 6
Варіант 1	0,004017	0,230209	0,440134	0,288995	0,012256	0,024389
Варіант 2	0,300835	0,043953	0,194745	0,052796	0,001212	0,406459
Варіант 3	0,369238	0,027276	0,000097	0,000325	0,223376	0,379689
Варіант 4	0,197214	0,010408	0,245888	0,396632	0,119751	0,030107
Варіант 5	0,007495	0,442143	0,104693	0,000167	0,328887	0,116615
Варіант 6	0,121202	0,246011	0,014444	0,261085	0,314517	0,042742

Джерело: Побудовано автором

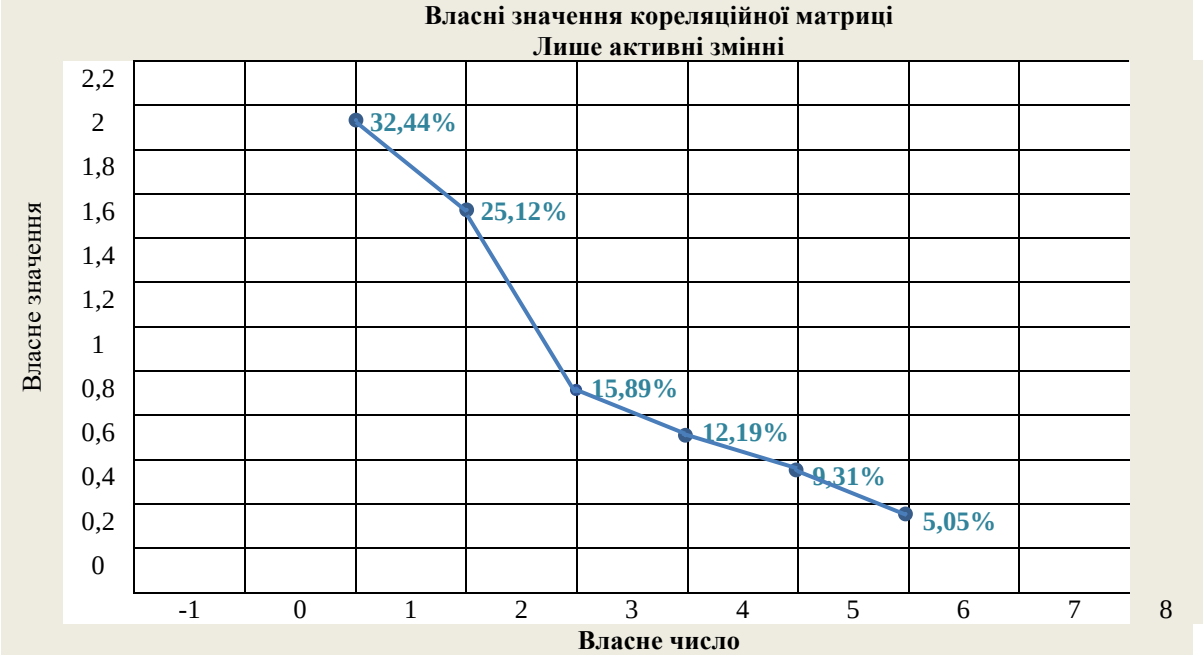


Рис. 2.12. Графік кам'янистого осипу в розрізі методу головних компонент оцінювання ризику використання криптобірж з метою легалізації кримінальних доходів

Джерело: Побудовано автором

Розрахунок вагових коефіцієнтів пріоритетності показників ризику легалізації кримінальних доходів через криптобіржі базується на факторних навантаженнях шести обраних для дослідження показників за трьома основними головними компонентами (табл. 2.14).

Таблиця 2.14

	Власні значення кореляційної матриці та відповідна статистика Лише активні змінні			
	Власне значення	% загальної дисперсії	Кумулятивне значення	Кумулятивний %
1	1,946621	32,44369	1,946621	32,4437
2	1,507443	25,12406	3,454065	57,5677
3	0,953393	15,88989	4,407458	73,4576
4	0,731148	12,18581	5,138606	85,6434
5	0,558326	9,30544	5,696933	94,9489
6	0,303067	5,05112	6,000000	100,0000

Джерело: Складено автором

Зведені результати проміжних розрахунків для обчислення вагових коефіцієнтів показників оцінки рівня ризику легалізації наведено в табл. 2.15.

Таблиця 2.15

Проміжні результати розрахунку вагових коефіцієнтів показників оцінки рівня ризику легалізації оцінювання ризику використання криптобірж з метою ВК

	Фактор 1	**Фактор 2**	**Фактор m**	**Сума добутків факторних навантажень на дисперсію впливу відповідних факторів**	**Ваги показників**
а	1	2	3	4	5
X_1	0,0040	0,2302	0,4401	12,9078	0,1757
X_2	0,3008	0,0440	0,1947	13,9590	0,1900
X_3	0,3692	0,0273	0,0001	12,6662	0,1724
X_4	0,1972	0,0104	0,2459	10,5670	0,1439
X_5	0,0075	0,4421	0,1047	13,0152	0,1772
X_6	0,1212	0,2460	0,0144	10,3425	0,1408
Дисперсія впливу факторів	32,4437	25,1241	15,8899		

Джерело: Складено автором

З отриманих вагових коефіцієнтів бачимо, що найбільший вплив на оцінку ризику легалізації кримінальних доходів мають показники операцій з ВА, розмічених за ознаками обходу санкцій, частки операцій з інструментами анонімізації від загальної суми надходжень, а також частки операцій з ВА, розмічених за ознаками високоризикових операцій. Вони найбільше впливають на оцінку ризику легалізації. Розраховані ваги дали змогу авторам створити інтегрований показник оцінки ризику та визначити кількісну оцінку взаємодії між розглянутою і «нормативною» криптобіржею k за ризиком легалізації. Для аналізу було взято дані глобального ринку віртуальних активів стосовно

блокчейн-платформ біткоїна (BTC) та стейблкоїна USDT на Tron станом на 30 серпня 2024 р.

У табл. 2.16, 2.17 подано результати проміжних розрахунків.

Таблиця 2.16

Проміжні розрахунки оцінки ризику використання криптобірж для ВК

$\omega_1(1-x_1^+)^2$	$\omega_2(1-x_2^+)^2$	$\omega_3(1-x_3^+)^2$	$\omega_4(1-x_4^+)^2$	$\omega_5(1-x_5^+)^2$	$\omega_6(1-x_6^+)^2$	$IRA(x_i)$	Норма резерву	SVA_{1i}	SVA'_{1i}	SVA_{2i}	SVA'_{2i}	SVA^*_i
0,150	0,122	0,047	0,144	0,024	0,094	0,238	1,000	6,971	0,999	0,037	0,381	0,443
0,112	0,000	0,000	0,063	0,034	0,000	0,543	0,352	1,123	0,722	0,526	0,554	0,460
0,149	0,107	0,087	0,127	0,013	0,076	0,253	0,181	0,294	0,475	0,671	0,600	0,487
0,139	0,073	0,003	0,124	0,035	0,086	0,321	0,152	0,344	0,492	1,079	0,712	0,488
0,131	0,164	0,172	0,144	0,015	0,079	0,160	0,239	0,222	0,449	0,285	0,472	0,495
0,135	0,190	0,172	0,144	0,008	0,052	0,163	0,150	0,174	0,431	0,555	0,563	0,497
0,158	0,186	0,172	0,144	0,002	0,043	0,160	0,151	0,171	0,430	0,541	0,559	0,519
0,120	0,190	0,087	0,135	0,009	0,045	0,234	0,124	0,233	0,453	1,015	0,696	0,528
0,158	0,168	0,000	0,077	0,002	0,046	0,328	0,143	0,343	0,492	1,198	0,740	0,537
0,167	0,190	0,068	0,000	0,005	0,048	0,308	0,095	0,283	0,471	1,827	0,851	0,546
…	…	…	…	…	…	…	…	…	…	…	…	…
0,157	0,190	0,172	0,144	0,000	0,042	0,160	0,005	0,118	0,411	3,968	0,981	0,710
0,124	0,190	0,172	0,144	0,012	0,077	0,152	0,006	0,112	0,409	3,704	0,976	0,711
0,063	0,190	0,172	0,141	0,000	0,055	0,212	0,005	0,156	0,425	5,284	0,995	0,711
0,104	0,190	0,172	0,144	0,002	0,049	0,187	0,005	0,137	0,418	4,658	0,991	0,712
0,176	0,190	0,172	0,144	0,017	0,017	0,154	0,005	0,113	0,409	3,854	0,979	0,712
0,140	0,190	0,172	0,144	0,003	0,013	0,186	0,003	0,136	0,418	4,857	0,992	0,715
0,169	0,183	0,172	0,144	0,001	0,041	0,158	0,004	0,116	0,410	4,046	0,983	0,719
0,176	0,190	0,172	0,144	0,005	0,047	0,144	0,004	0,105	0,407	3,684	0,975	0,720
0,096	0,190	0,172	0,144	0,000	0,011	0,217	0,004	0,159	0,426	5,467	0,996	0,723
0,176	0,168	0,172	0,144	0,177	0,111	0,026	0,004	0,019	0,375	0,671	0,600	0,727

Джерело: Складено автором

Таблиця 2.17

Візуалізація спектрального представлення криптобірж у розрізі оцінювання ризику ВК

Діапазон значень	< 0,5	0,5-0,6	0,6-0,7	0,7-0,8
Кількість криптобірж	6	6,000	38,000	15,000
Питома вага криптобірж	0,0923	0,0923	0,5846	0,2308

Джерело: Складено автором

За результатами вагових оцінок бачимо, що 58,46 % криптобірж мають ризик легалізації кримінальних доходів у межах від 0,6 до 0,7 частки одиниці, що свідчить про високий рівень ризику. Критичний рівень ризику (від 0,7 до 0,8 частки одиниці) мають 23,08 % криптобірж. Лише 9,23 % криптобірж мають ризик нижче 0,5 і 9,23 % - у проміжку від 0,5 до 0,6 частки одиниці.

Висновки до розділу 2

1. Ризик-орієнтований підхід є ефективним інструментом управління та оцінки ризику, оскільки ґрунтується на системному аналізі потенційних загроз, їхньому впливі на економічні процеси та забезпечує оптимальний розподіл ресурсів, концентруючись на найбільш критичних загрозах, знижувати регуляторне навантаження для низькоризикових суб'єктів і забезпечувати гнучкість у реагуванні на нові виклики.

З огляду на класифікацію ризиків у економічній теорії, автором сформульовано визначення сутності ризик-орієнтованого підходу до

регулювання обігу цифрових активів у сфері ПВК/ФТ, що полягає в забезпеченні систематичного здійснення оцінки ризиків використання цифрових активів у легалізаційних операціях та операціях маніпулювання віртуальними активами уповноваженими державними органами й учасниками обігу цифрових активів і особами, котрі обслуговують операції з цифровими активами, а також застосування широкої сукупності методів фінансового контролю за обігом цифрових активів з метою виявлення операцій щодо легалізації (відмивання) доходів, ухилення від сплати податків, корупційної діяльності, фінансування тероризму, уникнення санкцій, шахрайства для забезпечення фінансової цілісності та резилієнтності економічної системи.

Запропоноване визначення поєднало в собі основні чинники ризик-орієнтованого підходу, методи ідентифікації ризиків та дозволило систематизувати процеси управління ризиками.

2. Процеси ВК/ФТ являють собою серйозні загрози економічній безпеці держав, оскільки спричиняють зростання тіньової економіки, скорочення бюджетних надходжень, розвиток шахрайських схем та зниження інвестиційної привабливості. Вказані негативні наслідки збільшують державні витрати на боротьбу з фінансово-економічними злочинами.

Розроблені моделі класифікації допомагають ранжувати транзакції за рівнями ризику та виявляти підозрілі операції на ранніх стадіях. Регресійний аналіз сприяє встановленню зв'язків між факторами ризику та волатильністю віртуальних активів. Баєсові мережі дають змогу прогнозувати ймовірнісні сценарії ризиків ВК/ФТ на основі історичних даних, а гравітаційне моделювання аналізує транскордонні потоки нелегальних коштів у глобальному масштабі. Методи SEER (System for Evolutions and Review) та статистичні метрики (наприклад, метрики Мінковського) додатково уточнюють оцінку ризиків операцій із віртуальними активами. Зокрема, аналіз 65 глобальних криптобірж

підтвердив, що найбільші ризики пов'язані з анонімізацією трансакцій та обходом міжнародних санкцій.

3. Результати проведеного дослідження засвідчили актуальність і необхідність впровадження ризик-орієнтованого підходу до оцінки операцій з віртуальними активами в контексті ПВК/ФТ через один із ключових його інструментів так звані «червоні прапорці» – індикатори підвищеного ризику, які сигналізують про потенційно підозрілу діяльність.

У рамках дослідження було поглиблено аналіз схем кримінального використання віртуальних активів і сформульовано авторську систему з 13 критеріїв ризиковості, що дозволяє ідентифікувати операції з високою ймовірністю причетності до процесів легалізації злочинних доходів. Особлива увага приділялася децентралізованим платформам, анонімним монетам (наприклад, Monero, Zcash), міксерам, криптобанкоматам та операціям, пов'язаним із неліцензованими біржами. Усі ці фактори були класифіковані як високоризикові, що значно підвищують вірогідність обходу стандартних механізмів ПВК/ФТ.

Автор зазначає, що використання системи «червоних прапорців» як інструмента ризик-орієнтованого підходу значно посилює ефективність національної системи ПВК/ФТ. Це дозволяє не тільки своєчасно реагувати на сучасні загрози цифрового середовища, а й формувати прозоріші умови для обігу віртуальних активів, що, своєю чергою, підвищує інвестиційну привабливість країни та знижує витрати держави на боротьбу з економічною злочинністю.

Розроблені в дисертації критерії стали основою для побудови математичних моделей оцінки ризиків, орієнтованих на експертну оцінку поведінкових і транзакційних патернів користувачів цифрових активів. Застосування таких моделей дає змогу фінансовим установам, провайдерам криптопослуг та державним регуляторам не лише вчасно ідентифікувати ризиковані транзакції, але й оптимізувати ресурси, зосереджуючи контроль саме на тих операціях, які мають найвищу ймовірність зловживань.

4. Так, використані автором моделі класифікації допомагають ранжувати транзакції за рівнями ризику та виявляти підозрілі операції на ранніх стадіях. Регресійний аналіз сприяє встановленню зв'язків між факторами ризику та волатильністю віртуальних активів. Баєсові мережі дають змогу прогнозувати ймовірнісні сценарії ризиків ВК/ФТ на основі даних бухгалтерського обліку операцій з ВА, а гравітаційне моделювання аналізує транскордонні потоки нелегальних коштів у глобальному масштабі. Методи SEER (System for Evolutions and Review) та статистичні метрики (наприклад, метрики Мінковського) додатково уточнюють оцінку ризиків операцій із віртуальними активами. Зокрема, проведений аналіз 65 глобальних криптобірж підтвердив, що найбільші ризики пов'язані з анонімізацією трансакцій та обходом міжнародних санкцій.

Основні положення розділу містяться в роботах [36; 39; 121; 258; 264; 295; 298]

РОЗДІЛ 3
ЛЕГАЛІЗАЦІЯ ДІЯЛЬНОСТІ РИНКІВ ЦИФРОВИХ АКТИВІВ В УКРАЇНІ

3.1. Регулювання діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів в Україні

Відтоді, як FATF розширила свої стандарти з ПВК/ФТ на фінансову діяльність, пов'язану з ВА і ППВА [223; 73], щоб протидіяти загрозі їх використання у злочинних та терористичних цілях, вона опублікувала два глобальні огляди впровадження Стандартів щодо ВА та ППВА, а в жовтні 2021 р. оприлюднила оновлене Керівництво, щоб допомогти юрисдикціям та ППВА ефективно впровадити ці вимоги [72]. В останньому (третьому) Керівництві представлено цільовий огляд реалізації міжнародних стандартів, зосереджений на Правилі подорожей FATF, яке вимагає від приватного сектору отримувати/обмінюватися інформацією про бенефіціарів та ініціаторів переказів ВА. Воно також надає коротку інформацію про загальне виконання Рекомендації 15 FATF «Інноваційні технології» та пояснювальної записки до неї (R.15/INR.15) [223], про нові ризики та ринкові новації, які FATF продовжує відстежувати, наприклад, децентралізовані фінанси (DeFi, англ. decentralized finance), незмінні токени (NFT, англ. non-fungible token) та холодні гаманці [36].

Правило подорожей (Рекомендація 16 FATF «Грошові перекази», також відоме як Travel Rule), офіційно ухвалене FATF 21 червня 2019 р., було розроблено для запобігання неконтрольованому доступу терористів та інших злочинців до електронних переказів коштів із метою їх використання в незаконних операціях, а також виявлення таких зловживань у разі їх виникнення. З метою адаптації міжнародних регуляторних актів до оновлень платіжних

бізнес-моделей та еталонів обміну повідомленнями з лютого 2024 р. за ініціативою FATF проводиться публічне обговорення поправок до Рекомендації 16 FATF (R.16) та, відповідно, до Пояснювальної записки до R.16 FATF (INR. 16). У глосарії очікується зміна специфічного терміна, назви R.16/INR.16 «Грошові перекази» (англ. Wire transfers) на «Транспарентність платежів» (англ. Payment transparency) [78].

Правило подорожей ще часто називають «правилом криптоподорожей», оскільки воно імітує «правило подорожі» Закону США про конфіденційність банківської діяльності. Ми вже зазначали раніше, що це правило вдосконалює процедури, спрямовані на ПВК/ФТ та реалізацію політики ЗСК. Такі самі зобов'язання застосовуються до фінансових установ при здійсненні переказів ВА від імені клієнта. Це підкреслює потребу в тому, щоб юрисдикції продовжували координувати спільні питання, а приватний сектор – розвивати глобальні технологічні інструменти, які можуть враховувати нюанси відносин між юрисдикціями [36].

За останні роки юрисдикції досягли обмеженого прогресу в запровадженні Правила подорожей FATF, що є ключовою вимогою FATF, котра дозволяє приватному сектору виконувати вимоги санкцій та виявляти підозрілі трансакції.

Багато країн досі не впровадили в повному обсязі вимоги FATF щодо ВА та ППВА для запобігання їхньому використанню в незаконній фінансовій діяльності. Відсутність реалізації цих вимог (Рекомендація 15 FATF) створює значні прогалини в глобальній системі, які використовують злочинці та терористи.

У лютому 2023 р. Пленарне засідання FATF погодило дорожню карту для посилення впровадження стандартів FATF щодо віртуальних активів і постачальників послуг, пов'язаних із віртуальними активами [305]. FATF провела оцінку поточного рівня впровадження стандартів у межах глобальної мережі.

Після 12-місячного збору та аналізу інформації FATF публікує таблицю, яка показує статус впровадження Рекомендації 15 країнами-членами та іншими юрисдикціями, де активність ППВА є найбільш значущою.

FATF у своєму звіті щодо статусу впровадження Рекомендації 15 наголошує на важливості виконання урядами своїх зобов'язань щодо стандартів ПВК/ФТ у сфері віртуальних активів. Це необхідно для ефективної боротьби з відмиванням коштів та фінансуванням тероризму на національному і глобальному рівнях. Звіт також спрямований на підтримку юрисдикцій у регулюванні та нагляді за ППВА щодо ПВК/ФТ.

Звіт включає 38 членів FATF, які мають бути лідерами у впровадженні стандартів ПВК/ФТ, та 20 інших юрисдикцій, визначених за обсягом торгівлі віртуальними активами (ППВА, які відповідають за щонайменше 0,25 % глобального обсягу) чи кількістю користувачів (понад 1 млн).

Додаткові 20 юрисдикцій із суттєвою активністю у сфері ППВА: Багамські Острови, Кайманові Острови, Колумбія, Кіпр, Єгипет, Естонія, Гібралтар, Казахстан, Литва, Мальта, Нігерія, Філіппіни, Польща, Сейшельські Острови, Таїланд, Україна, ОАЕ, Венесуела, В'єтнам, Британські Віргінські Острови.

Аналіз даних про прогрес звіту показав:

- 100 % юрисдикцій провели або проводять оцінку ризиків у сфері ППВА (Австралія, Фінляндія, Греція, Малайзія, Португалія — у процесі);
- 9 % заборонили або перебувають у процесі заборони використання ППВА (Китай, Єгипет, Саудівська Аравія; Сейшельські Острови та Індонезія — у процесі);
- 17 % не створили регуляторної бази для реєстрації чи ліцензування ППВА (В'єтнам, Нова Зеландія, Туреччина, Аргентина, Колумбія);
- 22 % не зареєстрували ППВА на практиці (Україна, Аргентина, Колумбія);

– 28 % не вжили примусових заходів щодо ППВА (Україна, Аргентина, Бразилія, Китай);

– 33 % не запровадили «правило переказу» для ППВА (Україна, Австралія, Китай, Південна Африка та ін.).

У підсумку Багамські острови визнані серед 58 країн єдиною юрисдикцією, що повністю відповідає Рекомендації 15 (оцінка 2022 р.). Однак варто зазначити, що 13 юрисдикцій ще не пройшли оцінки стосовно відповідності оновленим стандартам FATF.

Таблиця зі звіту FATF є корисним довідником для розуміння стану впровадження Рекомендації 15 у різних юрисдикціях. Вона виступає інструментом оцінки ефективності національних регуляторних рамок у 58 країнах. Проте сектору криптовалют потрібні глобально узгоджені стандарти для ПВК/ФТ, особливо у сфері виконання Правила подорожей.

Щодо країн і державного сектору, то цей звіт наголошує на тому, що юрисдикції повинні приділити пріоритетну увагу впровадженню стандартів FATF для ВА з урахуванням національних оцінок ризиків. ППВА зобов’язані активно використовувати інструменти моніторингу та управління ризиками, а не лише мати доступ до них. Звіт має допомогти країнам визначити слабкі місця у своєму регулюванні та зосередити зусилля на їхньому усуненні. Невідповідність стандартам FATF може вплинути на статус юрисдикцій на міжнародному рівні, зокрема в оцінках інших країн.

Таблиця зазначеного звіту підготовлена на основі роботи членів Контактної групи FATF з питань віртуальних активів (англ. Virtual Asset Contact Group, VACG), а також завдяки внескам глобальної мережі FATF, до якої входять її члени та регіональні органи, що утворені та діють за стандартами FATF. Крім того, було враховано консультації з представниками приватного сектору та спільноти, що займається віртуальними активами і послугами, пов’язаними з ними [305] (табл. 3.1).

Таблиця 3.1.

Показники впровадження Рекомендації 15 FATF серед країн з активною діяльністю у сфері ВА (показники України)

Юрисдикція	Провела оцінку ризиків, що охоплює віртуальні активи та ППВА	Чітко заборонила використання ВА та ППВА	Прийняла законодавство/регулювання, що вимагає реєстрації або ліцензування ППВА і застосування заходів ПВК/ФТ	Зареєструвала або ліцензувала ППВА на практиці	Провела наглядову перевірку або включила ППВА до чинного плану перевірок	Застосувала примусові заходи або інші наглядові дії щодо ППВА	Прийняла або впровадила правило передачі даних для ППВА	Рейтинг Рекомендації 15 (де оцінено за оновленими стандартами FATF) та дата оцінки C = compliant (відповідний) LC = largely compliant (переважно відповідний) PC = partially compliant (частково відповідний) NC = non-compliant (невідповідний)
Україна	Так	Ні	Так	Ні	Ні	Ні	Ні	**PC (2020)**

Джерело: побудовано автором за матеріалами [305].

FATF висловив особливу подяку компаніям з блокчейн-аналітики за їхній цінний внесок у цей процес. Т. Раджа Кумар, президент FATF, наголосив: «Наша мета – встановити глобальні рівні правила гри, щоб індустрія відповідала регуляторним вимогам та зменшила можливості злочинців для зловживань у цьому секторі» [305].

Протягом останнього року приватний сектор досяг прогресу в сприянні впровадженню Правила подорожей. Наразі доступні технологічні рішення для підтримки відповідності, хоча й з певними обмеженнями, і ППВА, котрі мають забезпечити впровадження цього правила, почали робити перші кроки з метою забезпечення сумісності з іншими рішеннями. Однак приватному сектору необхідно посилити взаємодію між рішеннями та гарантувати повну відповідність стандартам FATF для їх ефективного глобального впровадження.

Розвиток новітніх технологій привертає дедалі більшу увагу міжнародних організацій та є одним із найважливіших напрямів дослідження, регулювання та розбудови системи впливу для забезпечення фінансової стабільності.

Першим кроком в унормуванні діяльності ринку ВА в Україні та впровадженні міжнародних стандартів, зокрема оновленої Рекомендації 15 FATF, Пояснювальної записки до неї та Правила подорожей, стало ухвалення законодавства у сфері ПВК/ФТ.

Так, 28 квітня 2020 р. набрав чинності Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [419], яким передбачено реалізацію Рекомендацій FATF шляхом упровадження заходів із ПВК/ФТ на ринку ВА. Проте, аби розпочати повноцінну легалізацію ринку ВА та впровадити ПВК/ФТ-процедури, потрібно було прийняти профільний закон, що містить основні визначення, розкриває правовий статус і ключові правила діяльності ринку. На початку 2020 р. було зареєстровано проєкт Закону «Про віртуальні активи» [437], який після розгляду 15 липня 2020 р. у Комітеті цифрової трансформації Верховної Ради України відправлений на доопрацювання з основним питанням стосовно визначення правової сутності в уже чинній системі національного законодавства.

Позитивними рисами цього законопроєкту були: класифікація ВА на незабезпечені й забезпечені, пропозиція регулювання забезпечених ВА тим державним наглядовим органом, котрий регулює об'єкт забезпечення, введення термінології і понять ринку таких активів. Також імплементовано види діяльності на ринку ВА, які підлягають обов’язковій реєстрації або ліцензуванню. Верховна Рада України після складного процесу врахування пропозицій і голосування 17 лютого 2022 р. ухвалила Закон «Про віртуальні активи» (далі – Закон) з пропозиціями Президента, який підписав його 15 березня 2022 р. [162].

У прикінцевих положеннях закону вказано, що він набирає сили після внесення змін щодо оподаткування операцій з ВА до Податкового кодексу України. У Верховній Раді України в листопаді 2023 р. зареєстровано два проєкти Закону «Про внесення змін до Податкового кодексу України щодо

оподаткування операцій з віртуальними активами» № 10225, над яким працювала Національна комісія з цінних паперів та фондового ринку [306], та № 10225-1 від Міністерства цифрової трансформації України [307], наразі триває їхнє обговорення. Детально порівняння цих законодавчих ініціатив ми розглянемо нижче.

Варто зазначити, що проєктом Закону України про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні від 07.11.2023 № 10225, окрім норм щодо оподаткування ВА, пропонуються нова редакція Закону України «Про віртуальні активи» та відповідні зміни до пов’язаних законодавчих актів, які імплементують вимоги Регламенту ЄС щодо діяльності крипторинку (Регламент Markets in Crypto assets (MiCA) [78]).

Проєктом закону шляхом внесення змін до Податкового кодексу України пропонуються, зокрема:

- запровадження механізму оподаткування податком на прибуток підприємств ВА шляхом запровадження окремого обліку результатів та коригування фінансового результату;
- запровадження механізму оподаткування віртуальних активів ПДФО;
- невизнання операцій з ВА об'єктом оподаткування ПДВ;
- неможливість віднесення суб’єктів господарювання (юридичні особи та фізичні особи – підприємці), котрі здійснюють операції з ВА, до платників єдиного податку першої – третьої груп.

В обговоренні питань упровадження законодавства щодо функціонування ринку ВА приватний сектор наголошує на необхідності швидкого внесення змін до Податкового кодексу України стосовно операцій з ВА. Саме визначеність в оподаткуванні діяльності ППВА сприятиме швидкості реєстрації учасників ринку. Варто зауважити, що в результаті внесених змін до закону наглядовим

органом за діяльністю ринку ВА вказано Національну комісію з цінних паперів та фондового ринку (НКЦПФР) [306].

Стосовно нормативних актів для врегулювання діяльності суб'єктів первинного фінансового моніторингу – ППВА Державній службі фінансового моніторингу та Міністерству фінансів України необхідно внести зміни щодо суб'єктів державного фінансового моніторингу, що регулює діяльність крипторинку, а НКЦПФР розробити Положення про здійснення установами фінансового моніторингу, в якому слід відобразити такі питання:

1) на підставі базових законів [162; 306] введення й пояснення єдиних термінів і понять для оперування ними в наступних нормативно-правових актах;

2) належна організація внутрішньої системи ПВК/ФТ установи з упровадженням РОП (розробити порядок ідентифікації, верифікації клієнта (представника клієнта), порядок здійснення відеоверифікації, процедури встановлення кінцевих бенефіціарних власників, спрощених та посилених заходів належної перевірки клієнта, заходи щодо неприбуткових організацій, додаткові заходи щодо клієнтів, які є політично значущими особами, членами їхніх сімей та особами, пов'язаними з політично значущими особами, політику використання інформації щодо належної перевірки клієнта, отриманої від третьої сторони, порядок відмови установи від встановлення (підтримання) ділових відносин / проведення фінансової операції, порядок зупинення, поновлення фінансових операцій та виконання рішень (доручень), порядок замороження/розмороження активів, порядок моніторингу фінансових операцій, їх реєстрації та здійснення інформаційного обміну зі спеціально уповноваженим органом, заходи щодо переказів ВА, порядок надання особами повідомлень про порушення у сфері ПВК/ФТ, порядок їх розгляду);

3) вимоги до внутрішніх документів установи з питань ПВК/ФТ;

4) належна система управління ризиками ВК/ФТ (критерії ризику; індикатори підозрілості фінансових операцій) [308];

5) використання рішень комплексної перевірки ППВА на основі блокчейн-аналітичних програмних продуктів для визначення та оцінки профілів ризику ППВА перед схваленням трансакцій або встановленням відносин із ними;

6) порядок призначення та звільнення відповідального працівника установи;

7) вимоги до єдиних правил з питань ПВК/ФТ групи;

8) організація і проведення навчальних заходів.

Крім того, необхідно забезпечити реєстрацію учасників ринку з їхнею одночасною реєстрацією як суб'єктів первинного фінансового моніторингу, для чого НКЦПФР зі спеціально уповноваженим органом у сфері ПВК/ФТ, окрім створення програмного продукту, який дав би змогу поєднати ці дві реєстрації, повинна розробити порядок такої реєстрації і провести відповідне навчання.

З огляду на необхідність упровадження Рекомендації 1 FATF щодо ризик-орієнтованого підходу в діяльність Національної системи ПВК/ФТ та діяльність ринку ВА варто виконати секторальну оцінку ризиків та долучити її до Національної оцінки ризиків, що має відобразити ризики взаємодії ринку ВА з іншими секторами економіки України, насамперед з банківським сектором.

Українська блокчейн-спільнота є однією з найбільших у світі та входить до п'ятірки лідерів. Крім того, в Україні спостерігається високий рівень цифрової грамотності населення. Країна також займає провідні позиції у світі за кількістю безготівкових платежів і має потужну освітню й інтелектуальну базу. Багато представників малого бізнесу займаються посередництвом на міжнародних маркетплейсах, використовуючи ВА для розрахунків.

Глобальний індекс упровадження криптовалют оцінює, зокрема, кількість депозитів, трансакцій і вартість криптоактивів, які належать користувачам країни. Згідно з дослідженням, високий рівень розвитку криптоіндустрії в Україні, ймовірно, пояснюється низьким рівнем довіри громадян до державних і фінансових установ (зокрема банків) та одночасно значною кількістю кваліфікованих програмістів (рис. 3.1).

Щодо майнінгу криптовалют, то Україна має частку лише 0,13% серед усіх потужностей майнінгу у світі [309]. І найближчим часом, за результатами хронічних атак на енергосистему України з боку рф у ході україно-російської, війни класичний майнінг криптовалют економічно буде не цікавий для легального підприємництва. Однак ситуація може змінитися за рахунок інноваційних та технологічних підходів до такої діяльності.

Україна 	Загальний рейтинг індексу	Показник обсягу централізованих сервісів БІРЖІ	Показник обсягу централізованих сервісів ОБМІННИКИ	Показник обсягів P2P трансакцій	Показник обсягів операцій в DeFi БІРЖІ	Показник обсягів роздрібних операцій в DeFi
2024	6	6	7	5	5	6
2023	5	5	3	11	10	10
2022	3	6	6	39	10	14
2021	4	6	5	40	-	-
2020	1	4	7	11	-	-

Рис.3.1. Динаміка глобального рейтингу сприйняття криптоактивів в Україні за 2020-2024 роки.

Джерело: побудовано автором за матеріалами [310].

Незважаючи на війну, що триває, та посилення міжнародних санкцій проти росії, крипторинок України у 2024 р. демонструє активний розвиток, а обсяг надходжень криптовалют становив 106,1 млрд дол. США.

Значну частину зростання крипторинку в Україні забезпечили інституційні та професійні перекази, що є важливим фактором на тлі змін у регулюванні галузі.

Як демонструє регіональна оцінка тенденцій за інформацією з WhiteBIT, криптобіржі з українським корінням, яка тепер має штаб-квартиру в Литві та вісім офісів по всьому світу, інституційні та професійні криптовалютні перекази

в Україні зросли, оскільки багато хто шукає фінансової стабільності в умовах війни, розглядаючи криптовалюти як безпечнішу альтернативу. На цей тренд впливають глобальні фактори, такі як волатильність ринку, інфляція, санкції, пов'язані з війною, а також зростаючий інтерес до Bitcoin ETF від таких компаній, як BlackRock [310].

WhiteBIT, попри війну, продовжує активно працювати в регіоні, як і низка інших централізованих бірж (CEX), хоч окремі з них перенесли операції до інших країн Східної Європи через питання безпеки.

Дані ордербуків показують, що за минулий рік покупки Bitcoin (BTC) за українську гривню (UAH) досягли 882,64 млн дол. США. Це зростання відбулося після піка інфляції гривні на рівні 26,6% у грудні 2022 р. та поступового зниження її курсу в I кв. 2023 р. З огляду на те, що поведінка споживачів зазвичай відстає від економічних тенденцій, українці, ймовірно, розглядали BTC як альтернативний засіб збереження вартості на тлі волатильності національної валюти. У WhiteBIT зазначили: «У період економічної нестабільності BTC сприймається як більш безпечна довгострокова інвестиція порівняно з волатильною національною валютою. Ліквідність і безпека BTC роблять його привабливим як для інституційних, так і для роздрібних інвесторів в Україні, котрі прагнуть зберегти стабільність та довгострокову цінність своїх активів в умовах війни» [310].

У Східній Європі у 2024 р. саме децентралізовані біржі показали найбільше зростання надходжень криптовалют, зокрема в Україні та Польщі. Загалом DEX отримали 148,68 млрд дол. США криптовалют. В Україні криптовалютні перекази на DEX збільшились на 160,23 %, досягнувши 34,9 млрд дол. США. У таких країнах, як Молдова, Угорщина та Чехія, теж спостерігається зростання послуг DeFi-кредитування.

Попри вибухове зростання криптовалютних надходжень через «мости» (bridges) в Угорщині та Молдові, їхня частка в загальному обсязі DeFi для регіону

залишається незначною. Наприклад, Угорщина отримала 151 млн дол. США через мости, тоді як в Україні цей показник становив 897 млн дол. США.

В Україні зростання DeFi-трансакцій свідчить про два ключові тренди: у великих інституційних трансакціях (понад 10 млн дол. США) зафіксовано зростання на 361,49 %, що стало основним драйвером її DeFi-ринку. Водночас зросли великі роздрібні трансакції (1–10 тис. дол. США) на 82,29 % та дрібні роздрібні трансакції (менше 1 тис. дол. США) на 91,99 %. Це свідчить про те, що криптовалюти активно використовуються для підвищення купівельної спроможності в умовах економічної нестабільності [310].

Активність у DeFi також може свідчити про те, що інвестори віддають перевагу швидкості, зручності та контролю, які пропонують децентралізовані платформи, уникаючи регуляторних складнощів, пов'язаних із CEX.

Ринок ВА в Україні демонструє значний рівень розвитку та обсяги операцій, які помітні навіть у світовому масштабі. Однак значна частина цього ринку залишається в сірій зоні, що створює потенційні ризики для держави, бізнесу та користувачів.

Водночас існують серйозні кримінологічні ризики, пов’язані з обігом криптовалют, які сприяють їхньому використанню у злочинній діяльності. Через технічну складність виникають проблеми з правовим регулюванням криптовалют. Відомо, що їх часто застосовують для фінансових та економічних злочинів, а також для незаконної торгівлі наркотиками, зброєю та боєприпасами, фінансування терористичних або екстремістських організацій.

Інтеграція кібернетичних методів у злочинну діяльність вимагає переосмислення кримінального законодавства, зокрема:

- визначення оптимального складу злочинів, спрямованих на захист інформаційної безпеки;
- адаптації традиційних кримінальних правопорушень до цифрової сфери;
- ідентифікації специфічних загроз у віртуальному середовищі.

Такі зміни мають забезпечити ефективне реагування на виклики, пов’язані з поширенням криптовалют і їхнім впливом на безпеку суспільства.

Криптовалюти використовуються для придбання широкого спектра нелегальних товарів і послуг. Їх застосовують у порноіндустрії, торгівлі персональними даними, підробленими документами, нелегальними ліками, а інколи навіть для оплати замовних вбивств. Однак найбільший сегмент незаконного використання криптовалют пов'язаний із незаконним обігом наркотиків і психотропних речовин, що становить близько 80 % загального обсягу нелегального ринку.

Найгучніші злочини в Україні, пов’язані з криптовалютою:

- викрадення людей із вимогою викупу в криптовалюті;
- крадіжка електроенергії для майнінгу;
- фінансування так званих «лнр», «днр» через майнінг;
- оперативно-розшукові заходи правоохоронних органів, спрямовані на виявлення та затримання осіб, які займаються операціями з криптовалютами з метою збагачення чи закриття «конвертаційних центрів»;
- зломи криптовалютних бірж;
- розкрадання коштів із криптогаманців.

З початком війни в Україні шахраї розробили нові способи зловживань, серед яких:

- зловживання благодійністю [311; 312];
- фіктивна роздача ВА [313];
- шахрайство з антиросійськими санкціями (табл. 3.2).

Ще одним популярним способом легалізації незаконних доходів є ВК через сайти азартних ігор. Приблизно три чверті «брудних» ВА проходять через ці платформи. Злочинці дедалі частіше використовують валюту віртуальних ігор як спосіб зберігання вартості криптовалют. Вони купують ігрову валюту, продають її за криптовалюту, а потім обмінюють на фіатну валюту через спеціальні сервіси [314].

Такі злочинні схеми підкреслюють необхідність посилення регулювання криптовалютного ринку та підвищення обізнаності користувачів.

Таблиця 3.2

Загрози, пов'язані з використанням ВА

Загроза	Рівень
Використання ВА під час скоєння предикатних злочинів	**Середній**
Застосування ВА у випадках ВК	**Середній**
Використання ВА для ФТ	**Високий**
Використання ВА у сфері фінансування розповсюдження зброї масового знищення (ФРЗМЗ)	**Високий**
Використання ВА для обходу санкцій	**Високий**

Джерело: складено автором

ВА можуть бути залучені до предикатних злочинів у таких аспектах:

- використання для ухилення від сплати податків;
- викрадення або шахрайське вилучення ВА у фізичних чи юридичних осіб;
- участь у схемах псевдоінвестування або фінансових пірамідах для масштабного обману вкладників;
- забезпечення анонімності під час придбання заборонених товарів та послуг (наркотиків, зброї, послуг, пов'язаних із корупцією);
- застосування ВА для вимагання викупу в різних випадках (шкідливе програмне забезпечення, викрадення людей).

Як легальний, так і нелегальний бізнес може використовувати ВА для обміну на фіатні валюти, зокрема через криптовалютні банкомати. У цьому контексті традиційні методи ПВК/ФТ є найефективнішими.

Однак попередні етапи ВК, пов'язані з приховуванням і маскуванням активів, часто реалізуються в межах обігу ВА, а саме:

- переміщення активів між численними криптогаманцями вручну або за допомогою автоматизованих програм;

- використання спеціалізованих сервісів змішування криптопотоків для ускладнення відстеження трансакцій;
- маскування криптотрансакцій під криптострахування, криптокредитування, трастові послуги або маніпуляції цінами на ринку токенів, що імітують збитки чи прибутки;
- підлаштування виграшів у віртуальних казино з виплатою у ВА.

Через глобальність і зручність використання криптовалют їх активно застосовують злочинні угруповання для відмивання коштів. Одна з основних технологій ВК у цій сфері полягає у придбанні ВА за «злочинні» кошти, подальшому їх подрібненні через біржі або сервіси-міксери, а також конвертації в інші ВА для ускладнення відстеження трансакцій [315].

За оцінками експертів, фінансові потоки з територій, контрольованих терористичними структурами «днр», «лнр» та рф, можуть потрапляти на підконтрольну Україні територію без фізичного перевезення готівки. Це стає можливим завдяки схемі, за якої криптовалюта купується за готівку на окупованих територіях, а потім реалізується за готівку [316]. Отримані таким чином кошти можуть використовуватися для підривної діяльності проти України: оплати оренди житла для підозрілих осіб, підкупу посадовців, придбання розвідувальної інформації чи транспорту для терористичних дій.

Зростання популярності криптовалют як інструменту краудфандингу теж потребує врахування ризиків їхнього використання для фінансування тероризму проти України.

Окремі системи обігу ВА, такі як Tornado Cash і Blender.io, потрапляють до санкційних списків певних країн. Це створює правові підстави для конфіскації відповідних активів, але вимагає значної пошуково-аналітичної роботи високої складності. Протидія таким системам потребує ефективної координації компетентних органів і суб’єктів фінансового моніторингу різних країн.

Водночас криптовалюти, які не включені до санкційних списків, можуть використовуватися для обходу санкцій. Однак їхнє значення в таких операціях

значно менше, ніж розрахунки у фіатних валютах або бартерні угоди. Є підстави припускати, що в уникненні персональних санкцій роль ВА значно вища, ніж у випадку секторальних санкцій.

Таблиця 3.3

Вразливості, пов'язані з ВА та ППВА

Вразливість	Рівень
Відсутність спеціалізованого правового регулювання у сфері обігу ВА та функціонування ППВА	**Високий**
Недостатність ресурсів для проведення розслідувань у сфері обігу ВА	**Середній**
Недосконаліть механізмів міжнародної співпраці у сфері нагляду та розслідувань, що стосуються обігу ВА та діяльності ППВА	**Середній**

Джерело: складено автором

На основі аналізу загроз і вразливостей (див. табл. 3.2; табл. 3.3) можна виокремити ключові ризики, які потребують управління для їхньої мінімізації:

- ризик невиявлення операцій і їхніх учасників у сфері обігу ВА;
- ризик невиявлення операцій і їхніх учасників у сфері обміну ВА на фіатні валюти і навпаки.

Таблиця 3.4

Ризики, пов'язані з ВА та ППВА

		Вразливості		
		відсутність спеціалізованого правового забезпечення у сфері обігу ВА та діяльності ППВА	недостатність ресурсів для проведення розслідувань у сфері обігу ВА	недосконаліть механізмів міжнародної співпраці у сфері нагляду та розслідувань, що стосуються обігу ВА і діяльності ППВА
Загрози	діяльність з ВА при скоєнні предикатних злочинів		Ризик	Ризик
	діяльність з ВА при ВК	Ризик	Ризик	Ризик
	діяльність з використання ВА для ФТ		Ризик	Ризик
	діяльність з використання ВА у сфері ФРЗМЗ		Ризик	Ризик
	діяльність з використання ВА для обхід санкцій		Ризик	Ризик

Джерело: складено актором

Покращання механізмів виявлення таких операцій і встановлення їхніх учасників стане основою для застосування заходів відповідальності до винних осіб та конфіскації їхніх активів (табл. 3.4)

Національний банк України також визначив потенційні ризики, пов'язані з ВА:

- заміщення національної валюти та формування паралельного грошового обігу поза контролем НБУ, що може обмежити його здатність ефективно здійснювати монетарну політику та забезпечувати стабільність гривні. Це становить загрозу для монетарного суверенітету держави;
- обхід державного регулювання та контролю, зокрема валютного регулювання, що може сприяти неконтрольованому переміщенню капіталів за кордон та створювати загрози стабільності валютного ринку;
- уникнення вимог фінансового моніторингу під час здійснення операцій із ВА, що може порушувати фінансову стабільність і послаблювати трансмісійний механізм монетарної політики;
- перелив банківських депозитів у ВА та витіснення традиційного банкінгу, що загрожує стабільності банківської системи та фінансової системи країни загалом;
- ризик із боку стейблкоїнів для фінансової системи через можливі складнощі з їхньою конвертацією у фіатні валюти, такі як долари США [317].

Водночас в Україні у 2024 р. спостерігалося зниження обсягів використання стейблкоїнів. З одного боку, багато українців купували криптовалюти з інвестиційною метою, тому це могло знижувати популярність стейблкоїнів. З другого боку, стейблкоїни часто використовувалися для P2P-переказів як платіжний засіб або інструмент для транскордонних операцій і могли не бути інвестиційними активами. У країнах зі стабільними валютами та доступом до банківських послуг потреба у стейблкоїнах як засобі збереження вартості значно менша. Проте через війну вартість гривні істотно знизилася і

громадяни схильні обмінювати свої заощадження на долари США, після скасування у грудні 2023 р. обмежень на купівлю іноземної валюти в Україні.

За результатами аналізу судових вироків, пов'язаних із вчиненням кримінальних правопорушень за ст. 209 КК України, протягом 2019–2021 рр. ВА використовувались як інструмент вчинення злочину ВК у 8 вироках, або 9 % загальної кількості вироків, пов'язаних з ВК [318].

Статистичних даних за 2022–2024 рр. в Україні немає. Відповідно до рішення Ради з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (протокол засідання № 14 від 29.12.2022 [319]), оприлюднення Звіту про проведення Національної оцінки ризиків у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення на офіційному вебсайті Держфінмоніторингу буде здійснено протягом місяця після скасування воєнного стану.

У майбутньому щодо Рекомендації 33 FATF [178] слід організувати збір статистичних даних відповідно до вимог Держфінмоніторингу стосовно збору загальних адміністративних даних щодо ПВК/ФТ у складі обов'язкової звітності всіх ППВА до державного наглядового органу діяльності ринку ВА в Україні.

До головних викликів у державному управлінні належать такі. По-перше, набуття чинності Законом України «Про віртуальні активи» [162], бажано з імплементацією європейських стандартів регулювання ринку ВА, а саме двох Регламентів ЄС MiCA, DORA та оновленої Директиви ЄС DAC8.

Нагадаємо: Європейський Союз у процесі впровадження законодавства стосовно діяльності крипторинку (Регламент MiCA [78]) одночасно для протидії викликам у сфері кібербезпеки єдиним пакетом прийняв Регламент DORA щодо операційної стійкості цифрових технологій у секторі фінансових послуг [81]. Він спрямований на створення всеосяжної й уніфікованої основи для гармонізації

процесів та стандартів, пов'язаних із операційною стійкістю цифрових технологій у фінансовому секторі, та оновлює Директиву 2011/16/ЄС про адміністративне співробітництво в галузі оподаткування DAC8 [82], яка вводить правила податкової прозорості для криптоактивів.

По-друге, хоча Національний банк України продовжує реформу фінансового сектору згідно зі стандартами Європейського Союзу, послідовно виконуючи вимоги Угоди про асоціацію України з ЄС (далі – Угода), ухвалені 9 березня 2023 р. Ключові напрями євроінтеграційного руху Національного банку у 2022 році [320] не містять пропозицій щодо розгляду чи розроблення власних нормативно-правових актів у сфері криптоактивів.

По-третє, постановою НБУ «Про внесення поправок до деяких нормативно-правових актів НБУ щодо авторизації діяльності операторів фінансових платіжних послуг» від 01.03.2023 № 14 та коментарями до цього документа регулятор встановив нові посилені правила для операторів платіжного ринку [321]. Хоча прямої згадки про криптовалюти та криптобіржі в них немає, але вони прямо стосуються криптообмінників та їхніх учасників. Це рішення Національного банку, прийняте через виявлені порушення в розрахунках грального бізнесу та нелегальне виведення коштів через криптоактиви за кордон, мало на меті переліцензування та/або нову авторизацію операторів, які надають платіжні послуги.

Крім того, нормативними актами варто визначити повноваження НКЦПФР щодо розвитку ВА (приватних криптовалют, службових та ігрових токенів, інструментів та інфраструктури децентралізованих фінансів DeFi, зокрема незмінних токенів NFT) з метою впровадження законодавчих актів Ради Європи та ЄС, міжнародних стандартів.

Сукупний обсяг капіталізації ринку криптовалют у світі на 20 листопада 2024р. становив 3,3 трлн дол. США (динаміка -0,6 % за останні 24 години; динаміка 123,33 % відносно обсягу минулого року). Ринкова капіталізація

Bitcoin (BTC) дорівнювала 1,8 трлн дол. США, що свідчило про його домінування на ринку в розмірі 56,7% [262].

Нині частка трансакцій, котра припадає на найбільші ВА, є мізерно малою порівняно з аналогічними показниками популярних платіжних систем. Водночас їх використання як зручного платіжного засобу є потенційно привабливим інвестиційним інструментом фінансової екосистеми для організації торгівлі, обміну й зберігання ВА, призначених для інвестування. Ключовим компонентом збільшення обігу та ринкової капіталізації криптовалюти є інтерес інвесторів, що зростає, до використання стабільних криптомонет, нових технологій, «розумних» контрактів (смарт-контрактів) і децентралізованих фінансів (DeFi) [322]. МВФ характеризує таку ситуацію як інноваційний процес, що змінить майбутній ландшафт банківської системи за відповідного зниження ризиків для фінансової стабільності та доброчесності, ефективності грошово-кредитної політики і стандартів конкуренції [323].

Віртуальні активи стають окремим об’єктом регулювання, який посідає особливе місце між об’єктами інтелектуальної власності та інформацією. Своєю чергою, це потребує визначення системи їхнього оподаткування, синхронізації з іншими законодавчими актами України, упровадження механізму захисту прав та інтересів інвесторів, а також розроблення гнучкої нормативно-правової бази для створення прогресивної моделі регулювання [324].

Фінансова система країни потребує розроблення ефективної та дієвої нормативно-правової бази для ринку криптоактивів. З огляду на популярність їх в Україні та потребу у воєнний час у розрахунках з іноземними партнерами, згадані обмеження НБУ ще більше віддалили ринок віртуальних послуг від легалізації та створили нові незручності для споживачів ВА, блокували діяльність операторів крипторинку та підсилили розвиток тіньового сектору економіки.

Дуже важливим є найскоріше утвердження в Україні дієвого правового поля для ВА, яке надасть змогу як бізнесу, так і громадянам здійснювати операції

з ними в регульованому, а отже, прогнозованому середовищі, отримувати безперешкодний доступ до банківської системи, декларувати доходи та сплачувати податки з них [324].

Оскільки юрисдикції та приватний сектор запроваджують Правило подорожей, вони виявляють проблеми в його впровадженні, особливо між юрисдикціями, котрі регулюють ВА та ППВА, і тими, які не регулюють («проблема сходу»).

«Проблемою сходу» (англ. «Sunrise») в останньому Керівництві FATF щодо ризик-орієнтованого підходу до ВА та ППВА, визначено проблему різних стадій імплементації міжнародних стандартів FATF у різних країнах, у нашому випадку насамперед Рекомендації FATF 15. Ринок криптоактивів є глобальним, тому різні стадії впровадження міжнародних стандартів послаблюють ефективність його регулювання навіть у тих країнах, які найбільше просунулись в імплементації міжнародних рекомендацій та вимог [325].

Крім того, юрисдикції певною мірою застосовують різні підходи до вимог цього правила, як передбачено стандартами FATF, тобто різні підходи до моніторингу холодних гаманців, правил захисту даних і визначення порогових значень операцій із ВА.

Тим часом, коли країни впроваджують технологічні рішення для реалізації Правила подорожей, в Україні навмисно затягується процес легалізації національного крипторинку. В результаті наша країна потрапляє до списку країн, що спричиняють так звану проблему сходу, яка уповільнює процес обміну інформацією на глобальному рівні, що, у свою чергу, гальмує діяльність інших країн у регулюванні ринку ВА та проведенні розслідувань злочинності, пов'язаної з їх оборотом.

Зниження рейтингу впровадження 15-ї Рекомендації FATF до рівня «не впроваджено» для України на черговому 6-му раунді проведення взаємних оцінок MONEYVAL, який призначено на кінець 2025 р., може призвести до

серйозних негативних наслідків як для фінансового ринку країни, так і для зовнішньоекономічної діяльності вітчизняних підприємств.

Неповне виконання Рекомендації 15 FATF, яка стосується Правила подорожей і запобігання використанню криптовалют для незаконних трансакцій, ставить під загрозу довіру міжнародних партнерів до фінансової системи України. Це може спричинити зниження привабливості країни для іноземних інвесторів, а також введення додаткових обмежень або санкцій з боку міжнародних фінансових інститутів і партнерів. Зокрема, зниження рейтингу здатне стати перепоною для інтеграції українських фінансових установ у міжнародну фінансову систему, ускладнити доступ до фінансових ринків, а також обмежити можливості вітчизняних підприємств у залученні інвестицій або веденні бізнесу із закордонними партнерами.

Усі Рекомендації FATF тісно взаємопов'язані, оскільки формують комплексну систему заходів, спрямованих на ПВК/ФТ на глобальному рівні. Зниження рейтингу впровадження однієї рекомендації безпосередньо впливає на загальну оцінку ефективності виконання стандартів FATF в Україні. Оскільки кожна рекомендація доповнює та підтримує інші, їх неефективне впровадження призводить до послаблення загальної системи протидії фінансовим злочинам.

Такий негативний вплив може не тільки обмежити доступ України до міжнародних фінансових ринків, а й погіршити загальну репутацію країни в очах партнерів, зокрема інвесторів, банків і торгових компаній. Як результат, підприємства зазнаватимуть труднощів при провадженні зовнішньоекономічної діяльності, а фінансова система країни стикнеться з підвищеними ризиками та недостатнім захистом від злочинних і терористичних фінансових потоків. Одним із найбільших ризиків є припинення операцій на кореспондентських рахунках українських банків із іноземними фінансовими установами.

Кореспондентські рахунки є важливим інструментом виконання міжнародних фінансових операцій. Вони дають змогу банкам здійснювати перекази коштів між країнами, а також забезпечують можливість приймати та

відправляти платежі в іноземних валютах. У разі зниження рейтингу і потрапляння України до списку підвищеного моніторингу з боку MONEYVAL іноземні фінансові установи можуть почати утримуватися від ведення кореспондентських рахунків з українськими банками через підвищення ризиків порушення міжнародних стандартів, що призведе до втрати довіри до банківської системи України [399].

Це, у свою чергу, спричинить суттєві обмеження в міжнародних платежах, ускладнить доступ до міжнародного фінансування та призведе до збільшення витрат для українських підприємств, що займаються зовнішньоекономічною діяльністю. Припинення операцій на кореспондентських рахунках також може обмежити здатність банків обробляти трансакції у іноземних валютах, що вплине на стабільність фінансової системи в цілому.

Отже, зниження рейтингу навіть одного стандарту може серйозно загрожувати національній економіці, оскільки ставить під сумнів загальний рівень дотримання міжнародних стандартів FATF, та стимулювати негативні економічні тенденції, зокрема втрату довіри до фінансових інститутів, погіршення умов ведення бізнесу та зростання фінансових ризиків для підприємств.

3.2. Удосконалення механізмів тестування української цифрової валюти та перспективи її впровадження

Технологія блокчейн, покладена в основу побудови цифрових фінансів, каталізує далекосяжні зміни грошей і фінансів, які глибоко вплинуть на домогосподарства, корпорації, інвесторів, центральні банки та уряди. Це система запису та передачі інформації, що дає змогу зберігати дані у вигляді ланцюжка блоків. Кожен блок містить інформацію про певну кількість трансакцій та хеш

попереднього блоку і, таким чином, забезпечує взаємозв'язок із попереднім блоком, що утворює ланцюжок. Блокчейн, дозволяючи безпечно володіти суто цифровими об’єктами, сприяє зростанню нових цифрових активів, таких як незамінні токени.

Цифрові гроші розвиваються вже деякий час. Через нові технології сподіваються демократизувати фінанси та розширити доступ до фінансових продуктів і послуг. Ключова мета полягає в досягненні набагато дешевших, миттєвих внутрішніх і міжнародних платежів.

Не кожна форма цифрових грошей виявиться життєздатною. Криптовалюти, такі як біткоїн, не можуть бути грошима [344]. Криптовалюти, такі як біткоїн, не можуть бути грошима. Останнє значне падіння вартості криптовалют відбулося в лютому 2025 року. Тоді ринок зазнав рекордних втрат, спричинених новими тарифами, запровадженими президентом США Дональдом Трампом проти Канади, Мексики та Китаю. Це призвело до ліквідації позицій на суму $2,2 млрд. Bitcoin впав до $91 000, а Ethereum втратив 20% вартості.

Раніше, в серпні 2024 року, криптовалютний ринок також зазнав значного триденного падіння, втративши приблизно $500 млрд. Це сталося на тлі слабких даних щодо зайнятості та побоювань рецесії в США. Bitcoin та Ethereum тоді втратили 20% та 28% вартості відповідно за тиждень.

Варто зазначити, що хоча ці падіння були значними, вони не досягали рівня втрати двох третин вартості криптовалют. Останній раз подібне масштабне зниження відбулося в 2018 році під час так званої «криптозими», коли Bitcoin втратив понад 80% своєї вартості від пікових значень. Хоча ними активно торгують і на них активно спекулюють, ціни на такі інструменти відокремлені від будь-якої основної економічної вартості. Для того щоб стримувати волатильність, розроблено стейблкоїни, але багато з них виявилися зовсім нестабільними й залежать від якості резервних активів, що їх забезпечують [344].

Однак децентралізовані фінанси (DeFi) і криптовалюта не тільки збережуться, а й, на нашу думку, можуть вирішити проблеми реального світу,

такі як енергетична криза. Регулювання є ключовим у тому, щоб навести лад на ринках і забезпечити безпечний простір для інновацій. Тим часом центральні банки розглядають питання створення власних цифрових валют.

За словами голови Банку міжнародних розрахунків Августіна Карстенса та його колег Джона Фроста і Хьон Сон Шина, «центральні банки повинні використовувати технологічні інновації, які пропонує криптовалюта, а також забезпечувати основу довіри» [326]. За допомогою відповідально розроблених цифрових валют центрального банку можна керувати ризиками конфіденційності та кібербезпеки.

Поки рано говорити, як буде розвиватися цифровий ландшафт. Але з правильною політикою та регуляторним вибором можна уявити майбутнє, в якому поєднуватимуться державні й приватні валюти, що безпечно зберігаються в цифрових гаманцях мільярдів людей.

Багато українських та зарубіжних дослідників звертають увагу на вивчення різних аспектів як функціонування, так і регулювання і приватних ВА, і цифрових валют центральних банків.

Цифрова валюта центрального банку (CBDC) – цифрова форма фіатних грошей, що вже емітовані центральним банком і є загальнодоступним законним платіжним засобом на території країни. Відповідно до комбінацій властивостей CBDC поділяють за таким призначенням: як цифровий еквівалент готівки; для міжбанківських розрахунків; як інструмент монетарної політики; як еквівалент рахунку, відкритого в центральному банку.

Офіційно загальні засади випуску та використання в Україні цифрових грошей Національного банку України (НБУ) та відмежування їх від електронних грошей було закріплено Законом України «Про платіжні послуги» від 30.06.2021 [327], який став результатом імплементації європейського законодавства. Зокрема, відповідно до п. 96 ст. 1 Закону «цифрові гроші Національного банку України являють собою електронну форму грошової одиниці України, емітентом якої є Національний банк України». Це відрізняє їх від одиниць вартості, що

зберігаються в електронному вигляді, випущених емітентом електронних грошей для виконання платіжних операцій (у тому числі з використанням наперед оплачених платіжних карток багатоцільового використання), які приймаються як засіб платежу іншими особами, ніж їхній емітент, та є грошовим зобов'язанням такого емітента електронних грошей [327, п. 14 ст. 1].

Водночас слід звернути увагу на те, що Закон України «Про платіжні послуги» досить декларативно підходить до регулювання особливостей випуску та використання цифрової валюти. Зокрема, нормативно-правовий акт наголошує на тому, що відповідна валюта може бути емітована НБУ виключно в безготівковій формі та використовуватися суб'єктами господарювання, а також звичайними громадянами. При цьому порядок випуску та зберігання цифрових грошей, а також особливості виконання платіжних операцій із їх застосуванням мають визначатися нормативно-правовими актами НБУ [327, ст. 62].

Незважаючи на те, що минуло майже чотири роки після прийняття та набуття чинності Законом України «Про платіжні послуги», подальші кроки щодо реалізації згаданої вище статті з боку регулятора (НБУ) відбуваються досить повільно. Так, лише 28 листопада 2022 р. НБУ презентував представникам банків, небанківських фінансових установ та ринку ВА для обговорення та отримання зворотного зв'язку проєкт концепції е-гривні – цифрових грошей Національного банку України.

Наразі регулятор розглядає й опрацьовує такі можливі варіанти використання е-гривні, від яких залежатимуть її дизайн та основні характеристики:

- е-гривня для роздрібних безготівкових платежів з можливістю функціонування «програмованих» грошей: для здійснення цільових соціальних виплат, зменшення державних витрат на адміністрування та контроль за цільовим використанням коштів, а також для використання технології смарт-контрактів, яка дає змогу програмувати різноманітні логіки розрахунків залежно від настання певних обставин та фактів;

- е-гривня для використання у сфері, пов’язаній з обігом ВА (наприклад, для обміну, забезпечення випуску та інших операцій з віртуальними активами). Е-гривня може стати одним із ключових елементів якісного розвитку інфраструктури ринку ВА в Україні;
- е-гривня для забезпечення можливості здійснення транскордонних платежів, що забезпечить проведення транскордонних платежів більш швидко, дешево та прозоро.

У звіті НБУ зазначалося, що анонімність клієнтів несе небезпеку посилення тіньової економіки та незаконної діяльності, тобто порушення вимог ПВК/ФТ). Тому впровадження е-гривні буде супроводжуватися заходами фінансового моніторингу: очікується інтеграція цифрової валюти у чинну систему національного законодавства щодо ПВК/ФТ та фінансового моніторингу. Вже прийнятий Закон України «Про платіжні послуги» визначив е-гривню як електронну форму національної валюти, що випускається НБУ, тим самим заклавши правову основу для регулювання її обігу [327].

Цифрова ідентифікація та ЗСК відіграють ключову роль в екосистемі CBDC. Багато країн спираються на існуючі національні ID-рішення: наприклад, у Китаї це прив’язка до телефону/банку, в Нігерії – до NIN/BVN, в Україні потенційно буде використано систему BankID або додаток «Дія» для верифікації громадян. ЄС в контексті цифрового євро також розробляє загальноєвропейську цифрову ідентифікацію (eIDAS 2.0), яка може стати фундаментом для відкриття цифрових євро-гаманців з високим рівнем довіри. Надійна цифрова ID дозволяє зробити ЗСК дешевшим та швидшим, а отже зменшує навантаження на користувачів і на посередників. До того ж, наявність єдиної ID платформи полегшує обмін інформацією між банками і регуляторами при розслідуваннях.

Спільною рисою національних стратегій запуску CBDC є вбудування принципів ризик-орієнтованості ПВК/ФТ безпосередньо у дизайн цифрової валюти. Майже всі розглянуті проєкти – від е-гривні до цифрового євро чи eNaira – реалізують концепцію диференційованих рівнів доступу. Це означає, що

ступінь перевірки особи та обсяг зібраних даних прямо пропорційні розмірам сум, з якими оперує користувач [342].

Така модель забезпечує досягнення двох цілей одночасно: з одного боку, спрощення доступу (і, як наслідок, фінансова інклюзія) для широких верств населення, а з іншого – строгий контроль за великими операціями та більш ризикованими клієнтами. Центральні банки та регулятори фактично адаптують перевірену практику банківського нагляду: клієнти з низьким ризиком (малі рахунки, соціально вразливі групи) підпадають під спрощений належний нагляд, тоді як клієнти з вищим ризиком (великі кошти, міжнародні перекази) – під розширений нагляд [342].

Аналітичні інструменти для оцінки ризиків у контексті CBDC при проєктуванні системи включають як попередню оцінку, так і поточний моніторинг транзакцій. При плануванні запуску цифрової валюти регулятори проводять НОР, враховуючи специфіку нових продуктів. Так, Багами і Нігерія перед запуском своїх CBDC аналізували ризики відмивання коштів у небанківських сегментах та встановлювали ліміти, виходячи з прийнятного рівня ризику для не клієнтів банків.

У процесі експлуатації CBDC велика увага приділяється моніторингу трансакцій у режимі реального часу. Оскільки CBDC – це повністю цифрові гроші, вони апріорі більш трасовані, ніж готівка. Багато центральних банків очікують, що CBDC підвищать прозорість фінансових потоків і спростять виявлення підозрілих операцій.

Наприклад, у разі впровадження е-гривні всі перекази відображатимуться в централізованій системі або розподіленому реєстрі під контролем НБУ – це створює можливості для використання алгоритмів і AI для аналізу трансакційних даних. Сучасні комплаєнс-системи вже переходять від простих правил до моделей, що враховують багато факторів ризику та використовують машинне навчання [321]. Такі системи зможуть відслідковувати незвичні моделі

поведінки, наприклад, дроблення трансакцій (smurfing), часті перекази на невідомі гаманці і сигналізувати про це фінансовій розвідці.

Правило подорожі та співпраця з правоохоронними органами забезпечують, щоб жодна трансакція була виявлена при переміщенні між різними системами. Якщо CBDC використовуватиметься лише всередині країни, Правило подорожі дещо втрачає актуальність, адже всі перекази і так проходять у межах єдиної платформи. Проте при крос-граничних платежах CBDC (такі проєкти вже тестуються, наприклад, між Китаєм, Гонконгом, ОАЕ та Таїландом у проєкті mCBDC Bridge) правила FATF щодо передачі інформації будуть критично важливими.

Національні стратегії передбачають, що CBDC будуть сумісні з вимогами міжнародних переказів SWIFT/SEPA, тобто до повідомлення про переказ у цифровій валюті включатимуться необхідні дані про відправника і одержувача, аналогічно сучасним банківським платіжкам. Законодавці ЄС, наприклад, вже зараз обговорюють, щоб цифровий євро мав вбудовані механізми відповідності Правила подорожі принаймні на рівні порогової для моніторингу суми 10 000 євро [329].

Співпраця з правоохоронними органами та фінансовими розвідками є невід'ємною частиною запуску CBDC. У багатьох країнах центральні банки спільно з ПФР розробляють процедури обміну інформацією: від автоматичного надсилання звітів про підозрілі транзакції (STR/SAR) до надання спеціального доступу до певних даних. Наприклад, у Японії розглядається можливість створення єдиного сховища ЗСК-даних, що полегшить правоохоронцям отримання потрібної інформації по запиту [51]. В Китаї оскільки система централізована правоохоронці мають технічну можливість в реальному часі відстежувати великі рухи e-CNY [47].

В Україні НБУ ймовірно інтегрує е-гривню з існуючою системою фінансового моніторингу НБУ та Держфінмоніторингу, що дозволить швидко

блокувати підозрілі операції або заморожувати кошти за рішенням суду/органів, аналогічно тому, як це робиться з банківськими рахунками.

Український підхід до впровадження е-гривні значною мірою відповідає міжнародним стандартам. Його головна мета — запобігти послабленню режиму ПВК/ФТ через використання цифрової валюти, а навпаки — застосувати сучасні технології для посилення контролю в необхідних сферах. Ризик-орієнтований підхід реалізується шляхом обмеження анонімності для невеликих сум та обов'язкової ідентифікації для значних транзакцій, використання національної цифрової ідентифікації для процедур ЗСК, а також впровадження лімітів та алгоритмів моніторингу операцій.

Міжнародний досвід підтверджує ефективність такої моделі. Кожна країна враховує власний контекст, зокрема рівень фінансової інклюзії, технологічну готовність та правову систему, проте всі приходять до подібного набору інструментів: багаторівневі акаунти, цифрова ідентифікація, транскордонні правила обміну даними та тісна співпраця з органами фінансової безпеки. Це забезпечує інтеграцію CBDC як інноваційного та безпечного елемента глобальної системи протидії фінансовим злочинам.

У відповідь на занепокоєння доступу приватного сектору до функціонування платіжних структур особливо під час періоду фінансових потрясінь центральні банки розглядають можливість випуску цифрових форм грошей центрального банку для роздрібних платежів [332]. Аргументи за впровадження роздрібних CBDC не настільки переконливі. Зазвичай це цифрова валюта, яку випускає центральний банк для широкої публіки, але вона відрізняється від інших регульованих цифрових валют, таких як стейблкоїни або токенізовані банківські депозити, тим, що є зобов'язанням центрального банку.

Цікавість до роздрібних CBDC раптово зросла в останні роки, і багато центральних банків проводять експерименти з ними. Є три основні аргументи на користь роздрібних CBDC [333].

По-перше, роздрібний CBDC забезпечить прямий доступ до державних грошей в цифровій економіці, де готівка втрачає свою актуальність. Однак відмінності між зобов'язаннями центральних банків і комерційних банків, як правило, не мають суттєвого значення для більшості людей, поки вони впевнені у безпеці своїх грошей та в тому, що центральні банки готові підтримувати систему під час криз. Для України це може стати новим кроком програми розвитку безготівкових платежів та інших ініціатив НБУ, що стосуються cashless-системи, яка знайшла відображення в реалізацію Стратегії розвитку фінтеху в Україні до 2025 року та Закону України «Про платіжні послуги» [327].

По-друге, роздрібна CBDC може виступати обмеженням монополії, яку мають банки або постачальники електронних гаманців у сфері роздрібних платежів. Але існують інші шляхи підвищити конкуренцію та забезпечити відповідність платіжних систем необхідним стандартам.

По-третє, роздрібна CBDC може забезпечити більшу конфіденційність і контроль над особистою інформацією та трансакціями, ніж сучасна система електронних платежів. Проте вдосконалення правил або законодавства для захисту конфіденційності користувачів і забезпечення надійного управління даними може бути альтернативою випуску роздрібних CBDC.

Роздрібні електронні платіжні системи швидкі, ефективні та безкоштовні, тоді як залишкова сума готівки збережеться в обігу і навряд чи зникне. Говорити надто категорично про майбутній розвиток цих різноманітних інновацій було б необачно. Центральні банки та регулятори повинні здійснювати постійний моніторинг тенденцій за допомогою таких інтернет-ресурсів, як CBDC Tracker [57]. Today's Central Bank Digital Currencies Status або CBDC Tracker фінансується за рахунок гранту від HRF, розроблений Peak Shift та створений стипендіатами CBDC Tracker [336].

За станом упровадження CBDC на травень 2024 р. найбільша кількість країн (107) перебувають на стадії дослідження (позначено зеленим кольором на рис. 3.2), 27 країн – обґрунтування запуску власної CBDC (позначено фіолетовим

кольором на рис. 3.2), 21 країна вже запустила пілотний проєкт (позначено помаранчевим кольором на рис. 3.2), у 4 країнах їхні CBDC вже працюють (позначено блакитним кольором на рис. 3.2) і 7 країн відмовились від упровадження CBDC (позначено червоним кольором на рис. 3.2).



Рис.3.2. Поточний статус впровадження CBDC в країнах світу.

Джерело: CBDC Tracker [57].

Доцільним є детальніший аналіз держав, які вже впровадили CBDC (Ямайка, Зімбабве, Нігерія та Багамські Острови), а також країн, що відмовилися від їхнього використання, серед яких Філіппіни, Кенія, Данія, Кюрасао, Сінгапур, Еквадор та Фінляндія.

Можна уявити майбутнє, в якому екосистема цифрових активів стане постійною складовою фінансового ландшафту, співіснуючи із сучасною системою, що базується на посередницькій діяльності. Традиційні фіатні валюти лишатимуться основними, але важливу роль забезпечення відіграватимуть приватні стейблкоїни та оптові CBDC. Імовірно, CBDC матимуть ключове значення у транскордонних платежах і розрахунках. Роздрібні CBDC можуть стати невеликим складником грошової бази з функцією, подібною до теперішньої ролі готівки.

І транскордонні розрахунки, і готівка підвищують на традиційних фінансових ринках ризик використання їх у злочинній діяльності, особливо в ВК.

Щодо CBDC, то вони підвищують прозорість операцій за рахунок блокчейн-технології, містять у собі процедури ПВК/ФТ, такі як ідентифікація та верифікація клієнта, оцінка його ризиковості клієнта та діяльності.

Причому з розвитком цифрових технологій, ці процедури виконуються в мережі Інтернет у віддаленому режимі. Для оптимізації процедур ПВК/ФТ та ефективного розподілу ресурсів відповідно до РОП автором дисертації запропоновано процедури комплаєнсу в ліцензованій діяльності ППВА впроваджувати за допомогою програмних продуктів блокчейн-аналітики. Завдяки програмному забезпеченню процедури оцінки ризику клієнта та його операцій також будуть автоматизовані [287–289].

Відповідно до принципів блокчейн-аналітики ідентифікація учасників операцій з ВА можлива завдяки фінансовим обмінним операціям, що здійснюються банківськими та платіжними установами, централізованими криптовалютними біржами та ППВА.

Наразі увага акцентується на трансакціях у DeFi, і ми вже зазначали, що послуги фінансових ринків вже адаптовані до цього сегмента децентралізованої цифрової економіки і працюють у ній. Тому через упровадження державного регулювання та регулювання на глобальному рівні такі компанії є також носіями інформації про своїх клієнтів.

Серед найактуальніших питань, на яких наголошується в загальнодоступних звітах як Європейського Союзу, так і США щодо впровадження цифрової валюти, виокремлюються такі:

– доцільність залучення посередників;

– важливість дотримання політики ЗСК і процедур ПВК/ФТ з одночасним дотриманням законів і нормативних актів про фінансову конфіденційність;

– характер і ступінь захисту конфіденційності, що надається фізичним особам за допомогою загальнодоступних DLT, таких як технологія блокчейн.

Крім того, залишаються невирішеними питання щодо:

– обрання централізованої чи децентралізованої моделі бухгалтерської книги обігу цифрової валюти;

– визначення суб'єктів, котрі матимуть доступ до ідентифікаційної інформації та даних про трансакції, зібраних і збережених у системі CBDC, і обмежених обставин, за яких до них можна отримати доступ;

– особливостей реагування системи CBDC на витоки даних або інші інциденти безпеки даних і відповідності вимогам звітування про витоки даних (як усередині країни, так і в усьому світі).

Стосовно доцільності залучення посередників, слід відзначити наявність різних підходів у відповідному напрямі. Водночас, якщо розглянути проєкти CBDC у світі, то з 11 запущених на міжнародному рівні CBDC усі їх країни-емітенти обрали посередницьку структуру. З 15 систем CBDC, які вступили в пілотну фазу, лише вісім чітко прийняли посередницьку модель, а решта все ще розглядають її переваги та ризики на противагу моделі без посередників (яка дає змогу фізичним та юридичним особам відкривати рахунки безпосередньо в установах центрального банку). Серед яскравих прикладів посередницької моделі слід виокремити пілотні проєкти CBDC Китаю, Норвегії, Швеції.

Так чи інакше, модель із можливістю збереження за банками (або їхньою частиною) функції посередників між центральним банком та індивідуальними власниками валюти, що мають рахунки в CBDC, здається більш прийнятною. Адже вона гарантуватиме непорушність балансу між доступністю конфіденційної інформації та захистом приватних інтересів і відповідатиме чинному законодавству України:

– про ПВК/ФТ, відповідно до якого банки, уповноважені оператори платіжних систем є суб'єктами первинного фінансового моніторингу, а суб'єктом державного фінансового моніторингу в цьому випадку є НБУ [422, ст. 76];

– збереження та порядку поширення персональних даних [337, ст. 14–16]) і розголошення банківської таємниці [337, ст. 60–63].

Практика впровадження українськими банками програм комплаєнсу для забезпечення виконання всіх міжнародних і державних вимог конфіденційності та безпеки даних напрацьовується вже тривалий час. Наприклад, глобальні фінансові установи зазвичай мають надійну інфраструктуру найвищого рівня для перевірки особи кожного власника рахунку відповідно до вимог щодо захисту інформації про клієнтів та моніторинг підозрілих трансакцій згідно з вимогами ПВК/ФТ та політики ЗСК.

У випадку, коли НБУ бере на себе обов'язок відкривати й обслуговувати рахунки в CBDC або обирає задля цих цілей іншу централізовану установу, виникає потреба в розробленні та впровадженні програм захисту даних і дотримання фінансової конфіденційності для безпеки нових власників рахунків з нуля. Більш практичним підходом з боку регулятора в такому разі видається використання для цих функцій приватного сектору [72].

Зважаючи на викладене, модель CBDC України має бути розроблена аналогічно до посередницької системи е-крони, але з однією ключовою відмінністю – обрані фінансові установи – посередники повинні підключатися до великої мережі CBDC лише через власну IT-інфраструктуру. Іншими словами, уповноважені оператори повинні бути фізично заблоковані від підключення до системи CBDC через IT-інфраструктуру НБУ. Крім того, корисними для застосування на національному рівні є законодавчі напрацювання Норвегії щодо технічного забезпечення випуску й обігу такого виду валюти.

Після з'ясування того, що посередництво є не лише бажаним, а й необхідним із правових та регуляторних міркувань, постає таке питання: Україна має додатково дослідити, чи може національна система CBDC працювати за допомогою різних типів технології розподілених реєстрів (Distributed ledger technology, DLT)), дотримуючись національних і глобальних вимог до конфіденційності інформації та захисту персональних даних?

Будь-який майбутній вибір у відповідному напрямі має базуватися на визначенні кола суб'єктів, котрі матимуть доступ до ідентифікаційних даних, і

конкретних обставин виникнення такого доступу, а також особливостях управління доступом до інформації, щоб захистити окремих учасників системи CBDC від незаконного розкриття їхньої особистої та фінансової інформації або юридичної відповідальності, пов'язаної з доступом до даних.

Основною перешкодою, з якою НБУ стикнеться при розробленні національної моделі цифрової валюти, що перебуває в основі проблем конфіденційності особистих даних і трансакцій, є те, чи повинна система працювати шляхом запису і відстеження трансакцій у централізованому реєстрі, що ведеться одним органом, або децентралізованому реєстрі, що ведеться і може бути змінений усіма учасниками, підключеними до мережі CBDC.

Якщо буде обрано децентралізовану модель, то перед НБУ постане питання, чи буде доступ до реєстру та історії реєстру публічним, приватним або з обмеженим доступом. У випадку застосування публічного реєстру інформація в ньому буде загальнодоступною для всіх учасників, що є активними в мережі CBDC (включно з кінцевими користувачами); приватного реєстру – доступ до інформації в ньому матиме лише обрана підгрупа приватних суб'єктів господарювання. У свою чергу, застосування реєстру з обмеженим доступом надає можливість отримання інформації з нього за умови отримання відповідного дозволу адміністратора.

Чи може гіпотетична модель цифрової гривні бути спроєктована таким чином, щоб скористатися інноваційними перевагами DLT, одночасно дотримуючись національних і глобальних законів і правил про конфіденційність? Те, що робить цифрові активи настільки привабливими для широкої громадськості як форма оплати, – це можливість здійснювати прямі та миттєві трансакції між одноранговими партнерами в анонімний спосіб, подібний до готівки, а також відстежувати та перевіряти дійсність усіх трансакцій за допомогою анонімного публічного реєстру.

Водночас повна анонімізація всіх трансакцій цифрової гривні та використання DLT може потенційно суперечити національному законодавству,

зокрема Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [419]. Вимога до уповноважених операторів повідомляти про підозрілі операції унеможливлює розроблення системи е-гривні, яка працює на основі децентралізованого, публічного та такого, що не потребує, реєстрації реєстру з повною анонімністю ідентифікаційних даних.

Розглядаючи деякі потенційні рішення, що враховують конфіденційність, варто зауважити таке. Насамперед система е-гривні могла би працювати на основі моделі централізованого реєстру, так само, як сьогодні функціонує платіжна система України, таким чином повністю уникаючи юридичних проблем, пов'язаних із DLT. За цієї моделі лише обрані банки-учасники матимуть доступ до реєстру трансакцій та його історії.

Централізована модель гарантує, що лише банки матимуть повноваження щодо деталей трансакцій та ідентифікаційних даних із метою дотримання вимог законодавства, забезпечуючи при цьому захист усіх персональних даних та даних про трансакції, які перебувають у руках обраних фінансових установ, що мають інфраструктуру для захисту приватності, та обмежуються ними. Централізована модель усуне будь-яку потенційну дисгармонію з європейським загальним регламентом захисту даних GDPR, якщо система буде доступною для резидентів ЄС або сумісною з системами CBDC ЄС у майбутньому. Зрозуміло, централізована модель е-гривні була би шляхом найменшого опору.

Як варіант НБУ може розглянути можливість функціонування системи цифрової гривні через приватну та дозволену платформу DLT, де деталі трансакцій цифрової валюти, що не відстежуються та не ідентифікуються, будуть доступні в приватному реєстрі для уповноважених фінансових установ-посередників. Однак ідентифікаційні дані про трансакції е-гривні повинні бути доступні для всіх фінансових установ-посередників (наприклад, через

високозахищену криптографічну технологію) з метою забезпечення відповідності програмам дотримання законодавства.

Уповноважені оператори-посередники після проведення всіх процедур на етапі відкриття рахунку можуть присвоювати випадково згенерований псевдонім кожному рахунку кінцевого користувача, який відображатиметься в приватній книзі протягом певного періоду (наприклад, псевдонім на один день).

Таким чином, уповноважені банки-посередники зможуть бачити суми трансакцій, пов'язані з випадково згенерованими щоденними ідентифікаторами рахунків, подібно до концепції псевдонімів e-krona [75], які самі по собі не можуть бути відстежені до конкретних кінцевих користувачів. Фінансові установи зможуть застосовувати наявні інструменти спостереження до частково анонімної приватної книги системи CBDC для виконання своїх обов'язків щодо спостереження та повідомлення про підозрілу діяльність або діяльність, що перевищує певні номінальні порогові значення, які підлягають повідомленню. Якщо фінансові установи підозрюють у книзі будь-яку злочинну або іншу підозрілу фінансову діяльність, пов'язану з призначеними псевдонімами, вони повинні мати можливість зіставити анонімну інформацію про псевдонім із конкретним власником рахунку, коли це необхідно для цілей звітності ПВК/ФТ.

НБУ може розглянути низку технологічних рішень для надійного блокування псевдонімів, одночасно надаючи можливість цільового зіставлення ідентифікаційних даних. Наприклад, Всесвітній економічний форум випустив серію довідкових документів з управління цифровими валютами, в яких розглядаються потенційні «методи підвищення конфіденційності для фінансових установ», включно з різними видами «криптографії», що можуть безпечно блокувати й розблоковувати ідентифікаційні дані та дані про трансакції. Ці криптографічні методи включають докази з нульовим знанням, криптографію із симетричним та асиметричним ключем, диференціальну конфіденційність та гомоморфне шифрування [339].

Підсумовуючи, можна зазначити, що питання конфіденційності, зумовлені DLT, є відносно новими і дуже складними. Якщо порівнювати їх з іншими режимами захисту даних у світі, такими як GDPR, ці проблеми конфіденційності стануть ще складнішими мірою розвитку технологій. З огляду на таку невизначеність доцільно, щоб Україна разом з іншими державними установами, які беруть участь у дослідницькому проєкті CBDC, активно долучалася до міжнародного діалогу та спільних досліджень, спрямованих на розроблення системи, орієнтованої на захист приватності. Створення системи, яка, наприклад, не відповідає вимогам GDPR, обмежить її довговічність і життєздатність у глобальній платіжній системі.

Як кандидат на вступ до Європейського Союзу Україна повинна привести національне законодавство у відповідність до європейських стандартів, зокрема, до Стратегії цифрових активів ЄС. Це передбачає адаптацію вітчизняного правового поля до європейських вимог, зокрема до законодавства, що регулює технологію розподіленого реєстру (DLT) та цифрові активи. Правовий документ ЄС, який регулює цю сферу [80], створює підґрунтя для формування національних норм, що дасть змогу Україні інтегруватися в глобальні фінансові процеси та забезпечить правову основу для розвитку цифрових активів, їхнього обігу та регулювання.

Донедавна у сфері кібербезпеки та діяльності центральних банків було проведено небагато публічних досліджень, спрямованих на вивчення конкретних ризиків кібербезпеки та конфіденційності, пов’язаних із CBDC. Також рідко розглядалося питання про те, чи можуть CBDC не тільки зменшити ризики, а й підвищити рівень кібербезпеки фінансової системи. Дослідження, опубліковане в останньому звіті Атлантичної ради під назвою «Відсутній ключ – виклик кібербезпеки та CBDC», аналізує нові ризики для кібербезпеки, які CBDC можуть спричинити для фінансових систем, і доводить, що політики мають широкі можливості для безпечного впровадження CBDC [79]. Існує

багато варіантів їхнього дизайну, починаючи від централізованих баз даних і закінчуючи розподіленими книгами та системами на основі токенів.

Перш ніж робити висновки щодо ризиків для кібербезпеки та конфіденційності, потрібно розглянути кожен дизайн. Ці конструкції також потрібно порівняти з поточною фінансовою системою, щоб визначити, чи можуть нові технології запропонувати безпечніші варіанти.

Багато із запропонованих варіантів дизайну для CBDC (зокрема для роздрібних) передбачають централізований збір даних про трансакції, що створює серйозні ризики для конфіденційності та безпеки. З точки зору конфіденційності ці дані можуть використовуватися для спостереження за платіжною діяльністю громадян. Накопичення такої кількості конфіденційних даних підвищує ризик безпеки, оскільки ймовірний виграш для потенційних зловмисників стає набагато більшим.

Однак ризики, пов’язані з централізованим збором даних, можна пом’якшити, якщо взагалі їх не збирати, або обравши архітектуру перевірки, в якій кожен компонент містить лише ту кількість інформації, що необхідна для функціонування. Реалізації такого підходу можуть сприяти криптографічні інструменти, зокрема докази з нульовим розголошенням, які підтверджують автентичність приватної інформації без її розкриття чи компрометації, а також методи криптографічного хешування.

Наприклад, у рамках проекту «Гамільтон» [341] (співпраця Федерального резервного банку Бостона та Массачусетського технологічного інституту для дослідження CBDC в США) розроблено систему, яка розділяє перевірку трансакцій на фази і кожна фаза потребує доступу до різних частин даних трансакції.

Ці криптографічні методи можна розширити ще більше, щоб створювати системи, які перевіряють дійсність трансакції лише за допомогою зашифрованого доступу до деталей трансакції, таких як відправник, отримувач або сума.

Хоча ці інструменти можуть здаватися надто ідеальними, вони пройшли ретельне тестування на конфіденційних криптовалютах, таких як Zcash, і ґрунтуються на значних досягненнях у сфері криптографії. Основна ідея полягає в тому, що ця технологія дає можливість центральним банкам забезпечити інтеграцію як кібербезпеки, так і захисту конфіденційності в будь-яку модель CBDC.

Загальним викликом для проєктів, що забезпечують конфіденційність (зокрема тих, які використовують спеціалізовані криптографічні методи), є зменшення рівня прозорості для регуляторів. Зазвичай регуляторні органи потребують достатнього обсягу інформації для ідентифікації підозрілих транзакцій, що можуть бути пов'язані з ВК/ФТ та іншою незаконною діяльністю.

Криптографічні методи можна застосовувати для розроблення цифрових валют центрального банку (CBDC), які забезпечують конфіденційність, схожу на готівку, до певного порога (наприклад, 10 тис. дол. США), при цьому дозволяючи державним органам здійснювати необхідний регуляторний нагляд. Такий поріг не відрізняється від системи в Сполучених Штатах, де звітність для трансакцій скорочується до 10 тис. дол. США. У такому разі новій системі CBDC не потрібно було би розробляти нові протоколи безпеки, оскільки наявні можна було б удосконалити.

Кілька країн взяли на себе зобов'язання або навіть розгорнули роздрібні CBDC, базова інфраструктура яких базується на технології розподіленої книги. Нігерійська eNaira, запущена в жовтні 2021 р., є хорошим прикладом [342]. Такі конструкції вимагають залучення третіх сторін як валідаторів трансакцій.

Це вводить нову роль для третіх сторін (наприклад, фінансових і нефінансових установ) у грошових операціях центрального банку. Важливо те, що гарантії безпеки реєстру залежатимуть від цілісності та доступності третьої сторони – валідаторів, над якими центральний банк може не мати прямого контролю, хоча можна реалізувати технологію DLT з усіма валідаторами, контрольованими центральним банком, що великою мірою перешкоджає меті

використання технології. Потенційно пов’язані ризики можуть бути зменшені за допомогою регуляторних механізмів, таких як вимоги до аудиту та розкриття порушень. Однак не існує чіткого плану розроблення цих правил у системі, що настільки чутлива до часу та настільки взаємопов’язана, як CBDC на основі DLT. Це обґрунтовує необхідність встановлення міжнародних стандартів і більшого обміну відомостями між банками, що є надзвичайно важливим у момент швидкого розвитку та впровадження е-гривні.

Протягом останнього часу деякі центральні банки передчасно вирішили, що CBDC створює надто багато ризиків для кібербезпеки та конфіденційності. Ми хотіли визначити, що насправді є загрозою, а що – можливістю. Ми дійшли висновку, що уряди мають багато варіантів дизайну CBDC на вибір, включно з новими варіантами, які ще не були повністю випробувані в поточних пілотних програмах центрального банку. Такі варіанти пропонують різні компроміси щодо продуктивності, безпеки та конфіденційності.

Уряди повинні вибрати варіант дизайну на основі потреб країни та пріоритетів політики. Виходячи з проведеної в дослідженні оцінки цих компромісів, CBDC за своєю суттю не є більш чи менш безпечними, ніж наявні системи. Однак вони вимагають відповідального проєктування з урахуванням вимог кібербезпеки.

Виконане дослідження підтверджує, що фрагментовані зусилля зі створення CBDC можуть створювати проблеми сумісності та транскордонні ризики кібербезпеки. Незалежно від того, чи вирішать країни розгорнути власні цифрові валюти, Федеральна резервна система Сполучених Штатів сприятиме розробленню глобальних стандартів для CBDC.

Як зазначалося, Європейський Союз перебуває в процесі впровадження законодавства для функціонування крипторинку (Регламент MiCA [78]), одночасно впроваджуючи єдиним пакетом Регламент DORA щодо операційної стійкості цифрових технологій у секторі фінансових послуг [81]. Він спрямований на створення всеосяжної й уніфікованої основи для гармонізації

процесів та стандартів, пов'язаних із операційною стійкістю цифрових технологій у фінансовому секторі. Крім того, оновлено Директиву 2011/16/ЄС про адміністративне співробітництво в галузі оподаткування DAC8 [82], яка вводить правила податкової прозорості для криптоактивів, що разом об’єднані в європейську Стратегію цифрових фінансів (A Digital Finance Strategy for Europe) [83].

Ця фінансова стратегія усуває прогалину в чинному законодавстві ЄС, гарантуючи, що поточна правова база не створює перешкод для використання нових цифрових фінансових інструментів і разом із тим такі нові технології та продукти підпадають під сферу фінансового регулювання й механізми управління операційним ризиком організацій, що працюють в ЄС. Таким чином, законодавчі акти спрямовані на підтримку інновацій та впровадження нових фінансових технологій, одночасно забезпечуючи належний рівень захисту споживачів та інвесторів. Сформовані європейські стандарти вже є умовами для прийняття України до спільноти країн – учасниць ЄС.

3.3. Декларування цифрових активів як елемент антикорупційної політики

Послуги, якими ми користуємося, і активи, якими ми володіємо, дедалі більше стають цифровими. Вони представлені даними, що десь зберігаються. Протягом останніх кількох років блокчейн рекламували як інструмент, що може обробляти безпечні, прозорі та незмінні трансакції цифрових активів. І там, де державні реєстри постраждали від втручання корумпованих державних службовців, блокчейн обіцяє прозорість і незмінні реєстри.

Величезні кошти було витрачено на розроблення концептуальних записок,

пілотних проєктів і тестування, щоб перевірити, чи виправдає блокчейн ті сподівання, що покладалися на нього як на антикорупційний інструмент.

Від самого початку біткоїн і блокчейн були розроблені для існування без центрального регуляторного органу. Останнім часом до криптовалюти зацікавилися державні структури. Ті самі інституції, від яких спочатку намагалися відмовитися цифрові валюти, тепер хочуть використовувати цю технологію у фінансових цілях.

У 2019 р. гігант серед соціальних медіа Facebook запустив проєкт із розроблення Libra, цифрової валюти, якою керуватиме консорціум компаній і неурядових організацій. Якщо проєкт буде реалізовано, Libra стане надійною валютою для приблизно 1,7 млрд користувачів Facebook і сприятиме створенню найбільшого банку на планеті [343]. Ніхто не знає, який вплив дещо на зразок Libra може мати на малі національні валюти. Уряди сумніваються в його потенціалі та побоюються ймовірного впливу. Тим часом кілька центральних банків досліджують, як включити національну цифрову валюту до своїх фінансових систем.

Технологія блокчейн була застосована в експериментах і пілотних проєктах у сфері управління ідентифікацією, прав на землю, відстеження походження та в логістиці. Перспективні випадки використання можна побачити в різних сферах. Управління ідентифікацією та грошова допомога біженцям у таборах зменшили трансакційні витрати та покращили відстеження коштів. Індустрія судноплавства використовує блокчейн для відстеження контейнерів і митного оформлення, щоб підвищити прозорість і прискорити рух вантажів планетою. Заявки в контексті земельних реєстрів і земельних прав натомість показали неоднозначні результати, особливо там, де є слабка цифровізація та нерозв’язані конфлікти.

Надійне підтвердження особи є фундаментальним для фінансової доступності. Блокчейн було запропоновано як технологію, що може забезпечити безпечну ідентифікацію, і в країнах, що розвиваються, тривають пілотні проєкти.

Оцифрування державних реєстрів і надання державних цифрових послуг є засобами підвищення прозорості. Захист таких реєстрів за допомогою технології блокчейн може перешкоджати корупції та фальсифікації записів.

Блокчейн може бути корисним для запобігання корупції, але лише за наявності певних передумов. Підключення, цифрова грамотність і надійні інституції є важливими для успіху цієї технології.

Поява криптоактивів (приватних цифрових активів, які переважно залежать від криптографії та технології розподіленої книги для ведення записів) зумовила впровадження безлічі фінансових інновацій, які, ймовірно, революціонізують форму грошей і способи їх використання [344]. Ці розробки створюють можливості, а також ризики. Як зазначає, наприклад, група політиків G-20, «…технологічні інновації, у тому числі ті, що покладені в основу криптоактивів, мають потенціал для підвищення ефективності та інклюзивності фінансової системи й економіки загалом», але «криптоактиви […] викликають проблеми щодо захисту споживачів та інвесторів, цілісності ринку, ухилення від сплати податків, відмивання грошей і фінансування тероризму» [345].

Псевдонімність криптоактивів (тобто трансакції вимагають лише цифрової ідентифікації) робить їх потенційним засобом для незаконних потоків, у тому числі доходів від корупції. Цей псевдонім є не внутрішньою особливістю базової технології, а радше вибором, зробленим у дизайні та практиці більшості наявних нині криптоактивів. Водночас готівка забезпечує повну анонімність, а банкноти великого номіналу є інструментом транскордонного переміщення нелегальних активів та ухилення від сплати податків [346]. Криптоактиви в їхній поточній формі дають змогу швидко переміщувати навіть більші суми з більшою легкістю в будь-яку країну світу [347]. Оскільки криптоактиви швидко набувають макроекономічної актуальності, а політики розглядають оптимальний ступінь регулювання, необхідно терміново надати емпіричні докази того, чи сприяють вони корупції. Крім того, варто дослідити, наскільки криптоактиви використовуються для обходу контролю за капіталом у країнах, де діють такі

обмеження, а також чи зросте їхня популярність у державах, де місцева валюта історично не вважалася надійним засобом збереження вартості [347].

Цим питанням присвячені дослідження таких іноземних науковців та аналітиків як Есвар С. Прасад, Кеннет Рогофф, Граф фон Клеменс Люкнер, Кармен М. Рейнхарт, Рене Чу, Адріаніт Ібрагімі, Аріф Беса [227; 348; 346; 347: 364].

Існують також потенційні переваги технологій, на яких базуються криптоактиви. Зокрема, розумно розроблені цифрові валюти центрального банку можуть запропонувати додаткову стійкість, безпеку та доступність із меншими витратами [348]. Ці технології також можна використовувати для покращання прозорості та ведення записів для закупівель або інших платежів, пов’язаних з урядовими проєктами, тим самим підвищуючи підзвітність і зменшуючи простір для корупції. Так само можна вдосконалити системи власності та реєстру, зменшивши бюрократичну тяганину й оптимізувавши процеси. Однак наразі ці ініціативи менш просунуті чи поширені, ніж криптоактиви.

Емпіричне дослідження факторів, які сприяють зростаючому використанню криптоактивів, перебуває на початковій стадії через обмеженість даних. Ми аналізуємо взаємозв'язок між використанням криптоактивів і такими показниками, як корупція, контроль за капіталом, висока інфляція в минулому та іншими факторами. Результати дослідження показали, що використання криптоактивів значною мірою позитивно корелює з рівнем корупції та контролем за капіталом. Оскільки вибірка є невеликою, а якість даних про криптоактиви невизначена, наші висновки слід інтерпретувати з обережністю. Також варто зауважити, що помилка вимірювання зазвичай зменшує ймовірність виявлення істотного емпіричного зв'язку, тому важливо звертати увагу на результати навіть за умов низької якості даних. З огляду на ці застереження та необхідність термінових дій, не чекаючи на переконливі докази, логічно вважати, що результати дослідження надають підстави для підтримки регулювання криптоактивів, зокрема впровадження підходів типу ЗСК.

Використані базові дані про використання криптовалюти отримано від Statista [349], який зібрав їх у рамках свого Глобального опитування споживачів у 2020 р., що охопило по 2000–12 000 респондентів у 55 країнах (ми не можемо підтвердити, чи є респонденти представниками всього населення). Змінна стосується частки респондентів, які вказали, що володіють або користуються криптовалютами. З огляду на нерівний розподіл змінної, щоб зменшити вплив кількох країн із великою часткою використання криптовалюти, в аналізі ми використовуємо логарифм одиниці плюс частка користувачів у загальній кількості населення.

Наявні ще чотири інших джерела даних, які, однак, мають методологічні недоліки. У звіті Chainalysis Geography of Cryptocurrency за 2024 р. наведено Глобальний індекс упровадження криптовалюти за липень 2023 р. – червень 2024 р., побудований за дещо складнішою формулою [350].

Індекс складається з п’яти показників:

– вартість криптовалютних активів, отриманих через централізовані біржі, зважена за паритетом купівельної спроможності (ПКС) на одну особу;

– вартість роздрібних криптовалютних активів, отриманих через централізовані біржі, зважена за ПКС на одну особу;

– обсяг торгівлі на P2P-біржах, зважений за ПКС на одну особу та кількістю інтернет-користувачів;

– вартість криптовалютних активів, отриманих через DeFi-протоколи, зважена за ПКС на одну особу;

– вартість роздрібних активів, отриманих через DeFi-протоколи, зважена за ПКС на одну особу.

Усі п’ять показників зважено за ВВП на одну особу. Третій показник також зважений кількістю користувачів інтернету.

Заради повноти та прозорості ми повторили нашу оцінку з використанням даних Chainalysis, але вважаємо їх менш надійними. Другий альтернативний набір даних від Finder базується на опитуваннях із ще більшою вибіркою

учасників у кожній країні, але охоплює лише 27 країн [351] порівняно з вибіркою Chainanalysis по 154 країнах світу, що дасть недостатній ступінь свободи в регресії. Третій і четвертий альтернативні набори даних — Global crypto acceptance (Triple A) [352] і Coin Dance [353] — мають серйозні недоліки (наприклад, застосування основного припущення, яке базується лише на прикладі Канади та охоплює тільки обсяг біткоїнів). Ми не проводили регресійну оцінку з використанням цих трьох останніх джерел даних. Ці різні набори даних не дають узгодженої картини, оскільки рейтинги, що вони містять, слабо або зовсім не корелюють.

Список потенційних пояснювальних змінних відображає основні можливі стимули до використання криптоактивів, а контрольна змінна (захищені інтернет-сервери) використовується для відображення здатності брати участь у трансакціях з криптоактивами. Змінні включають Індекс контролю за корупцією за Всесвітніми індикаторами управління. Індекс коливається від -2,5 до 2,5 і складається із сукупного показника, який поєднує погляди багатьох підприємств, громадян і експертів, респондентів опитування в промислово розвинутих країнах і країнах, що розвиваються. Він базується на більше ніж 30 окремих джерелах даних, створених різними дослідницькими інститутами, аналітичними центрами, неурядовими організаціями, міжнародними організаціями та фірмами приватного сектору. Результати, по суті, з використанням індексу сприйняття корупції Transparency International, який сильно корелює (0,99) з контрольним індексом корупції від WGI. Хоча ці показники корупції переважно ґрунтуються на сприйнятті, навряд чи на них вплинуло використання криптовалюти, оскільки рейтинг корупції в країнах був досить стабільним протягом багатьох років, а впровадження криптовалюти є недавнім явищем [346; 347].

Історія високої інфляції (середній рівень інфляції споживчих цін за 2011–2020 рр. з огляду МВФ щодо світової економіки) може зробити національну валюту менш привабливою як засіб збереження вартості. Минула інфляція використовується як проксі для стабільності валюти, що може вплинути на

привабливість криптоактивів як альтернативного засобу збереження вартості. Для зменшення ваги впливових спостережень застосовано таке логарифмічне перетворення: логарифм (1 + рівень інфляції) [348].

Дослідники стверджують, що криптоактиви можуть використовуватися для обходу контролю над капіталом. Наприклад, Graf von Luckner et al. (2021) дійшли висновку, що «уявлення про те, що використання криптовалют змінює економіку ухилення від контролю над капіталом і що, у свою чергу, ухилення від контролю над капіталом є важливою рушійною силою для розширення криптовалютних ринків», що загалом відповідає суті дослідження, яке вони представляють [348]. Ми використовуємо загальний індекс відкритості рахунку капіталу (також відомий як індекс Чінна-Іто), отриманий за допомогою методології, розробленої Чінном та Іто (2008) [356]. Він поєднує кілька двійкових змінних, що кодифікують таблицю обмежень на транскордонні фінансові операції, про які повідомляється в щорічному звіті МВФ про валютні домовленості та валютні обмеження (AREAER) [357]. У нашій вибірці по різних країнах індекс коливається від -1,9 до 2,3, вищі значення означають більшу фінансову відкритість. Ми використовуємо останнє доступне значення цього індексу за 2019 р., показник реального ВВП на одну особу в ПКС як загальний показник економічного розвитку, показники середні грошових переказів за 2017–2019 рр. та отриманих особистих грошових переказів у відсотках до ВВП.

Показник кількості відділень комерційних банків на 100 000 дорослих осіб, згідно з дослідженням фінансового доступу МВФ, використовується як проксі для внутрішнього фінансового розвитку та фінансової доступності. Жителі країн, де традиційний фінансовий сектор добре розвинутий, можуть рідше відчувати потребу в криптоактивах.

Показник кількості захищених інтернет-серверів, виміряних на 1 млн людей згідно з оцінками чисельності населення Світового банку, використовується як контроль проникнення інтернету та цифровізації економіки. Ми очікуємо, що ця змінна позитивно корелює з використанням криптоактивів,

оскільки для криптотрансакцій потрібне цифрове підключення. Описову статистику всіх змінних наведено в табл. 3.3.

Таблиця 3.3

Описова статистика за даними Глобального показника сприйняття криптоактивів Chainanalysis Crypto Adoption

Змінні	Кошти	Середнє	Станд. розробник	Мін.	Макс.
Прийняття криптовалюти	0.093	0.084	0.045	0.036	0.277
Контроль корупції	0.579	0.566	1.031	-1.097	2.270
Інфляція	1.217	1.050	0.650	-0.124	3.317
Реальний ВВП на душу населення	10.196	10.386	0.775	8.475	11.445
Відкритість капіталу	1.239	2.322	1.386	-1.226	2.322
Відділення комерційних банків	2.462	2.603	0.906	-0.570	3.818
Середнє співвідношення грошових переказів до ВВП (2017-2019)	0.017	0.004	0.025	0.000	0.098
Захищені інтернет-сервери	8.870	9.576	2.348	3.784	12.532

Джерело: Складено автором

З огляду на високу кореляцію між пояснювальними змінними мультиколінеарність є методологічним викликом. Зокрема, існує відносно висока кореляція між контролем показників корупції та реальним ВВП на одну особу і контролем капіталу.

Звертаючись до багатофакторного регресійного аналізу, враховуючи сильну мультиколінеарність, для виключення потенційно надлишкових змінних використовувався підхід до тестування від загального до конкретного, який був вперше запропонований Гендрі (1995) [358] і детально пояснений у Гувера та Переса (2004) [359]. Аналіз фактора дисперсії інфляції (VIF) підтверджує, що присутня мультиколінеарність, і це передбачає необхідність з'ясувати, яка(і) змінна(и) серед мультиколінеарних має первинну кореляцію із залежною

змінною. VIF є мірою колінеарності між пояснювальними змінними в регресії. Значення VIF пояснювальної змінної є функцією R2 від регресії цієї змінної на інші пояснювальні змінні. Зазвичай вважається, що значення VIF вище 4 свідчить про наявність значної мультиколінеарності. Змінні в цій регресії мають середній VIF 3,74, при цьому ВВП і контроль над корупцією мають VIF вище 4.

У дослідженні проведено кілька багатофакторних регресій, починаючи з усіх потенційних пояснювальних змінних, з подальшим поетапним виключенням найменш значущих. На кожному етапі застосовувався стандартний F-тест для виключення найменш значущих змінних, щоб підтвердити, що їх виключення не призводить до зміщення регресії. Також було проведено F-тести для підтвердження надмірності різних комбінацій змінних. Контроль над корупцією та контроль над капіталом залишаються значущими навіть після виключення найменш значущих змінних. F-статистика для спільного виключення трьох інших змінних (ВВП, інфляція та кредит приватного сектору) становить 0,22, що відповідає p-значенню 0,88. На останньому етапі ці змінні не розрізняються за рівнем значущості, і жодна з них не виявилася зайвою. Таким чином, було побудовано остаточну регресію OLS (з надійними стандартними помилками):

$$\boldsymbol{y_i = \alpha + \beta_1 c_i + \beta_2 k_i + \varepsilon} \quad (3.1)$$

де y – впровадження криптовалюти; c – контроль над корупцією; k – відкритість капіталу; α – константа; β – коефіцієнт інтересу.

У цій останній регресії p-значення для коефіцієнтів контролю корупції та відкритості капітального рахунку становлять 0,053 та 0,05 відповідно. Країни зі слабшим контролем над корупцією (більше корупції) і нижчим ступенем відкритості капіталу (більше контролю над капіталом), як правило, мають більшу частку впровадження криптовалют, що свідчить про можливість використання криптовалютних активів для переказу доходів від корупції або обходу контролю над капіталом. Перехід від 25-го процентиля до 75-го процентиля в контролі над корупцією та відкритістю капіталу (за інших рівних умов) пов’язаний зі

зниженням впровадження криптовалют приблизно на 2 і 4 відсоткові пункти відповідно.

Використання альтернативних змінних (індекс сприйняття корупції від Transparency International та індекс заходів контролю капіталу від Fernandez et al.) [368; 360] не вплинуло на отримані висновки. Вони залишаються стійкими до альтернативних способів вимірювання пояснювальних змінних. Видалення потенційно впливових спостережень із регресійного аналізу, зокрема значних аномальних значень у використанні криптовалюти та середньої інфляції, також не вплинуло на результати. Регресійні оцінки залишаються статистично значущими навіть за умови використання альтернативного визначення рівня впровадження криптовалюти. Водночас, це визначення має суттєві обмеження, що знижують його надійність, головним з яких є складність точного визначення рівня впровадження криптовалюти для окремих країн.

Характеристики криптовалют означають, що вони потенційно можуть використовуватися для сприяння корупції, а саме для переказу доходів від неї. На думку автора, кореляція між високим рівнем корупції та широким використанням криптовалюти потенційно також може пояснюватися тим фактом, що країни з високим рівнем корупції, як правило, мають слабкі політичні й фінансові інститути, що може знизити довіру в офіційній банківській системі.

Більшість наукових досліджень, що розглядають зв'язок між криптовалютами та корупцією, фокусуються лише на питанні, чи можуть криптовалюти сприяти корупції або, навпаки, знижувати її. Автори, які вважають, що криптовалюти можуть слугувати засобом для корупційних операцій, зазвичай підкреслюють анонімність користувачів криптовалюти.

Проте кілька авторів (наприклад, Альдаз-Карролл, 2018) [361] дотримуються протилежної точки зору, стверджуючи, що криптовалюти можуть зменшити корупцію. Вони вважають, що якщо криптовалюта містить інформацію про всі минулі трансакції, можна ідентифікувати, принаймні приблизно, різні сторони трансакцій з використанням сучасних методів (Big

Data) або, за необхідності, створити криптовалюту, в якій інформація про сторони договору включена до трансакції. Важливо підкреслити, що не всі автори поділяють цей оптимізм. Простіше кажучи, якщо ті, хто при владі, все ще прагнуть здійснювати шахрайство, особливо те, що включає змову, блокчейн не буде стримуючим фактором. Дадлі, Понд і Карден (2019), [362] таким чином, пропонують, на нашу думку, реалістичний погляд, наголошуючи на тому, що криптовалюти можуть як зменшувати корупцію, так і сприяти їй.

Деякі дослідники, такі як Ібрагімі, Адріаніт і Беса Аріф, стверджують, що криптоактиви можуть сприяти корупційним трансакціям, здійсненим в інтернеті, зменшуючи деякі обмеження корупційної поведінки, такі як трансакційні витрати та ризик бути спійманим [363]. Наприклад, учасники корупційної угоди можуть потенційно зменшити ймовірність бути виявленими органами влади, якщо використовують анонімний веббраузер Tor і приховують сліди за допомогою вебдодатків, призначених для приховування походження та призначення трансакцій.

Криптовалюти значно спрощують процеси, пов'язані з корупцією, знижуючи ризики, які супроводжують традиційні методи передачі хабарів. Використання готівки пов'язане з можливими втратами або використанням підроблених купюр, а банківські перекази можуть бути легко відстежені, що підвищує ризик викриття. Інші форми хабарів часто вимагають особистої зустрічі між сторонами, що також несе певні ризики. Завдяки псевдонімності криптовалют та складності їх відстеження корумповані особи можуть анонімно передавати хабарі, зменшуючи ймовірність виявлення їхньої незаконної діяльності. Це робить криптовалюти привабливими для тих, хто прагне уникнути виявлення своїх корупційних дій.

Історично передача хабарів вимагала особистої взаємодії між злочинцем і одержувачем або їхніми посередниками. Завдяки розвитку цифрових технологій, зокрема криптовалют, корупційні трансакції стали менш помітними для правоохоронних органів, що ускладнює боротьбу з такими злочинами.

Такі фактори можуть призвести до розширення корупційної практики, оскільки криптовалюти та онлайн-середовище знижують трансакційні витрати, спрощуючи контакт між сторонами корупційних угод. Це підвищує ефективність та анонімність корупційних операцій, що ускладнює їх виявлення та попередження [363].

Визнаючи зростаюче значення криптовалют і необхідність забезпечення відповідності нормативної бази поставленим цілям, міжнародні організації відіграють істотну роль у встановленні та просуванні стандартів для країн, щоб розробити законодавчу і нормативну базу, пов'язану з криптовалютами.

Як висновок можна зазначити: міжкраїновий регресійний аналіз із застосуванням підходу від загального до конкретного показує, що більше використання криптовалют емпірично пов'язане з вищою сприйнятою корупцією та інтенсивнішим контролем капіталу. Загалом наше тлумачення в поєднанні з принципом обачності, враховуючи швидке зростання макроекономічної значущості криптоактивів, полягає в тому, що ці докази додають до аргументів для регулювання використання криптовалюти, наприклад, вимагаючи від посередників упровадження процедур ЗСК. Аналіз також показує потребу в кращих даних для розуміння динаміки та ключових факторів, що спонукають до впровадження криптовалюти. Тим часом слід продовжувати роботу з використання технологій, покладених в основу криптоактивів, щоб реалізувати потенційні переваги для фінансової доступності та ефективності урядів.

Блокчейн може бути корисним для запобігання корупції, але лише за наявності певних передумов. Легалізація ринку віртуальних активів, цифрова грамотність і надійні інституції є важливими складовими для успіху технологій блокчейн.

Легалізація ринку криптоактивів може відігравати важливу роль у зниженні ризиків, пов'язаних зі злочинним використанням криптовалюти. Відповідні дії включають координацію розроблення та впровадження

нормативної та законодавчої бази, інформування громадськості про ризики використання криптовалюти і зміцнення потенціалу правоохоронних органів для ліквідації злочинних мереж.

Лідери Європейського Союзу в Брюсселі 23 червня 2022 р. затвердили рекомендації Європейської комісії про надання Україні статусу кандидата на вступ до Європейського Союзу [364]. Однак слід зазначити, що Європейська комісія, ухвалюючи свій висновок 17 червня 2022 р., напередодні прийняття резолюції висунула кілька умов для України з метою збереження статусу кандидата і подальшого просування до статусу повноправного члена Європейського Союзу. Розглянемо дві з семи вимог, які стосуються нашого дослідження:

- далі посилювати боротьбу з корупцією, зокрема на високому рівні, через проактивні та ефективні розслідування і наявність достовірних результатів кримінальних переслідувань та засуджень;
- забезпечити відповідність законодавства з ПВК/ФТ стандартам FATF і ухвалити загальний стратегічний план реформування всього сектору правоохоронних органів у межах безпекового середовища України.

Слід підкреслити, що Верховна Рада України значно раніше ратифікувала міжнародні стандарти боротьби з відмиванням грошей, фінансуванням тероризму та поширенням зброї масового знищення, рекомендовані FATF [365]. Проте, згідно з рекомендаціями Європейської комісії, їхня реалізація була недостатньо якісною. Ці дві вимоги Європейської комісії до України можна підсумувати як боротьбу з корупцією та відмиванням коштів [366].

Корупція є підступною загрозою з широким спектром руйнівних наслідків для суспільства. Вона підриває демократію та верховенство права, призводить до порушень прав людини, спотворює ринки, погіршує якість життя та сприяє процвітанню організованої злочинності, тероризму та інших загроз безпеці людини. Всі країни, великі та малі, багаті та бідні, стикаються з цим злом, але його наслідки найбільш руйнівні саме в країнах, що розвиваються. Корупція

вражає бідних непропорційно, відволікаючи кошти, призначені для розвитку, підриваючи здатність уряду надавати базові послуги, посилюючи нерівність і несправедливість, а також знижуючи рівень зовнішньої допомоги та інвестицій. Корупція є ключовим елементом економічної неефективності й основною перешкодою для подолання бідності та розвитку.

В Україні було прийнято Антикорупційну стратегію на 2021–2025 роки, яка показує, що, за результатами соціологічних досліджень, частка громадян, які мали безпосередній досвід корупції, значно зменшилася (у 2013 р. близько 60 % мали такий досвід, станом на початок 2020 року – лише 40 % громадян). Спостерігається поступове покращання порівняльних показників рівня корупції в Україні. Згідно з даними міжнародної організації «Transparency International», у період з 2013 до 2019 р. Індекс сприйняття корупції (ІСК) в Україні зріс із 25 до 30 балів. Це підтверджує, що досягнутий прогрес не задовольняє суспільство, оскільки є надто повільним. Європейська комісія у своєму висновку щодо заявок на членство в Європейському Союзі, поданих Україною, Грузією та Республікою Молдова 17 червня 2022 р., зазначила, що Україна досягла істотного прогресу на шляху до верховенства права, але все ще має пройти довгий шлях у боротьбі з корупцією [367: 368].

Крім того, зазначається, що, на додаток до згаданого покращення показника ІСК за 2013–2019 рр., наведеного в Антикорупційній стратегії на 2021–2025 роки, Індекс сприйняття корупції за 2021 р. погіршився, опустивши Україну зі 117-го на 122-ге місце зі 180 країн. Протягом 2022–2023 р. динаміка ІСК почала покращуватись, проте 2024 р. ознаменувався гучними подіями, пов’язаними з оголошеною в Україні мобілізацією у зв’язку з повномасштабною агресією з боку рф. Це можна побачити в табл. 3.4.

Таблиця 3.4

Аналіз індексу ІСК для України у 2012-2021 роках

за рейтингом 188 країн

№	Рік	Місце України в рейтингу країн за індексом ІСК	Індекс України (ІСК)
1	2012	144	26
2	2013	144	25
3	2014	142	26
4	2015	130	27
5	2016	131	29
6	2017	130	30
7	2018	120	32
8	2019	126	30
9	2020	117	33
10	2021	122	32
11	2022	116	33
12	2023	104	36

Джерело: складено автором за матеріалами [368]

Низький рівень реалізації антикорупційної політики в Україні значно уповільнює її економічне зростання. Опитування бізнесу показує, що поширеність корупції та недовіра до судової системи є основними перешкодами для залучення іноземних інвестицій. Зосередження зусиль на реалізації антикорупційної політики дасть змогу Україні найближчими роками наздогнати показники ІСК країн Східної Європи – членів Європейського Союзу та досягти середніх європейських значень ІСК протягом 10 років.

З цією метою Україна створила мережу спеціалізованих державних органів для протидії корупції. Слід одразу зазначити, що вона є досить розгалуженою та

включає сім спеціалізованих державних установ: Національну раду з питань антикорупційної політики, Національне антикорупційне бюро України, Національне агентство з питань запобігання корупції, Спеціалізовану антикорупційну прокуратуру, Державне бюро розслідувань, Вищий антикорупційний суд, Національне агентство України з питань виявлення, розшуку та управління активами, отриманими від корупційних та інших злочинів. Варто зазначити, що перелічено лише спеціалізовані установи, без урахування загальної правоохоронної системи України, яка має такі основні відомства: Офіс Генерального прокурора, Національну поліцію, Бюро економічної безпеки, Верховний Суд та ін.

За словами Президента України, останніми роками Україна створила антикорупційну структуру, яка не має аналогів у Європі [369]. Однак така значна кількість спеціалізованих державних установ для боротьби з корупцією в Україні, м'яко кажучи, дивує на тлі досить невисоких результатів їхньої роботи, що випливає з наведеного вище аналізу показників ІСК у табл. 2.13.

Одним із антикорупційних інструментів, запроваджених ще у 2014 р., стало зобов’язання державних службовців подавати електронні декларації про майно, доходи та фінансові зобов’язання (декларація), які належать державному службовцю. Це зобов’язання набрало чинності після створення НАЗК та Єдиного державного реєстру декларацій у серпні 2016 р. [370].

Закон України «Про запобігання корупції» [40] та Порядок заповнення і подання декларації особою, яка виконує функції держави або місцевого самоврядування [371], передбачають три випадки подання декларації державними службовцями:

5) Щорічна декларація, що охоплює звітний рік (період з 1 січня по 31 грудня включно), який передує року подання декларації. Обов’язок подавати щорічну декларацію виникає в суб’єкта декларування:

- щороку під час виконання діяльності, що передбачає обов’язок подавати декларацію, або обіймання посади, яка вимагає такої діяльності (щорічна декларація у зв’язку з продовженням діяльності);
- наступного року після припинення діяльності, що передбачає обов’язок подавати декларацію, або обіймання посади, яка вимагає такої діяльності (щорічна декларація після звільнення);

6) Декларація при звільненні, що подається за період, який не охоплений раніше поданими деклараціями суб’єкта декларування, і містить інформацію станом на останній день такого періоду, який є останнім днем діяльності, що передбачає обов’язок подавати декларацію, або обіймання посади, яка вимагає такої діяльності

7) Декларація кандидата на посаду, що подається після визначення особи переможцем конкурсу, але до дня призначення або обрання особи на посаду.

Державні службовці можуть нести дисциплінарну, адміністративну та кримінальну відповідальність за неподання або подання неправдивої інформації в декларації. Інформація про осіб, притягнутих до відповідальності за корупційні або пов’язані з корупцією правопорушення, вноситься до Єдиного державного реєстру осіб, які вчинили корупційні або пов'язані з корупцією правопорушення (Реєстр корупціонерів) [372]. Цей портал містить дані про всіх осіб і юридичні особи, які вчинили корупційні правопорушення; адмініструванням цього реєстру з лютого 2019 р. займається НАЗК. На декларантів покладається дисциплінарна, адміністративна та кримінальна відповідальність.

До останнього часу Кримінальний кодекс України містив статті 366-1 «Декларування недостовірної інформації» та 368-2 «Незаконне збагачення», які принаймні становили серйозну загрозу для корупціонерів. Стаття 368-2 передбачала склад злочину за набуття у власність активів у значному розмірі особою, що має право виконувати функції держави або місцевого

самоврядування, законність підстав набуття яких не підтверджена доказами, а також за передачу таких активів іншій особі.

З початку впровадження державної політики, спрямованої на легалізацію криптовалют в Україні, що стала здійснюватися у 2016 р., з поданням до Верховної Ради України перших проєктів законів у цій сфері, ситуація з декларуванням криптовалют посадовими особами, які нібито перебувають у їх володінні, також змінилася. Таблиця 3.5 показує динаміку щодо декларування Bitcoin (BTC) посадовими особами з 2016 по 2023 р. У декларуванні ВА особливо важливою є декларація, в якій вони вперше зазначені (нульова декларація), оскільки наступні декларації будуть спиратись на попередні дані в динаміці. Нижче наведемо статистичні дані з Єдиного державного реєстру декларацій.

Таблиця 3.5.

Динаміка декларування володіння BTC посадовими особами в 2016–2023 роках

	Дата	Кількість осіб, які володіють BTC (осіб)	Збільшення до попереднього року (%)	Збільшення до 2016 року (%)
1	01.01.2016	25	0	0
2	01.01.2017	58	132	132
3	01.01.2018	71	22	184
4	01.01.2019	424	497	1596
5	01.01.2020	652	54	2508
6	01.01.2021	356	- 46	1424
7	01.01.2022	648	82	2592
8	01.01.2023	782	21	3128

Джерело: Складено автором

З початку повномасштабного вторгнення рф в Україну Національне агентство з питань запобігання корупції (НАЗК) закрило доступ до публічної частини Реєстру декларацій. Агентство також заявило, що під час дії воєнного

стану суб'єкти декларування не зобов'язані витрачати час на заповнення або подання декларацій чи повідомлень про суттєві зміни в майновому стані [373].

Однак у жовтні 2023 р. набув чинності закон про відновлення електронного декларування [374], а в грудні НАЗК відновило публічний доступ до Реєстру [375].

Відповідно до закону, посадовці повинні подати декларації за 2021–2022 рр. до 31 січня, а за 2023 р. — до 31 березня 2024 р. Декларувати своє майно, зокрема криптовалюту, зобов'язані всі особи, які виконують функції держави або місцевого самоврядування. Крім того, у деклараціях вони також мають вказувати активи, що належать членам їхніх сімей.

У проаналізованих документах криптовалюти згадуються в 1834 деклараціях, у яких зазначено загалом 10 163 різні токени. Серед найпоширеніших активів, вказаних у цих деклараціях, — Bitcoin, Ethereum, Tether, Polkadot, BNB, Cardano, Ripple, Solana, а також мемкоїн Shiba Inu та Dogecoin. Частку задекларованих віртуальних активів у загальному обсязі зображено на рис. 3.3.



Рис.3.3. ТОП-10 криптоактивів у деклараціях державних посадовців України за 2023 рік.

Джерело: Incrypted [376].

З публікації інтернет-видання Incrypted випливає, що розмаїття криптоактивів стає більшим [376]. Починаючи з 2020 р., у деклараціях з'являється дедалі більше криптовалют, інших, ніж біткоїн, блокчейн-платформ, монет та NFT.

Декларанти вказали загалом близько 834 BTC, що на момент підрахунку оцінювалися у понад 55,7 млн дол. США (близько 2,1 млрд грн), приблизно 3964 ETH (майже 13 млн дол. США, або 505 млн грн) і USDT на суму понад 4,1 млн дол. США (майже 160 млн грн) (табл. 3.6).

Таблиця 3.6.

Найбільші обсяги задекларованих криптоактивів у 2023 році

	Державний орган	**Посада**	**Кількість ВА**	**Еквівалент вартості ВА станом на 05.04. 2024р. (млн. дол. США)**
1	Одеська обласна рада	Депутат	121 BTC	8,1
2	Хмельницька районна рада	Депутат	100 BTC	6,69
3	Подільська районна рада Одеської області	Депутат	1800 ETH	5,87
4	Комітет з питань екологічної політики та природокористування	Голова	80 BTC	5,41
5	МВС	Заступник начальника регіонального сервісного центру	80 BTC	5,41
6	Хмельницька районна рада	Депутат	1000 ETH	3,26
7	ВРУ	Депутат	42 BTC	2,81
8	Управління міграційного контролю в Одеській області	Начальник	37 BTC	2,47
9	Дніпровська міська рада	Начальник Департаменту благоустрою та інфраструктури	20 BTC	1,33
10	НПУ в Миколаївській області	Заступник начальника Головного управління	15 BTC	1,0
	Загалом:		**485 BTC 2800 ETH**	**42,35**

Джерело: складено автором

До таблиці не внесено даних за активами в USDT. Це можна пояснити тим, що стейблкоїни мають забезпечення у фіатній валюті та низьку волатильність, тому не можуть бути аргументом придбання їх у ранні періоди обігу і значного зростання курсу, як BTC та ETH. Мемкоїни (токени в DeFi), зокрема Dogecoin і Shiba Inu, також популярні серед декларантів.

Варто зазначити, що під час підрахунку загальної кількості SHIB не враховано 204 357 574 000 000 токенів, зазначених у декларації співробітника Головного управління Держпродспоживслужби в Одеській області Олексія Клімова [377]. Імовірно, під час заповнення декларації декларант припустився помилки у зазначенні кількості активів Shiba Inu, оскільки ця сума становила б майже половину всіх токенів SHIB в обігу.

У деклараціях за 2023 р. криптовалюти згадувалися у багатьох випадках, зокрема біткоїн задекларували 792 особи. Найбільшим власником першої криптовалюти став депутат Одеської облради Микита Кузькевич [378], який зазначив 121 BTC (понад 8,2 млн дол. США на момент підрахунку). Із них 88 BTC належать самому декларанту, а 33 BTC — його дружині. Подружжя володіє криптовалютою з 2012 р.

Серед топ-10 найбільших власників біткоїнів також є ранні інвестори, зокрема: голова Комітету з питань екологічної політики та природокористування апарату Верховної Ради Олег Бондаренко [379], голова Державної регуляторної служби Олексій Кучер [380] і заступник начальника ГУНП у Миколаївській області Едуард Соловйов [381]. Всі вони задекларували біткоїни, отримані ще у 2013 р.

Другим за розміром біткоїн-активів є депутат Хмельницької районної ради Олександр Кізляр [382], який володіє 100 BTC (понад 6,7 млн дол. США). Він також увійшов до топ-10 за кількістю Ethereum і додатково придбав 6,5 млрд PEPE та 1500 SOL у 2023 р.

Ще один декларант, народний депутат Дмитро Гурін [383], зазначив у декларації, що його дружина володіла 42 BTC (2,8 млн дол. США) на гаманці

Opendime, однак ці активи були викрадені.

Стейблкоїн USDT став другим за популярністю криптоактивом у деклараціях. Найбільшим власником є директор департаменту Державної виконавчої служби Мін'юсту Максим Кисельов [384], який задекларував понад 647 000 USDT та отримав близько 2,6 млн грн від продажу криптовалюти.

На другому місці за кількістю USDT — начальник департаменту Офісу Генпрокурора Віталій Бровко [385]. У декларації зазначено, що його дружина володіє понад 619 000 USDT і заробила близько 8,3 млн грн від продажу криптовалют у 2023 р.

Ethereum було задекларовано в 606 випадках. Найбільшим власником є депутат Подільської райради Одеської області Ігор Осіпов [386], який вказав 1800 ETH (понад 6 млн дол. США), проте заявив про втрату доступу до цих активів. Друге місце посів Олександр Кізляр [382] із 1000 ETH (3,3 млн дол. США), а третє — спеціалістка Дніпровської міськради Крістіна Павлова [387], чоловік якої володіє 130 ETH.

Далі розглянемо агрегацію ВА за групами власників у табл. 3.7.

Таблиця 3.7

Агрегація ВА за групами їх власників (державних службовців) за результатами декларації за 2023 рік

	Група дослідження	**Загальна кількість ВА**	**Еквівалент суми в млн. дол. США**
1	Топ-десять найбільших власників BTC	585	39,24
2	Топ-десять найбільших власників ETH	1827	10,61
3	Топ-десять найбільших власників USDT	2,548,786	1,9
	Загалом:		51,75

Джерело: Складено автором

Найпоширенішою платформою, яку використовують українські посадовці

для роботи з криптовалютами, стала Binance. У більше ніж половині декларацій за 2023 р. саме ця біржа вказана як основний постачальник послуг. На другому та третьому місцях, із суттєвим відривом, розташувалися WhiteBIT і Bybit відповідно. Також у 2,5 % декларацій згадуються холодні гаманці (табл. 3.8).

Таблиця 3.8

Перелік популярних для посадових осіб криптоплатформ, на яких зберігалась на момент декларування криптоактиви в 2023 році

	Назва платформи	Кількість зазначення в деклараціях	Обсяг від загального обсягу (%)
1	Binance	7374	67,7
2	Інше	1673	15,1
3	WhiteBit	346	3,1
4	ByBit	315	2,9
5	Холодні гаманці	272	2,5
6	Trust Wallet	271	2,5
7	OKX	248	2,2
8	Kuna	198	1,8
9	MetaMask	135	1,2
10	Qmall	114	1

Джерело: Складено автором

Кількість декларацій, у яких українські чиновники зазначають криптоактиви, продовжує зростати. Україна стабільно займає провідні позиції серед країн із високим рівнем прийняття цифрових активів. Згідно з оцінками Chainalysis, як зазначалося, у 2023 р. українські інвестори заробили 850 млн дол. США на інвестиціях у криптоактиви [388]. З огляду на ці показники, тенденція до зростання кількості декларацій, пов’язаних із криптовалютами, є цілком імовірною в майбутньому.

Продовжимо аналізувати хронологію впровадження механізмів перевірки криптоактивів у деклараціях державних службовців як потенційного

інструменту для відмивання їхніх доходів. Справді, щодо особливостей декларування криптоактивів Закон України від 02.10.2019 № 140-XI [389] змінив п. 6 частини першої ст. 46 Закону України «Про запобігання корупції»: «Нематеріальні активи, що належать суб'єкту декларування або членам його сім'ї, включаючи об'єкти інтелектуальної власності, які можуть бути оцінені в грошовому виразі, криптовалюти. Інформація про нематеріальні активи включає дані про тип і характеристики таких активів, їх вартість на момент володіння, а також дату набуття права на них [389]».

Як бачимо, зменшено лише вимоги до декларацій щодо криптоактивів, щоб відображати:

- тип і характеристики;
- вартість;
- дату виникнення права на них.

Закони України не вимагають іншої інформації, такої як інші свідчення щодо місць зберігання таких активів, права власності на них, історії їхнього походження.

На нашу думку, НАЗК намагалася виправити таке становище своїм наказом № 449/21 та роз'ясненням № 11 від 12.09.2021 [390], тобто за два дні до початку нової кампанії з подання декларацій про доходи за 2021 р., яка тривала з 1 січня 2022 р. по 4 січня 2022 р. Розглянемо причини, чому це не вдалося.

По суті, це мало би бути відображено в ст. 46 Закону України «Про запобігання корупції», щоб не суперечити йому або не розширювати його самостійно (що є неконституційним). В іншому випадку ці положення не матимуть юридичної сили, оскільки відображаються лише в наказі № 449/21 та роз'ясненні № 11 і суперечать Закону України «Про запобігання корупції». Крім того, як можна зрозуміти, НАЗК не мала достатньо часу до початку нової кампанії з подання декларацій про доходи за 2021 р.

Законодавство України є системою нормативно-правових актів та міжнародних договорів, які сформовано на ієрархічній основі.

Нормативно-правовий акт — це офіційний документ, прийнятий (виданий) уповноваженим органом у формі та порядку, визначеному законом, який встановлює правові норми для невизначеного кола осіб і призначений для повторного використання.

Закон — це нормативно-правовий акт, прийнятий Верховною Радою України або всеукраїнським референдумом, який регулює найважливіші соціальні відносини шляхом встановлення статусу, загальнообов'язкових правил поведінки суб'єктів таких відносин та відповідальності за порушення цих правил. Закони України мають найвищу юридичну силу після Конституції України і приймаються на основі Конституції України та повинні їй відповідати.

Ця думка підтверджується преамбулою роз'яснення № 11: «Воно надається для забезпечення єдиного застосування закону щодо заходів фінансового контролю, розглядається як рекомендації і не містить нових правових норм» [390].

Важливо зрозуміти, що містить наказ № 449/21 і що визнано як відсутнє в ст. 46 Закону України «Про запобігання корупції» для того, щоб ці норми набули безсумнівної юридичної сили. Розділ IV «Правила заповнення розділів декларації» (п. 11) містить такі вимоги: «У розділі 10 «Нематеріальні активи»: 3) інформація про криптоактив включає дані про тип об'єкта; ідентифікатор у системі обігу віртуальних активів; кількість і вартість криптовалюти; дату придбання; постачальника послуг, пов'язаних з обігом криптовалюти; особу, до якої належить об'єкт (суб'єкт декларування та/або члени його родини). Інформація, що ідентифікує криптоактив та особу, до якої вона належить, а також кількість криптовалюти, дата придбання та її вартість, мають бути зазначені» [390].

Роз'яснення № 11 визнає недоліки ст. 46 Закону України «Про запобігання корупції» для того, щоб ці норми мали безсумнівну юридичну силу:

– кількість певного типу криптовалюти може змінюватися через її обмін (конверсію) на інші типи криптовалют. Щоб підтвердити зміну кількості,

яка сталася внаслідок низки торгів (обмінних) операцій, варто зберігати історію відповідних трансакцій;

– наявність «публічної адреси» криптовалюти дає змогу відстежувати попередні дати трансакцій і кількість криптовалюти, придбаної на ці дати. Крім того, суб'єкт декларації може підтвердити дату придбання криптовалюти через історію відповідних трансакцій;

– у полі «Ідентифікатор у системі обігу віртуальних активів (публічна адреса)» має бути зазначена публічна адреса криптовалюти, так званий публічний (публічний) ключ. Наявність публічної адреси характеризує будь-який криптоактив, що належить особі;

– у полі «Інформація про постачальника послуг, пов'язаних з обігом криптовалюти» має бути вказана назва криптовалютної біржі [390].

Відповідно до звіту Державної служби фінансового моніторингу України, спільно з командою Міністерства цифрової трансформації та провідними криптоекспертами України було створено список російських біткоїн-бірж, пов’язаних із банками під санкціями, з метою повного блокування їхнього хостингу [391].

Крім того, було запущено «механізм спонтанного блокування» російських гаманців у співпраці з постачальниками криптовалютних послуг. Державна служба фінансового моніторингу України повідомила, що звернулася до біржі Binance «з конкретними пропозиціями щодо дій для стримування російської агресії на ринку віртуальних активів». «[Після розгляду цього питання] Binance змінила свою політику, і 20.03.2022 виключила можливість P2P-операцій для ряду російських банків і платіжних систем, які були включені до списку санкцій. Крім того, було реалізовано інші практичні заходи для блокування російських криптоактивів та трансакцій російських резидентів», — ідеться у звіті [391].

Детально діяльність з обходу санкцій, накладених на всіх суб’єктів рф у зв’язку з російською воєнною агресією в Україні, ми розглянемо в наступному розділі.

Однак необхідно зазначити, що одним із превентивних заходів протидії корупції, крім зазначеної вище відкритої інформації про декларування державних посадовців, є навчання. Освітні заходи є вимогою базового закону щодо ПВК/ФТ та Рекомендацій FATF у розділі «Міжвідомча взаємодія».

Так, представники державних регуляторних, антикорупційних та правоохоронних органів, депутати в рамках заходів, що проводились у жовтні – грудні 2022 р. у Відні (Австрійська Республіка), організованих за підтримки ОБСЄ та UNODC, брали активну участь в обговоренні таксономії віртуальних активів, регуляторної діяльності ринку віртуальних активів, оцінки секторальних ризиків сектору віртуальних активів, поточних інструментів та технічних можливостей для розслідування віртуальних трансакцій і огляді міжнародного та національного законодавств у сфері ВА [392].

Також для представників національної антикорупційної системи, а саме для НАЗК у 2020 р. та 250 детективів та аналітиків НАБУ в 2023 р. за підтримки Посольства США в Україні та фінансової підтримки Бюро з міжнародних питань у сфері боротьби з незаконним обігом наркотиків та правоохоронних питань Державного департаменту США було проведено тренінги щодо криптовалютних технологій та методики розслідування злочинів із використанням ВА [393].

Необхідно зазначити, що після оновлення у 2019 р. базового Закону України про ПВК/ФТ з боку антикорупційної системи було ініційовано внесення ВА як виду активів до статей Кримінального та Кримінально-процесуального кодексів України, що стосуються корупційних злочинів.

Для подальшого розвитку національної системи боротьби з відмиванням грошей Державна служба фінансового моніторингу України за підтримки ОБСЄ та УНП ООН з іншими зацікавленими сторонами продовжила співпрацю в рамках проєкту «Інноваційні політичні рішення для зменшення ризиків відмивання грошей, пов'язаних з віртуальними активами» [394].

У 2022 р. Національне агентство України з розшуку та управління активами (АРМА) почало співпрацювати з кількома криптовалютними біржами,

а саме Binance, Coinbase, KuCoin, Kraken та WhiteBit, для обміну інформацією. Криптобіржі також зазначили, що агентство встановлює наявність цифрових активів у руках підозрюваних у рамках кримінальних проваджень [395]. У результаті такої співпраці АРМА змогло отримувати ідентифікаційні дані власників криптогаманців, зокрема: документ, що посвідчує особу; електронну адресу; VPN (IP-адресу); ім'я та IMEI пристрою, який використовувався для входу в акаунт криптовалютної біржі; інформацію про трансакції; наявність додаткових криптогаманців і банківських рахунків, через які поповнюються ці криптогаманці; номери банківських рахунків та рахунків платіжних систем, на які виводяться кошти.

Крім того, взаємодія з криптовалютними біржами дає можливість додатково встановити наявність цифрових і віртуальних активів осіб, залучених до кримінальних проваджень. Це сприяє ефективності взаємодії з правоохоронними органами для надання додаткової інформації з метою арешту виявлених криптовалютних активів.

АРМА спільно з експертами розробила рекомендації щодо ідентифікації, відстеження та арешту криптоактивів у кримінальних провадженнях. Ці настанови висвітлюють основні аспекти організації кримінальних проваджень, що включають операції з використанням криптогаманців, методи підготовки до процесуальних дій, способи виявлення програмного забезпечення, пов'язаного з використанням віртуальних валют у злочинних цілях, їхні ключові ідентифікатори, а також правові аспекти арешту ВА, що використовуються у кримінальній діяльності [396].

Настанови містять шість розділів, де наведено актуальну інформацію щодо методів виявлення програмного забезпечення, необхідного для використання віртуальних валют, а також пошуку збережених паролів, включно з їхніми найпоширенішими формами та місцями зберігання. Крім того, настанови надають зразки заяв на проведення обшуків та арешт майна, поданих правоохоронними органами до суду. Розроблені настанови дають змогу

впорядкувати алгоритм дій, тим самим збільшуючи ефективність заходів з ідентифікації, пошуку та арешту криптоактивів.

Також, дотримуючись проактивного підходу до формування державної політики та впровадження найкращих міжнародних практик у сфері розшуку активів, зокрема криптоактивів, АРМА звернулася до міжнародних організацій, що працюють у галузі розшуку та відновлення активів, з пропозицією ознайомитися з практикою України, поділитися своїми підходами та долучитися до розроблення досліджень у цій сфері.

АРМА ініціювало консультації з Інтерполом та Європолом, глобальними мережами відновлення активів (Camden Asset Recovery Inter-Agency Network (CARIN) та Stolen Asset Recovery Initiative (StAR), регіональними мережами повернення активів в Азійсько-Тихоокеанському регіоні, Південній та Східній Африці, Західній Африці та Карибському басейні, платформою з повернення активів країн – членів Європейського Союзу.

На сьогодні платформа для обговорення ініціатив АРМА об'єднує понад 150 юрисдикцій. В АРМА вважають, що це сприятиме обміну досвідом між спеціалізованими установами та вирішенню низки проблемних питань, з якими стикаються уповноважені органи в галузі розшуку, блокування та подальшого арешту криптовалют. Крім того, АРМА сподівається на встановлення діалогу з іноземними партнерами для подальших можливих спільних дій у цій сфері [396].

Віртуальні активи в Україні до 15 березня 2022 р. не мали визначеного правового статусу та юридично встановленого механізму підтвердження їхнього володіння. Багато державних службовців скористалися цією ситуацією, декларуючи їх як власність за відсутності правового поля, що спричинило підозри в суспільстві щодо відмивання грошей. Це пов’язано з тим, що декларування криптовалюти не виключає можливості фіктивності таких дій, спрямованих на відмивання доходів, отриманих від корупції, а саме: статки більшості декларантів – державних службовців, з огляду на рівень їхньої зарплати, не давали їм змоги придбати заявлені криптоактиви на мільйони

доларів США.

Конституційний Суд України 27 жовтня 2020 р. ухвалив рішення № 13-р/2020, яким скасував низку антикорупційних інструментів [397]. Зокрема, було скасовано ст. 366-1 Кримінального кодексу, що передбачала кримінальну відповідальність за недекларування або подання завідомо неправдивої інформації суб'єктом декларування. Це рішення спричинило закриття кримінальних проваджень у справах, пов'язаних із декларуванням недостовірної інформації про майно або повним невнесенням декларації, які перебували у процесі розгляду. В результаті відповідальність за такі порушення було зведено лише до адміністративних санкцій. Згодом парламент України запровадив нові подібні норми, проте втрата часу призвела до негативних наслідків.

Насправді, це фактично була амністія для державних службовців, які раніше подали інформацію до своїх декларацій, навіть якщо вона була ненадійною.

Інформація про наявність криптоактивів у власності державних службовців не стала винятком із такої інформації. Ці задекларовані статки, ймовірно, були отримані від корупції, враховуючи дисбаланс між низьким рівнем заробітної плати чиновників і рівнем задекларованих статків у криптоактивах.

Навіть після повторного введення 30 грудня 2020 р. двох кримінальних статей (366-2 та 366-3), що передбачають склад злочину, подібний скасованій статті 366-1, стало неможливо притягти державних службовців до відповідальності за раніше вчинені злочини у сфері корупції. Адже відповідно до ст. 58 Конституції України прийняті закони та нормативно-правові акти не мають зворотної сили в часі, у нашому випадку до 30 грудня 2020 р. (дати прийняття нових санкцій).

На 30 грудня 2020 р. відновлення кримінальної відповідальності за неналежне подання декларацій державними службовцями через введення статей 366-2 та 366-3 до Кримінального кодексу України спочатку не мало санкції у

вигляді позбавлення волі, лише у вигляді обмеження волі. Після повторних змін до цих статей, які набрали чинності 21 липня 2021 р., з'явилася максимальна санкція у вигляді ув'язнення: у ст. 366-2 – до двох років, у ст. 366-3 – до одного року.

Набагато жорсткіші норми було введено після завершення кампанії декларування 2020 р., що дало змогу державним службовцям задекларувати за 2020 р. 46 351 біткоїн, що на 1 квітня 2020 року становило майже 2 млрд 564 млн дол. США або 2 млрд 348 млн євро.

Це сталося на фоні майже повної відсутності ефективних санкцій у законодавстві, оскільки максимальною мірою, яка могла загрожувати корупційним чиновникам (можна припустити, що такі існують, зважаючи на дисбаланс у рівні їхньої заробітної плати та заявленому багатстві), був штраф. Навіть обмеження волі не могло бути застосоване до них, оскільки для тих, хто притягується до відповідальності вперше, найсуворіше з доступних покарань застосовується вкрай рідко.

Як зазначалося, ст. 46 основного антикорупційного Закону України «Про запобігання корупції» [40] містить недостатньо жорсткі вимоги до декларування криптоактивів державними службовцями. Закон вимагає лише відображення типу криптоактивів, їх характеристик, вартості та дати набуття права на них. Інша інформація, зокрема докази місць зберігання криптоактивів, права на їх володіння та історія їх походження, не передбачена. Це обмежує можливості правоохоронних органів у розслідуванні корупційних схем, пов'язаних із придбанням криптоактивів.

Спроба усунути цей недолік була зроблена наказом № 449/21 та Поясненням № 11, виданими НАЗК, які регламентують порядок заповнення декларацій державними службовцями. Хоча ці нормативні документи, за твердженням НАЗК, уточнюють і розкривають поняття «типів і характеристик» криптоактивів, що згадані у Законі «Про запобігання корупції», НАЗК у цьому випадку вийшов за межі своїх повноважень. Таким чином, їхні положення

фактично перевищують повноваження, надані статтею 46 Закону, і можуть бути оскаржені як нелегітимні як в українських, так і в міжнародних судах.

Водночас, важливо підкреслити, що такі вимоги до декларування повинні бути закріплені безпосередньо у Законі «Про запобігання корупції», а не міститися в підзаконних актах, щоб мати непохитну юридичну силу.

Іншим країнам, на нашу думку, доцільно врахувати досвід України, який продемонстрував новий шлях можливого відмивання грошей через декларування криптовалют до їх легалізації, що вимагає розроблення та прийняття превентивних норм у чинному законодавстві щодо легалізації криптоактивів.

Недостатньо ефективна та неповна законодавча політика держави у сфері ПВК/ФТ через криптовалюти може фактично призвести до так званої мовчазної амністії раніше задекларованих криптоактивів, отриманих унаслідок корупції та інших незаконних дій.

Перспективним напрямом подальшого дослідження цього явища є моніторинг криптоактивів із використанням блокчейн-аналітичних програм, зокрема в контексті декларування державними посадовцями активів, що можуть бути пов’язані з ВК.

Виявлення та протидія легалізації кримінальних доходів повинні продовжуватися в таких напрямах:

1) покращання механізмів запобігання та боротьби;

2) розроблення (експериментування) нових механізмів, що повинні відповідати викликам фінансово-технологічної галузі, які постійно зростають, та кримінальним схемам їх використання.

Досвід українських державних установ у боротьбі з відмиванням коштів через криптовалюти, зокрема співпраця АРМА з Binance, Coinbase, KuCoin, Kraken і WhiteBit, практичні та теоретичні напрацювання НАЗК щодо перевірки криптоактивів у деклараціях, а також превентивні заходи Державної служби

фінансового моніторингу України та НАЗК можуть бути впроваджені на глобальному рівні для запобігання ВК.

3.4. Методологічні засади запобігання порушенням, пов'язаним із використанням криптоактивів у процесі застосування санкцій

Розвиток новітніх технологій привертає дедалі більшу увагу міжнародних організацій та є одним із найважливіших напрямів дослідження, регулювання та розбудови системи впливу для забезпечення фінансової стабільності.

Також новітні технології забезпечили активну громадянську позицію людей із різних країн світу. З початком повномасштабного російського вторгнення в Україну оперативну та дієву допомогу країні було організовано через збір коштів благодійними криптофондами. Водночас така активність, пов'язана з підтримкою українського народу, активізувала злочинний світ, трансакції в якому видавалися за благодійну діяльність. Тому потрібне підвищення стандартів та оперативності у сфері оцінки й управління ризиками та комплаєнсу.

Запровадження міжнародних санкцій як інструменту протидії неспровокованій російській збройній агресії в Україні вплинуло на пріоритети антилегалізаційної діяльності на глобальному рівні. Останнім часом використання новітніх технологій привернуло увагу FATF та інших міжнародних організацій. Міжнародні санкції мають на меті зменшити витрати країна-агресорів, спрямованих на мілітаризацію власних військових сил, що має зупинити їхню агресію.

Пакети санкцій застосовуються до різних галузей економік і за результатами впровадження країнами виробляються наступні пакети санкцій. Так, за результатами впровадження санкцій до визначених російських

банківських установ встановлено їх обхід з використанням інструментів і операторів крипторинку, які взаємодіють із санкційними російськими банками, компаніями та фізичними особами.

Для зупинення неспровокованої агресії російської федерації проти України багато країн світу, такі як Велика Британія, Сполучені Штати Америки, країни Європейського Союзу розробляють та впроваджують економічні санкції. Зокрема, Рада ЄС запровадила вже п'ятнадцятий пакет економічних і персональних санкцій проти росії за її "агресивну війну" проти України. Узгоджений пакет включає низку заходів, спрямованих на посилення тиску на російський уряд та економіку, а також на обмеження ресурсів кремля для агресії.

На жаль, санкційні російські та білоруські юридичні та фізичні особи обходять введені обмеження різними засобами, включно з фінансовими технологіями, криптоактивами та юридичними інструментами. Використання традиційних фінансових послуг, фінансових технологій та альтернативних платіжних послуг є ефективнішим способом обходу санкцій з точки зору обсягів і витрат, ніж застосування криптоактивів. Але, як зазначив прем'єр-міністр росії в доповіді уряду у 2022 р., росіяни мають 130 млрд дол. США у криптовалютах, що еквівалентно половині ВВП Фінляндії у 2020 р. І це ще на 84 млрд дол. менше, ніж в оцінці, оприлюдненій кремлем на початку лютого 2022 р. [398].

Як відомо, криптоактиви не забезпечують достатньої ліквідності, щоб дати змогу російській федерації повністю обійти санкції SWIFT за їхнє використання. Проте, оскільки дослідники блокчейн-мереж розглядають сплески трансакцій у різних юрисдикціях, докази обходу санкцій збираються та передаються державним регуляторним і правоохоронним органам для вжиття додаткових заходів.

Обмежений обсяг ліквідності в просторі DeFi, зростаюча кількість дослідників блокчейнів, низка законодавчих актів з останніх директив ЄС із ПВК/ФТ та імплементація правила подорожей FATF роблять уникнення надто дорогим або неможливим. Однак особи можуть спробувати обійти ці санкції,

адаптувавши стратегії ухилення від санкцій, які традиційно використовуються для банківських санкцій. Використання підставних компаній, довіреностей, довірених осіб – лише окремі з таких прийомів.

У сфері криптоактивів необхідно використовувати всі технологічні та правові інструменти для цілеспрямованого застосування санкцій. Галузь, регулятори та законодавці пройшли довгий шлях з моменту створення перших інструментів візуалізації, щоб виявляти, групувати й дозволяти правоохоронним органам конфіскувати невиконані трансакції. Посилене відстеження трансакцій у блокчейні допомагає відкрити новий простір для розслідування можливої тактики ухилення росії від санкцій з використанням криптовалют.

Скотт Джонстон, старший розробник рішень Chainalysis і колишній працівник правоохоронного органу США зазначає: «Підвищена прозорість блокчейну надає недооцінені можливості для державного та приватного секторів для виявлення й запобігання незаконній діяльності, включно з ухиленням від санкцій, і співпраці через кордони» [405].

Тому санкції можуть діяти лише в тому випадку, якщо ті, хто повинен їх упроваджувати, розуміють, що робити, аби їх не можна було легко обійти. Розгалужена російська мережа нерегульованих (OTC) провайдерів потребує ретельного розслідування санкційними комітетами, оскільки вони можуть бути використані для обходу санкцій.

З урахуванням загрози неспровокованої збройної агресії з боку російської федерації, яка була засуджена резолюцією Генеральної Асамблеї ООН A/RES/ES-11/1 від 02.03.2022 [400], США та ЄС запровадили жорсткі санкції проти російських фінансових установ, причетних до агресії проти України, таких як Сбербанк Росії, ВТБ Банк та ін.

У період із 24 березня по 1 квітня 2022 р. Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) наклало санкції на понад 400 представників російської еліти, депутатів державної думи та оборонних компаній відповідно до Указу спеціального призначення (SDN) ЕО

14024 [401]. OFAC також опублікувало чотири нові обмежені загальні ліцензії щодо певної гуманітарної, пов'язаної з імпортом, дипломатичної та журналістської діяльності, додавши один новий поширений запит, та рішення щодо ЕО 14024. Окремо Білий дім вказав, що Сполучені Штати серйозно розглядати можливість введення вторинних санкцій проти компаній, які займаються ухиленням від упровадження санкцій до росії або бізнесом, який іншим чином підриває санкції. Доцільно зазначити, що згадані Загальні ліцензії не дозволяють здійснювати трансакції чи перекази, до яких залучені особи зі списку спеціально визначених громадян і заблокованих осіб (SDN), якщо такі операції прямо не передбачені положеннями цих чи інших Загальних ліцензій, виданих OFAC.

Міністерство торгівлі 1 квітня 2022 р. оголосило про додавання 120 російських та білоруських організацій до списку організацій BIS, встановивши вимогу отримання ліцензії з політикою відмови для всіх позицій, які підпадають під дію Регламенту управління експортом (англ. Export Administration Regulations (EAR)) [417; 405]. Зі 120 організацій 95 є так званими військовими кінцевими користувачами, позначеними виноскою 3, що підпорядковує їх додатковим, розширеним правилам нового російського/білоруського військового кінцевого користувача стосовно «прямого продукту», виробленого за кордоном.

ЄС також наклав повну заборону на трансакції на чотири ключові російські банки, включно з ВТБ, які представляють 23% ринку в російському банківському секторі. Після відключення від SWIFT активи цих банків тепер підлягають заморожуванню, у такий спосіб вони є повністю відрізаними від ринків ЄС [417; 405]. Крім того, Рада ЄС вирішила накласти санкції на компанії, чиї продукти чи технології відіграли роль у вторгненні в Україну, ключових олігархів та бізнесменів, пропагандистів, а також членів сімей тих, хто вже потрапив під санкції [417; 405].

Через обмежену ліквідність криптовалют і простір децентралізованих фінансів загалом для росії залишається майже неможливим обійти системи на основі SWIFT за допомогою криптовалют. Однак росіяни можуть тримати в криптоактивах до 200 млрд дол. США, до того ж вони керують третьою за величиною індустрією крипто майнінгу в світі. Ці кошти потенційно можна вивести з російських позабіржових провайдерів [406].

П'ятий пакет санкцій Європейського Союзу проти Росії, ухвалений у квітні 2022 року, включав обмеження на криптоактиви для російських громадян та юридичних осіб. Зокрема, було заборонено надання високовартісних криптовалютних послуг, що фактично обмежувало суми, які російські особи могли тримати на європейських криптоплатформах. Хоча точна сума обмеження в 10 000 євро не була офіційно підтверджена в доступних джерелах, численні повідомлення вказують саме на цю цифру як на ліміт для криптоактивів російських громадян та організацій. Варто зазначити, що ці обмеження були спрямовані на запобігання обходу фінансових санкцій через використання криптовалют. Щоб обійти ці санкції, були використані російські позабіржові провайдери, які представляють мережу фізичних ППВА, які пропонують виплати готівкою з переказів криптоактивів [407].

У надто спрощених термінах «позабіржовий» стосується процесу, в якому люди теоретично можуть домовитися про ціну та зустрітися, щоб завершити трансакцію. Прикладом такого процесу є особиста зустріч, під час якої одна сторона приносить сумки з готівкою або будь-якими іншими заздалегідь узгодженими коштами, а друга сторона може провести трансакцію на блокчейні на місці. Трансакції переважно з більшими сумами можуть бути, м’яко кажучи, ризикованими. На відміну від однорангових бірж (P2P), у яких беруть участь незалежні сторони, позабіржові біржі діють так само, як і фізичні ломбарди. У спеціально відведених фізичних місцях із оголошеними годинами роботи фізичні особи можуть відвідати й обміняти свої криптовалюти в росії на готівку або банківські перекази.

Залежно від бізнес-моделей ППВА як позабіржові, так і P2P-провайдери існували в різних юрисдикціях від початку фінансової взаємодії між особами. Прикладом такої платформи в ЄС є LocalBitcoin, зареєстрований в Управлінні фінансового нагляду Фінляндії. На відміну від російських позабіржових провайдерів, котрі підпадають під дію 6-ї Директиви ЄС про боротьбу з відмиванням грошей і пов’язані з так званим законодавством про боротьбу з фінансуванням тероризму, LocalBitcoin став унікальним випадком [408].

Нарешті, було вжито особливих заходів щодо боротьби з обходом санкцій. Так, організації та особи в третіх країнах, які сприяють порушенню європейських санкцій, теж можуть потрапити під їхню дію. Під час прийняття восьмого пакета санкцій було додано новий санкційний критерій, що дозволив включати до санкційного переліку особи або організації, котрі сприяють порушенню європейськими суб'єктами заборони на обхід санкцій.

Проаналізуємо інструменти уникнення санкцій російським фінансовим ринком з використанням нових технологій та операторів крипторинку.

Варто зазначити, що вимоги до реєстрації на криптобіржі або ОТС у російській федерації значно відрізняються. З одного боку, росія схвалила використання криптовалюти як інструменту інвестування або способу оплати з І кв. 2021 р., але з другого – її центральний банк запропонував довгий список заборон, які мають перешкоджати обігу криптовалют усередині країни. Через такі незрозумілі правові обставини нормативні акти щодо державного ліцензування та нагляду майже не працюють. У зв’язку з відсутністю платформ, які обрали процедури комплаєнсу та ПВК/ФТ як ділову стратегію, багатьом російським провайдерам доводиться працювати в сірому законодавчому полі.

Вражає те, що, попри утримання росіянами до однієї п’ятої резервів центрального банку в цифрових активах, вони не розкривають чіткої інформації про себе та свою діяльність ні для ППВА, ні для інших учасників децентралізованих фінансів (DeFi).

Уникаючи прозорості щодо гравців у сфері цифрових активів, уряди москви та мінська продовжують втрачати потенційні податкові надходження та регуляторний контроль над понад 623 криптоплатформами, пов'язаними з росією та білоруссю. Рішення ігнорувати легко оподатковуваний приріст капіталу від криптоінвестицій видається доволі сумнівним. Домініка Куберська, доктор філософії, з факультету економічних наук Вармінсько-Мазурського університету в Ольштині, наголошує: «Чи не парадоксально, що, незважаючи на заяву прем'єр-міністра росії про те, що росіяни володіють криптовалютою на суму 200 мільярдів доларів, росія досі не сформулювала всеосяжного законодавства для легалізації криптовалюти чи встановила для неї процес оподаткування?» [408].

За відсутності регульованих гравців у росії існує добре розвинутий сірий ринок позабіржових провайдерів, котрі полегшують торгівлю цифровими активами в обмін на рублі як готівкою, так і банківськими переказами. Джерела, які бажають залишитися анонімними, підкреслюють, що банківські перекази фізичним або юридичним особам від позабіржових брокерів позначаються як оплата за IT або консультаційні послуги. Російський уряд офіційно оподатковуватиме прибуток від таких переказів податком на доходи фізичних осіб або підприємств (ПДФО, ППП).

Більше того, для клієнтів, котрі бажають придбати або обміняти значну кількість цифрових активів, у москві є щонайменше 10 фізичних брокерів або працюють вебсайти порівняння цін, такі як BestChange.ru, що відображають поточні курси позабіржових провайдерів у різних регіонах. Через характер бізнес-моделі клієнти часто можуть обміняти готівку на цифрові активи у фізичних офісах цих бірж, які можуть відвідувати і фізичні особи, і члени російських органів фінансового нагляду, якщо вони визнають їх існування. Більшість постачальників позабіржових послуг працюють без ідентифікації своїх клієнтів. Багато джерел повідомляють про пряму співпрацю між спеціалізованими «схемами Понці» або санкційними брокерами з мережею

позабіржових операторів. Навіть якщо переконливі докази, такі як угода або обмін електронною поштою між підтвердженими сторонами, постійно збираються, аналітика блокчейну продовжує надавати ознаки незаконних трансакцій. Росію пов'язують із підвищеним обсягом незаконної діяльності для країни з населенням 144 млн осіб, що в 1,5 раза більше, ніж у Німеччині [409].

За словами практиків блокчейн-аналітичної компанії Global Ledger Protocol, «росія має напрочуд велику кількість підтверджених незаконних «єдинорогів», таких як обмін BTC-e/WEX, ринок темної мережі Hydra, десятки пірамідних схем, таких як PRIZM, найбільші атаки програм-вимагачів та інші кіберзлочини, котрі експерти розглядають як діяльність, що частково спонсорується державою» [405].

Оскільки фіксується так багато підтверджених незаконних дій, що виходять з однієї юрисдикції, варто дослідити можливості потенційного переведення в готівку прибутків від незаконної діяльності. Як детально описано вище, перевага публічного блокчейну полягає в тому, що він залишається відкритим і відстежується.

Прикладом такої підтвердженої незаконної діяльності, яку можна вивести з російського позабіржового провайдера, можуть бути рух коштів постачальника криптовалютного гаманця під назвою Konvert.im. (рис. 3.4) (Додаток Ґ).

Він охоплює понад 100 трансакцій і характеризується більш як 69 % ризику для коштів, що надходять із нещодавно санкціонованого Hydra Darknet Marketplace.

Результати розслідування показали, що на ньому зберігається майже 74% незаконних коштів, що надходять від санкціонованої організації Hydra, що підтверджує рис. 3.5.



Рис. 3.4: Результати розслідування адреси 3HdSxDUirbVjjD4MEiQmu6fbCvsNcGWJWf криптовалютного гаманця Konvert.im

Джерело: побудовано автором [289, доступ 1 травня 2022 р.]

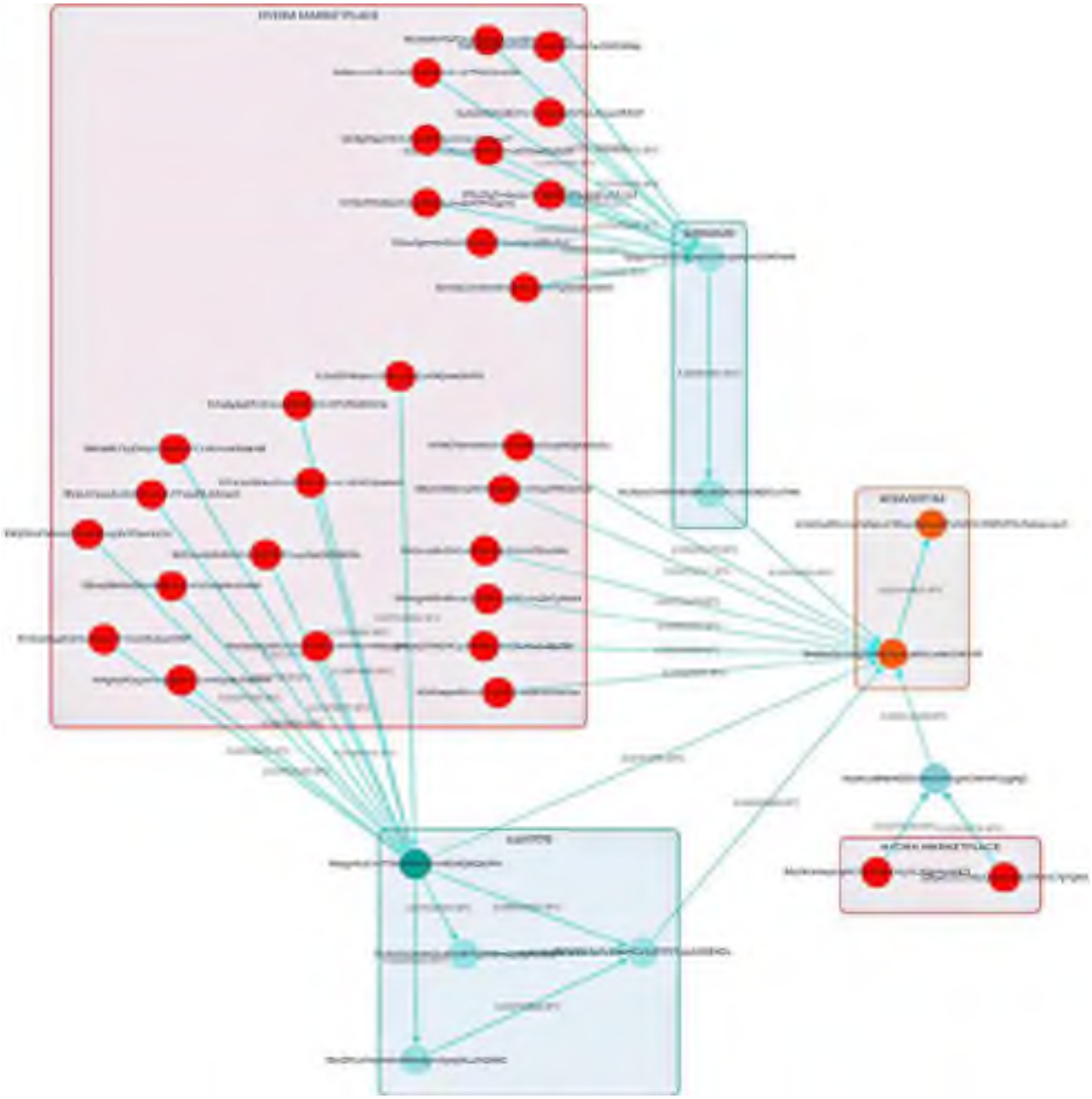


Рисунок 3.5: Аналітика на основі блокчейну з гаманців, пов’язаних з Hydra.

Джерело: побудовано автором [289, доступ 1 травня 2022 р.].

Результати аналізу потенційно незаконних кластерів блокчейну можна було б вивести з російських позабіржових провайдерів, оскільки екосистема Blockchain позначила ці трансакції. Кошти, отримані від таких трансакцій, відображаються в Blockchain і, швидше за все, не будуть обмінюватися в майбутньому на платформі, яка відповідає вимогам ПВК/ФТ.

Надамо пояснення до графіка. Червоні точки представляють адреси гаманців криптовалют, ідентифіковані та підключені до санкційної платформи Hydra; помаранчеві точки – адреси гаманців криптовалют, пов'язані з переказами на konvert.im Сині крапки та стрілки представляють інші гаманці криптовалюти та спрямування або перекази між такими гаманцями.

Рисунок вище зображає трансакції, які походять із уже санкційного кластера Hydra (представлені червоними крапками), які проводяться через посередницькі гаманці 1kzqyn1ucntty1bze3wq4ka8jdqbs2sjph і 13etennrsypcbh4hgxjcepp, FCqqNG8EXDL так само як 14L11zwChHRYBk58KLdxD6LKWD8ZGuv7Hb (представлені блакитними крапками) до гаманця 3HdSxDUirbVjjD4MEiQmu6fbCvsNcGWJWf, який належить до кластера Konvert.im (позначений помаранчевими крапками).

Оскільки Konvert.im представляє біржу, безсумнівно, ого представники повинні знати про походження цих коштів із санкційної Hydra. Саме в рамках таких схем кошти можуть бути змішані з іншими коштами, які потенційно можуть бути спрямовані позабіржовим провайдерам для виведення в готівку.

Незалежно від вибору постачальника, який використовується для аналітики на основі Blockchain, через природу розслідувань на основі Blockchain, які накопичують усі кошти та їх сліди між різними брокерами, завжди буде певний ризик незаконного трафіку, який здебільшого, ймовірно, буде однозначним у відсотках. З огляду на це неможливо стверджувати, що вплив Hydra на 69 % було технічною помилкою. Це радше слід сприймати як спеціальну дію, і відстеження грошей від Konvert.im до російського позабіржового провайдера може слугувати символом того, що така стратегія може бути прийнята для уникнення санкцій на основі SWIFT і легкого обходу обмеження, зазначеного в п’ятому пакеті санкцій ЄС.

У сфері криптоактивів необхідно використовувати всі наявні технологічні та правові інструменти для цілеспрямованого застосування санкцій. Акцент слід зробити на нагляді, потреби змінювати нормативну базу немає.

Головною метою нині має бути швидке взяття добровільних зобов’язань у формі кодексів поведінки крипто- та фінансовими технологічними компаніями у співпраці з регуляторами й органами нагляду за фінансовими ринками. Зловживання ліцензованими особами у сфері фіатних платіжних послуг становить більший ризик, ніж усе ще менш поширений ринок криптоактивів, які загалом пропонують кращі засоби відстеження трансакцій.

Одним із шляхів уникнення санкцій є виведення капіталу за допомогою криптоактивів, включно з NFT, послуги з фінансових технологій (і традиційних фінансових), приховування особи та/або організації, які постраждали від санкцій (використання інших організацій, переважно бізнес-корпорацій, часто зареєстрованих у податкових гаванях на членів сім'ї або інших пов'язаних осіб), зловживання SWIFT для обходу санкцій за допомогою посередників, котрі дозволяють доступ до нього через власні системи, використання небанківських платіжних послуг як альтернативи проведенню операцій у разі недоступності традиційних платіжних інструментів, придбання державних та/або ліквідних приватних цінних паперів через конвертаційні майданчики (нелегальні утворення фінансових груп для конвертації готівкових коштів у безготівкові й навпаки), вкладання в інструменти страхового та товарного ринків, зловживання організаціями, ліцензованими в ЄС, ЄЕЗ або США, також шляхом їх придбання. Однак здебільшого це стосується суб’єктів, котрі вже мають зв’язки з російськими/білоруськими суб’єктами або діють у сірій зоні. Для цієї мети можна використовувати директиву про бенефіціарне володіння, але також корисним може бути глибший аналіз, зокрема інвесторів таких організацій [403].

Необхідним, крім того, є застосування суворіших процедур ПВК/ФТ, таких як профілактичні перевірки суб'єктів та осіб, пов'язаних із суб'єктами санкцій, у тому числі перевірки осіб, близьких до осіб, зазначених у списках санкцій. Для цих цілей та з метою запобігання неправильній ідентифікації трансакцій як підозрілих слід звернутися до національних органів із ПВК/ФТ.

До глибшого аналізу криптовалютних операцій необхідно включити використання операції обміну в криптовалютних банкоматах (АТМ). Трансакції в більшості криптоактивів утворюють зв'язаний ланцюжок, який можна простежити назад або вперед у часі. Аналіз ланцюжка трансакцій може виявити, що походження коштів пов'язане з програмним забезпеченням-вимагачем, шахрайством, крадіжками, темними ринками тощо. У такому аналізі корисні публічні дослідники або власні аналітичні рішення блокчейну.

Національний банк України продовжує працювати над підвищенням стабільності та прозорості ринку небанківських фінансових послуг, зокрема платіжних, а також посиленням захисту їхніх користувачів. З цією метою Національний банк вніс зміни до порядку здійснення авторизації діяльності надавачів фінансових платіжних послуг і обмежених платіжних послуг, встановив додаткові вимоги до заявників, котрі мають намір отримати авторизацію діяльності на платіжному ринку України. Такі вимоги повинні також виконуватися протягом усього строку дії авторизації. Зокрема, встановлено додаткові вимоги в частині:

- ділової репутації та професійної придатності відповідального працівника за проведення фінансового моніторингу;
- технічних та інших умов, необхідних для надання фінансових платіжних послуг (наявність комп'ютерної техніки, належних облікових і реєструючих систем, приміщення за місцезнаходженням заявника);
- відсутності виявлених фактів порушень у сфері фінансового моніторингу та в реалізації спеціальних економічних та інших обмежувальних заходів (санкцій) протягом одного року, що передує даті подання до Національного банку пакета документів для авторизації.

У зв'язку з цим заявники, котрі мають чинну ліцензію на переказ грошових коштів та вже подали до Національного банку пакети документів для переліцензування, повинні:

– надати Національному банку запевнення (у довільній формі) щодо відповідності встановленим регулятором вимогам (протягом п’яти робочих днів із дня набрання чинності цими вимогами);

– подати до Національного банку власну політику винагороди (протягом 30 робочих днів із дати авторизації);

– провести опитування користувачів щодо наявності в них відносин із країною-агресором та надати Національному банку інформацію про результати такого опитування (протягом 60 робочих днів із дати авторизації).

Заявники, які мають чинну ліцензію на переказ і подаватимуть документи для отримання авторизації вперше або повторно (пакети документів яких було залишено без розгляду), повинні подавати документи для отримання авторизації з урахуванням нових вимог, зокрема додати до інших документів нову заяву з підтвердженням відповідності новим вимогам. Також вони зобов’язані протягом 30 робочих днів із дати авторизації подати власну політику винагороди та протягом 60 робочих днів із дати авторизації провести опитування користувачів щодо наявності в них відносин із країною-агресором, надати Національному банку інформацію про результати такого опитування.

Заявники, котрі подаватимуть документи для отримання авторизації вперше, мають надати Національному банку пакет документів з урахуванням нових вимог, зокрема разом з іншими документами – оновлену заяву, власну політику винагороди. Подібне посилення вимог до надавачів фінансових платіжних послуг спрямоване на унеможливлення отримання ліцензій «недоброчесними» учасниками ринку та недопущення потрапляння на ринок фіктивних учасників чи компаній-оболонок, особливо в умовах дії воєнного стану в Україні, а також забезпечення додаткових гарантій прозорості українського фінансового ринку й унеможливлення його використання в цілях держави-агресора.

Крім того, це сприятиме мінімізації ризиків, пов’язаних із наданням фінансових платіжних послуг, та забезпеченню достатнього захисту

користувачів платіжних послуг. Строк для переліцензування заявників, які мають ліцензії на переказ коштів у національній валюті без відкриття рахунків, продовжено з шести до дев'яти місяців. Відповідні норми містить постанова Правління Національного банку України «Про внесення змін до деяких нормативно-правових актів Національного банку України щодо порядку здійснення авторизації діяльності надавачів фінансових платіжних послуг» від 01.03.2023 № 14, що набрала чинності 3 березня 2023 р. [413].

Це стало причиною проблем в операціях криптобірж з українськими картками. Подібна проблема виникала і раніше. У вересні 2022 р. в Україні було обмежено виведення коштів з криптобірж на картки банків згідно з постановою НБУ № 18 від 20.04.2022 (далі – Постанова № 18). Згідно з нею, банк зупиняє (повертає) вхідні та вихідні перекази в іноземній валюті, якщо існує підозра, що вони пов'язані із забороненою в Україні діяльністю [414].

Постанова № 18 стосується, зокрема, переказів, «отриманих в результаті купівлі та продажу однієї іноземної валюти за іншу іноземну валюту задля отримання прибутку від зміни валютного курсу (форексні угоди), а також переказів з електронною валютою» [414]. У НБУ пояснили, що згадані операції слід трактувати «як такі, що призводять до непродуктивного виведення капіталу з країни».

Криптобіржі, які працюють з українськими фінансовими компаніями, зокрема Kuna, Binance, Qmall, WhiteBit та ін., призупинили виведення коштів на картки українських банків. Як альтернативу пропонують використовувати інші методи отримання грошей, зокрема P2P-сервіс. Про складнощі повідомили також представники інших криптобірж, але криптообмінники та криптобіржі переважно повернулись до старих способів роботи, що не сприяють підвищенню прозорості операцій з криптоактивами.

Наведемо окремі з найбільш легко реалізованих санкцій щодо припинення повномасштабної агресії в Україні на основі блокчейну:

По-перше, це санкції проти російських та білоруських криптоброкерів. Нині існують понад 623 криптовалютні платформи, які діють у межах юрисдикцій росії та білорусі або принаймні пов’язані з цими країнами. Подібно до припинення доступу російських банків до SWIFT криптовалютні брокери можуть потрапити і вже потрапили під санкції. Запровадження санкцій проти таких платформ обмежує не лише традиційні банківські та карткові трансакції з таких переказів, а й усі трансакції, які вже здійснюються ними в блокчейні. Санкції щодо криптовалютних брокерів із високим ризиком не є чимось новим. Такі платформи, як Garantex, Hydra і Tornado Cash, вже підпали під санкції за програмне забезпечення-вимагачі, яке включене до санкційного списку OFAC.

Коротко розповімо про кожну з них:

1) Hydra була найбільшим ринком Даркнету у світі, поки її сервери не були конфісковані німецькою поліцією одночасно з визнанням OFAC у квітні 2022 р., що фактично закрило ринок. Розташована в росії Hydra не тільки сприяла продажу наркотиків, а й пропонувала послуги з ВК кіберзлочинцям, зокрема зловмисникам програм-вимагачів.

2) Garantex — криптобіржа з високим ризиком, розташована в росії, що водночас із Hydra потрапила під санкції за аналогічну діяльність із ВК. Так само як Hydra, Garantex припинала діяльність, однак блокчейн-аналітиками виявлено криптобіржу Greenex, яка продовжила працювати з клієнтами Garantex за таким самим призначенням.

3) Tornado Cash — це децентралізований протокол змішування транзакцій на блокчейні Ethereum, до якого у серпні та листопаді 2022 року було застосовано санкції з боку Управління з контролю за іноземними активами США (OFAC). Підставою стало сприяння сервісом відмиванню коштів, отриманих кіберзлочинцями, пов’язаними з Північною Кореєю, під час хакерських атак на криптовалютні платформи. Наразі Tornado Cash є єдиним DeFi-протоколом, що потрапив під санкції OFAC, тоді як всі інші санкціоновані сервіси були централізованими платформами або індивідуальними криптогаманцями.

Враховуючи децентралізовану природу цього протоколу, жодна особа чи організація не має технічної можливості так само легко зупинити роботу Tornado Cash, як це можливо з централізованими сервісами. Це, у свою чергу, викликало дискусії щодо ефективності та доцільності застосування санкцій саме до таких децентралізованих послуг, а також питання визначення суб'єкта відповідальності за злочинну діяльність, якій сприяє протокол.

Незважаючи на те, що цей підхід, здається, найпростіший для впровадження законодавцями, є необхідність уточнення інформації, поданої криптовалютними брокерами до підрозділів фінансової розвідки, які відповідають за обробку таких повідомлень.

На відміну від традиційних фінансів, сучасні програми для забезпечення комплаєнсу на основі блокчейну реагують навіть на невеликі трансакції. Наприклад, якщо користувач здійснює операцію на понад 10 тис. дол. США, або якщо трансакція з криптовалютою на суму лише 5 дол. США пов'язана із суб'єктами санкцій, блокчейн-аналітична система генерує сигнал тривоги для запуску ручної перевірки. У таких випадках криптоброкеру, ймовірно, буде доцільно подати звіт про підозрілу трансакцію (англ. Suspicious Transaction Report, STR) до правоохоронних органів.

Таким чином, навіть якщо позначений криптовалютний гаманець не належить конкретному користувачеві, служби комплаєнсу в більшості юрисдикцій все одно подають звіти про підозрілу трансакцію (STR) до правоохоронних органів, а клієнту блокують можливість проводити операції. Такий надмірний підхід спричиняє витрачання цінних ресурсів, обтяжуючи й без того перевантажені ПФР та поліцію, які займаються обробкою цих звітів. Відсутність міжнародних стандартів для звітності про трансакції на основі блокчейну залишається значною перешкодою для ефективного моніторингу цієї сфери.

По-друге, встановлення порогових значень та заморожування наявних рахунків великих гравців. Регулятори також можуть розглянути можливість

заморожування таких рахунків, що відкриті як у централізованих, так і в децентралізованих фінансових проєктах, які мають ліцензії на банківську діяльність та емісію електронних грошей (англ. Electronic Money Institution, EMI) від національних та міжнародних фінансових органів з ідентифікованими та неявними (наприклад, повторний доступ з IP-адрес (VPN) в росії) російськими філіями.

По-третє, припинення видачі нових банківських і фінтех-ліцензій проєктам, пов'язаним із росією та білоруссю. Компанії, в яких частка кінцевого бенефіціарного власника серед російських або білоруських громадян становить 10–25 % (залежно від юрисдикції) капіталу чи прав голосу в головній організації, не повинні отримувати фінансових ліцензій. Компанії, що вже мають фінансові ліцензії, зокрема у сфері DeFi, і мають російських чи білоруських бенефіціарів або отримують фінансування від так званих сірих кардиналів, котрі надають значні кредити організаціям, можуть бути перевірені, наприклад, органами фінансового нагляду.

По-четверте, заморожування активів осіб, які перебувають під санкціями (наприклад, олігархів). Це вже реалізується, оскільки криптовалютні брокери та ППВА мають юридичні зобов'язання проводити санкційні перевірки осіб, котрі користуються їхніми платформами.

Процес моніторингу працює ефективно, якщо користувачі обмінюють криптовалюту на фіатну валюту через традиційні банківські рахунки або кредитні картки. Недоліки цього рішення зумовлені складністю контролю коштів, якщо вони вже увійшли до простору DeFi до того, як тіньові особи були піддані санкціям. Якщо гроші вийшли з традиційної банківської системи, ці особи можуть доволі легко спробувати уникнути санкцій, використовуючи децентралізовані біржі, змішувачі, тумблери, купуючи NFT або монети конфіденційності.

Якщо такі користувачі прийняли обґрунтоване рішення уникати продуктів DeFi з юрисдикцій, які вже запровадили правило подорожей FATF або піддали

криптовалютні трансакції регулюванню протидії ВК, то ймовірність відстеження таких коштів на кількох різних біржах криптовалюти може вимагати більше часу та ресурсів, але не є неможливою.

Станом на червень 2021 р. FATF повідомляла, що лише 58 зі 128 звітних юрисдикцій запровадили переглянуті стандарти та рекомендували ППВА припинити зв'язки з компаніями, які працюють у юрисдикціях, де рекомендація щодо правила подорожей не була виконана [415].

Однак, оскільки рекомендації FATF є не законами чи нормативними актами, а рекомендаціями, вони не мають юридичної сили. За результатами недавнього опитування лише 11 % ППВА вирішили припинити переказ коштів іншим брокерам у країнах, які ще не запровадили згадане правило. Оскільки майже 45 % юрисдикцій його ще не застосовують, рекомендація припинити операції з брокерами, котрі базуються в юрисдикціях, де вони не запроваджені, означатиме виключення значної частини ринку. Брокери не вважають себе зобов'язаними це робити [416].

По-п'яте, зупинення операцій на DeFi-платформах, які взаємодіють із російською платіжною системою, включно з MIR Pay. Після того як Visa, Mastercard і American Express припинили співпрацю з російськими банками, все ще залишаються платформи, що дають змогу користувачам здійснювати банківські перекази з росії на основі рубля через як національні, так і міжнародні системи переказів. Лише невелику частину банків було відключено від SWIFT. Крім того, Росія, хоч і в обмеженому масштабі, використовує власну платіжну систему "МИР". Провайдери та платформи, що пропонують продукти DeFi, такі як стейблкоїни чи NFT, і надають можливість росіянам поповнювати або виводити кошти, можуть стикнутися з вибором: припинити ці трансакції або стати об'єктами санкцій.

По-шосте, запровадження санкцій на продаж обладнання для майнінгу криптовалют до росії. У минулому країни, багаті енергоресурсами, такі як Іран, що перебували під санкціями, могли масово закуповувати обладнання для

майнінгу криптовалют і використовувати дешеву електроенергію для забезпечення своїх майнінгових центрів. Наприклад, станом на 21 серпня 2021 р., за даними Cambridge Bitcoin Electricity Consumption Index, середня місячна частка хешрейту в Ірані становила 3,11 %, що майже вдвічі більше, ніж у 2019 р. [417]. Хешрейт демонструє ефективність та продуктивність пристроїв для видобутку криптовалюти. Вимірюється в хешах за секунду (Х/с).

Майнінг визначається як фактор низького ризику щодо ризик-орієнтованого підходу дотримання вимог ППВА [418].

Такі кошти можуть бути переведені в готівку в третіх країнах і інтегровані в традиційну фінансову систему. Обладнання для майнінгу криптовалют і його компоненти дають змогу росії конвертувати природні ресурси в енергію. Хоча білорусь великою мірою залежить від російської енергетики й навряд чи активно інвестуватиме в майнінгове обладнання, вона історично була відома як точка обходу санкцій. Наприклад, у 2014 р. білорусь, не маючи виходу до моря, стала найбільшим експортером лосося до росії: норвезька риба, оброблялася й експортувалася, обходячи заборони.

Аналогічно в Казахстані вжито заходів щодо закриття комерційних підприємств із росії, які використовують банківську систему країни для здійснення розрахунків за товари без фактичного переміщення через митну територію. Такі підприємства, очевидно, застосовують ці схеми для обходу санкцій, накладених на російські банки.

Санкції можуть бути дієвими лише тоді, коли ті, хто їх застосовує, мають чітке розуміння своїх обов’язків. Однак чинний регламент створює істотну невизначеність, особливо у випадку з обмеженнями на цифрові активи. П’ятий пакет санкцій ЄС щодо росії, зокрема ліміт у 10 тис. євро на криптоактиви для російських громадян і організацій, залишається недостатньо зрозумілим. Ця межа лімітує володіння криптоактивами через одного провайдера (рахунок, гаманець чи сховище). Проте через нестабільність криптовалют складно передбачити їхню вартість, щоб не порушити цей ліміт. Наприклад, постає

питання, як ППВА слід тлумачити ситуацію, коли криптоактиви на момент депозиту коштують менше порогового значення, але їхня вартість зростає з часом. Запит до ЄС щодо додаткових роз'яснень цієї санкції не надав чітких відповідей. У результаті постачальники послуг змушені самостійно розробляти інтерпретації та механізми запобігання порушенням, що ускладнює уніфіковане застосування санкцій і знижує їхню ефективність. Через ці невизначеності санкція, пов'язана з лімітом у 10 тис. євро, викликає більше запитань, ніж відповідей, що підриває її практичність і контрольованість.

На виконання Закону від 06.12.2019 № 361-IX щодо ПВК/ФТ, який набув чинності 28 квітня 2020 р. [419], Уряд затвердив оновлену редакцію Положення про Єдину державну інформаційну систему (ЄДІС) у сфері запобігання та протидії відмиванню коштів [420]. Зокрема, оновлено порядок формування Переліку осіб, пов'язаних із терористичною діяльністю або щодо яких застосовано міжнародні санкції. Нова редакція документа передбачає, що підставами для включення або виключення осіб із Переліку є: рішення адміністративного суду про відповідність критеріїв, визначених резолюціями Ради Безпеки ООН, або інформація міжнародних організацій щодо осіб, котрі пов'язані з терористичними організаціями чи підпадають під міжнародні санкції [421]. Дані про громадян, іноземців, юридичних осіб та трасти подаються до ДСФМУ, СБУ та МЗС для їх внесення до Переліку. Ті самі органи розглядатимуть запити на виключення осіб із цього списку. МЗС, зокрема, відповідатиме за забезпечення зв'язку з Комітетом Ради Безпеки ООН для розгляду таких питань [421]. Крім того, передбачено оперативне інформування суб'єктів первинного фінансового моніторингу про відповідні зміни. Реалізація цих положень спрямована на забезпечення відповідності українського законодавства міжнародним стандартам FATF.

На додаток зазначимо, що існує ряд хостинг-провайдерів, які забезпечують у рамках їхньої комерційної політики захист російських постачальників криптовалютних послуг, сприяють обходу обмежень, встановлених Указом

США 14024 та Регламентом Ради ЄС 833/2014 [453; 422]. Для багатьох криптовалютних операторів зі списку таку підтримку хостингу надає сервіс DDOS GUARD, підконтрольний громадянам росії [422].

DDOS-GUARD сьогодні є одним із найважливіших елементів кіберсистеми російської федерації, що підтримує її зовнішню фінансову та пропагандистську діяльність. Доступна інформація з відкритих джерел показує, що:

- DDOS-GUARD (DG) надає хостинг і захист від ddos-атак як криптооператорів рф, так і пропагандистських ресурсів, подібних RT-news (всі вони або безпосередньо перебувають під санкціями, або сприяють обходу санкцій)

- DG юридично створена як COGNITIVIVE CLOUD L.P., компанія в Шотландії, що контролюється двома громадянами росії

- частина серверів DG розташована за межами російської федерації.

Міністерство закордонних справ на виконання резолюції Віце-прем'єр-міністра України – Міністра з питань реінтеграції тимчасово окупованих територій України від 16.04.2022 № 9330/1/1-22 до листа заступника Секретаря Ради національної безпеки і оборони України від 11.04.2022 № 768/14-05/2-22 направило звернення до Посольства Великої Британії та Посольства США щодо припинення обслуговування постачальників криптовалютних послуг, підключених до Росії, які сприяють обходу обмежень, встановлених резолюцією Генеральної Асамблеї ООН A/RES/ES-11/1 від 02.03.2022, Указом США № 14024, Регламентом Ради ЄС 833/2014 там Положення про санкції Великої Британії щодо російської федерації 2022 р.

Припинення діяльності DDOS-GUARD (DG) через застосування санкцій та ретельне розслідування його діяльності може розкрити мережу російських фінансових, пропагандистських та інших активів і порушить підтримувану росією інфраструктуру криптовалютних сервісів, що сприяє обходу санкцій.

Крім того, у тісній взаємодії з криптопровайдерами України і світу запущено механізм спонтанного блокування криптогаманців рф. Вжито інших спеціальних дій зі стримування агресії рф на ринку віртуальних активів.

Співпраця з наглядовими та правоохоронними органами ґрунтується на конкретній звітності про будь-які підозрілі дії та операції, що здійснюються постачальниками фінансових послуг, які працюють на ринку ЄС і США.

Ще одна ініціатива щодо розбудови ефективної взаємодії з боку Департаменту кіберполіції Національної поліції України в рамках виконання основного завдання, а саме реалізації державної політики у сфері протидії кіберзлочинності, завчасного інформування населення про появу новітніх кіберзлочинів та впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини, спрямована на об’єднання зусиль органів центральної влади, представників правоохоронних і судових органів, ПФР та державних наглядових органів, що мають повноваження й володіють інформацією, яка направлена на прискорення реагування на сучасні виклики кібербезпеки та захисту економічної безпеки України при Раді національної безпеки та оборони України. За відсутності ефективного державного наглядового органу над ринком ВА така ініціатива може об’єднати зусилля державного і приватного секторів.

Об’єднання зусиль із боку органів центральної влади, представників правоохоронних та судових органів, ПФР та державних наглядових органів, що мають повноваження й володіють інформацією, а також експертів криптоспільноти, котрі є розробниками аналітичних програм щодо відстеження операцій з ВА, експертами банківського сектору та платіжних систем сприятиме створенню ефективного інструменту протидії обходу санкції проти російських фінансових установ, причетних до агресії рф проти України.

Оскільки процедури нагляду щодо ідентифікації та скринінгу списків клієнтів базуються на ризик-орієнтованому підході, фінансовим установам доцільно запровадити ризик-орієнтований підхід і до заходів щодо перевірки

джерел походження ВА у клієнта, з огляду на основні ризики, які створюють такі активи.

Зобов'язання розвивати розумний підхід щодо «мети та характеру ділових відносин» під час моніторингу рахунків на предмет виявлення підозрілої діяльності доцільно застосовувати до угод з ВА так само, як і стосовно операцій із фіатними грошима. Знову-таки, якщо у фінансових установ виникають особливі занепокоєння щодо діяльності на ринку ВА, таким установам, швидше за все, доцільно розробити спеціальні «червоні прапорці» (критерії ризику), які застосовуються на торгових майданчиках з віртуальними активами блокчейн-аналітичними компаніями, навчити відповідальних працівників оцінці ризиків щодо уникнення санкцій в операціях з ВА.

Важливо враховувати, що в Україні запустили портал «Війна і санкції», аби запровадити санкції до якомога більшої кількості співучасників війни рф проти України, і цю базу даних українським державним і комерційним банківським установам необхідно терміново інтегрувати в політики й процедури комплаєнсу та ПВК/ФТ [423] (рис. 3.6).

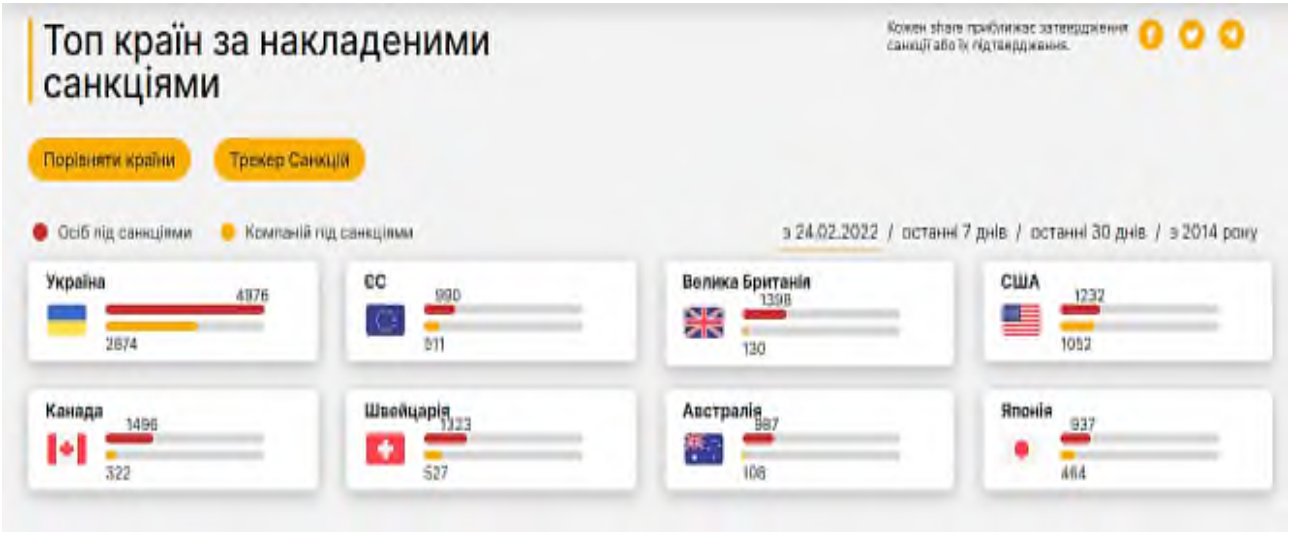


Рис. 3.6. Аналіз запровадження країнами санкцій щодо російської збройної агресії в Україні

Джерело: побудовано автором [423].

Портал дає змогу переглянути перелік осіб, на котрих уже накладено санкції з початку повномасштабної війни проти України, а також ознайомитися із кандидатами на потрапляння до санкційних списків. Головна мета порталу — поінформувати іноземні уряди та громадян про вже запроваджені санкції, залучити громадськість до глобальної кампанії з розширення санкційних списків щодо осіб, які підтримують війну, зокрема фінансово та інформаційно. Це допоможе забезпечити максимальний економічний тиск на співорганізаторів війни та наблизити перемогу України Водночас нерегульований ринок ВА в Україні унеможливлює відстеження й управління грошовими потоками, які переміщуються всередині та за межами країни через віртуальні активи.

Міжнародні та державні організації дедалі більше співпрацюють із представниками приватного сектору, а саме фахівцями криптоіндустрії, у сфері аналізу ризиків використання криптоактивів у злочинних операціях. Це міжнародні аналітичні компанії, котрі розробляють і вдосконалюють безперервно в часі програмні продукти дослідження операцій у блокчейні. Серед визнаних компаній за останні п’ять років відзначено Chainalysis Reactor, Elliptic, CipherTrace, Certik, Coinfirm, Slowmist, Crystal, Global Ledger, AMLbot [424-429; 287-289]. Не можна однозначно віддати належне одній з перелічених компаній, оскільки всі вони мають свої переваги в певний час і в конкретній ситуації. Для досконалого дослідження (розслідування) часто необхідно використовувати не один програмний продукт. Але з огляду на значну вартість (100–300 тис. дол. США на рік) отримати ліцензії на певну кількість програмних продуктів часто проблематично, передусім для державних органів влади, правоохоронної та судової системи.

Наявність програмного забезпечення вимагає обізнаного персоналу, що викликає потребу в додаткових ресурсах на навчання та підвищення кваліфікації. Саме завдяки проведенню розслідувань збирається доказова інформація для правоохоронних і судових органів, здійснюється регуляторний нагляд за ППВА.

Інструменти аналізу блокчейну підтримали та використовують успішні правоохоронні органи.

Наразі дедалі більшого визнання й поширення набуває ризик-орієнтований підхід, застосування котрого створює сприятливі умови для розвитку нових ринків, запобігання використанню нових інструментів зі злочинними намірами, ефективному державному регулюванню й діяльності правоохоронної та судової системи. Особливої уваги в контексті врегулювання й визначення ризиків потребують взаємодія криптобізнесу із секторами реальної економіки, так звані шлюзи обміну віртуальних активів на фінансові інструменти, цінні папери, нерухомість, майнові права тощо. Важливо забезпечити гармонійну співпрацю наглядових органів реальних секторів економіки із наглядовим органом ринку ВА, наявність якого рекомендована міжнародними стандартами.

За першими результатами впровадження десятого пакета санкцій Європейського Союзу, спрямованих на протидію обходу санкцій з використанням криптоактивів та новітніх технологій щодо неспровокованої агресії російської федерації до України, реальними викликами стали регулювання ринку ВА, взаємодія державних, правоохоронних органів із приватним сектором та блокчейн-експертами, залучення їх до співробітництва при уповноваженому державному органу з питань національної безпеки.

В умовах широкомасштабної збройної агресії рф проти України, що триває, та у зв’язку з реальними на цій підставі загрозами національним інтересам і національній безпеці України, а також діями, що порушують права і свободи людини і громадянина з боку держави-агресора, яке, зокрема, проявляється у використанні ВА з метою обходу раніше накладених обмежувальних заходів (санкцій), фінансування терористичної, розвідувальної та диверсійної діяльності держави-агресора, виникає необхідність подальшого розширення санкцій.

Актуальність зазначеного посилюється і проблемою неврегульованості обороту ВА в Україні. Ухвалення Закону України «Про віртуальні активи» від

11.06.2020 № 3637 [430] хоч і стало істотним кроком вперед у регулюванні й створенні легального ринку віртуальних активів на національному рівні, однак нові правила ще не набрали чинності. Термін їх введення залежить від внесення відповідних поправок до Податкового кодексу, які вже певний час перебувають на стадії обговорення (13 березня 2022 р. у Верховній Раді України зареєстровано проєкт Закону про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами (реєстраційний номер 7150)). Така ситуація створює поле для махінацій у відповідній сфері, зокрема можливості уникнення раніше накладених обмежувальних заходів (санкцій) на державу-агресора та її суб'єктів, що здійснюють обхід санкцій за допомогою віртуальних активів.

Відповідно до ст. 3 Закону України «Про санкції» підставами для застосування санкцій є: дії іноземної держави, іноземної юридичної чи фізичної особи, інших суб'єктів, які створюють реальні та/або потенційні загрози національним інтересам, національній безпеці, суверенітету і територіальній цілісності України, сприяють терористичній діяльності та/або порушують права і свободи людини і громадянина, інтереси суспільства та держави, призводять до окупації території, експропріації чи обмеження права власності, завдавання майнових втрат, створення перешкод для сталого економічного розвитку, повноцінного здійснення громадянами України належних їм прав і свобод [431].

Статтею 6 Закону України «Про національну безпеку України» Верховна Рада України визначена одним із суб'єктів демократичного цивільного контролю у відповідній сфері [432].

У свою чергу, пропозиції щодо застосування, скасування та внесення змін до санкцій виносяться на розгляд Ради національної безпеки і оборони України Верховною Радою України, Президентом України, Кабінетом Міністрів України, НБУУ (ст. 5 Закону України «Про санкції»).

Сучасні реалії вимагають від України швидких та ефективних кроків у врегулюванні законодавства. Тому доцільно схвалити й подати на розгляд Ради

національної безпеки і оборони України пропозиції щодо застосування секторальних економічних та інших обмежувальних заходів (санкцій) до ППВА, котрі співпрацюють із банками рф та рб, а також пов’язаних із ними осіб:

1) блокування активів – тимчасове обмеження права особи користуватися та розпоряджатися належним їй майном;

2) стягнення в дохід держави активів, що належать фізичній або юридичній особі, а також активів, щодо яких така особа може прямо чи опосередковано (через інших фізичних або юридичних осіб) вчиняти дії, тотожні за змістом здійсненню права розпорядження ними;

3) обмеження торговельних операцій;

4) запобігання виведенню капіталів за межі України;

5) анулювання або зупинення ліцензій та інших дозволів, одержання (наявність) яких є умовою для провадження певного виду діяльності;

6) обмеження або припинення надання електронних комунікаційних послуг і використання електронних комунікаційних мереж.

Також доцільно передбачити встановити зобов'язання Національному банку спільно з Державною службою фінансового моніторингу України розробити методику виявлення учасниками фінансового та платіжного ринків активів, що належать (мають відносини контролю) ППВА, на яких поширюються такі дії, їх блокування та повідомлення державних органів України про такі активи, що має забезпечувати:

1) блокування ВА – тимчасове обмеження права користуватися та розпоряджатися особам до котрих застосовані санкції, належним їм майном (або таким, що перебуває під контролем такої особи) – віртуальними активами;

2) блокування активів – тимчасове обмеження права користуватися та розпоряджатися особам, до яких застосовані санкції, належним їм майном (або таким, що перебуває під контролем такої особи),

3) стягнення в дохід держави активів, що належать фізичній або юридичній особі, а також активів, щодо яких така особа може прямо чи опосередковано

(через інших фізичних або юридичних осіб) вчиняти дії, тотожні за змістом здійсненню права розпорядження ними;

4) обмеження операцій з придбанням чи реалізації ВА особам до котрих застосовані санкції, усіма суб'єктами (юридичними і фізичними особами) в межах юрисдикції України;

5) заборона обміну ВА, що належать, або що перебувають під контролем осіб, до яких застосовано санкції, на інші віртуальні активи;

6) повна заборона вчинення правочинів щодо віртуальних активів, емітентами яких є особи, до яких застосовано санкції;

7) блокування правочинів щодо ВА, в історії блокчейну яких міститься запис щодо належності трансакцій особам, до котрих застосовано санкції;

8) заборона обміну ВА, власниками яких є особи, до котрих застосовано санкції, на національну валюту України та іноземні валюти;

9) блокування трансакцій (грошових переказів та платежів) щодо ВА, в історії трансакцій блокчейну яких міститься запис щодо належності особам, до яких застосовано санкції;

10) блокування трансакцій (грошових переказів та платежів) від третіх осіб на користь осіб до яких застосовано санкції, у разі обміну, сплати штрафних санкцій у національній чи іноземній валюті, припинення зобов'язання відступним, припинення зобов'язання заліком зустрічних однорідних вимог, припинення зобов'язань збігом боржника і кредитора, якщо ВА, що були або є предметом правочину, в історії трансакцій блокчейну містять запис щодо належності особам, до котрих застосовано санкції.

Тісна співпраця з наглядовими та правоохоронними органами, повідомлення про будь-які підозрілі дії та операції, що здійснюються постачальниками послуг, пов'язаних з оборотом ВА, та фінансових послуг, які працюють в Україні та за її межами, є потужним інструментом зупинення російської агресії. Витрати, пов'язані з підвищеною обачністю, є однією з форм підтримки України і безпеки в Європі та США.

Водночас моніторинг трансакцій (грошових переказів та платежів) щодо віртуальних активів не повинен призводити до суцільного блокування таких трансакцій. В Україні криптокошти використовувалися для підтримки різноманітних бойових дій – від закупівлі бронежилетів і шоломів до обладнання для розмінування та безпілотників. Інші криптодонати йшли на медичне та радіообладнання. Найбільші українські фонди підтримки армії «Повернись живим» та «Сергія Притули» отримали у криптовалюті мільйони доларів США, передусім у перші дні вторгнення. Децентралізований характер криптовалют робить їх швидким і зручним засобом для переміщення грошей у зони конфліктів та катастроф. Війна росії проти України стала однією з найкраще задокументованих воєнних кампаній в історії та першою великою кібервійною між двома країнами з помітною складовою в ній використання криптовалют.

Боротьба з ухиленням від санкцій через використання віртуальних активів є невід'ємною складовою ризик-орієнтованого підходу до регулювання обороту цифрових активів у сфері ПВК/ФТ. Цей зв'язок реалізується шляхом систематичної оцінки та управління ризиками, які виникають через специфічні технологічні властивості віртуальних активів, такі як псевдонімність, децентралізація та транскордонний характер операцій.

Ризик-орієнтований підхід передбачає застосування диференційованих заходів регулювання та контролю, залежно від рівня ризиків, пов'язаних з конкретними типами операцій, послугами, продуктами чи юрисдикціями. У цьому контексті санкційні ризики можуть бути оцінені на основі критеріїв, таких як використання децентралізованих бірж, міксерів, анонімних криптовалют, а також обслуговування транзакцій із регіонами, що перебувають під санкціями.

Для ефективного управління такими ризиками необхідне впровадження відповідних інструментів моніторингу і контролю, зокрема технологій блокчейн-аналітики для ідентифікації й аналізу підозрілих транзакцій, пов'язаних з

обходом санкцій та застосування системи «червоних прапорців», що сигналізують про підозрілі або ризикові трансакції. Розробка моделей прогнозування санкційних ризиків на основі баєсових мереж, регресійного аналізу та гравітаційного моделювання дозволять оцінити ймовірності та наслідки ухилення від санкцій. Імплементація заходів фінансового контролю, таких як підвищені вимоги до належної перевірки клієнтів (ЗСК), моніторинг високоризикових географічних зон, та обов'язковий обмін інформацією відповідно до міжнародних стандартів, наприклад, «Правило подорожі» сприятиме модернізації протидії уникнення санкцій [434].

Поєднання цих елементів в рамках РОП забезпечує комплексний контроль обороту цифрових активів, дозволяючи ефективніше попереджати та припиняти спроби ухилення від міжнародних санкцій, що позитивно впливає на глобальну фінансову безпеку та стабільність фінансових систем.

Висновки до розділу 3.

1. В підрозділі 3.1. автором наголошено на необхідність в найкоротші строки легалізувати український крипторинок шляхом розроблення комплексного законодавства, відповідного європейським стандартам, із встановленням вимог до операторів і сервісів криптоіндустрії щодо ліцензування, звітності, безпеки та оподаткування, а також із забезпеченням постійного моніторингу ринку і впровадженням ризик-орієнтованого підходу до управління ризиками. Надані пропозиції з регулювання крипторинку щодо залученню як внутрішніх, так і іноземних інвестицій, стимулювання економічне зростання, розвитку інноваційних технологій, забезпечення захисту прав

споживачів і підвищення безпеки фінансових операцій, що сприятиме загальному економічному розвитку країни.

Автором проаналізовані ризики затримки легалізації, що вказують на можливе зниження рейтингу України в 6-му раунді взаємних оцінок MONEYVAL щодо впровадження 15-ї Рекомендацій FATF (категорія «не впроваджено»). Це може ускладнити доступ до міжнародних фінансових ринків, обмежити можливості українських підприємств у залученні інвестицій та веденні бізнесу з іноземними партнерами, а також спричинити скорочення обсягів міжнародної торгівлі через побоювання партнерів щодо недотримання міжнародних стандартів протидії ВК/ФТ. Для банківського сектору особливо критичним є ризик потрапляння до списку країн з підвищеним моніторингом, що може призвести до припинення операцій за кореспондентськими рахунками з іноземними фінансовими установами та вплинути на стабільність фінансової системи.

2. Розвиток пілотного проєкту е-гривні є необхідним кроком модернізації фінансової системи України в контексті глобальних тенденцій упровадження CBDC. Запровадження е-гривні сприятиме підвищенню ефективності внутрішніх та міжнародних платежів, забезпеченню прозорості операцій і зниженню корупційних ризиків. У дисертації наголошено, що повноцінна реалізація е-гривня має відповідати вимогам ПВК/ФТ – зокрема, необхідно впровадити ліміти на баланс електронних гаманців та обсяги транзакцій згідно з міжнародними стандартами ПВК/ФТ. Це фактично означає застосування ризик-орієнтованого підходу: невеликі суми можуть використовуватися анонімно або напіванонімно, тоді як для здійснення більших платежів користувачі повинні пройти ретельнішу перевірку та ідентифікацію.

Український підхід враховує потенційні ризики зловживань. Проте існують виклики, пов'язані з конфіденційністю платежів, кібербезпекою та забезпеченням операційної стійкості фінансових установ. Наявність неповного законодавчого регулювання цифрових валют уповільнює практичну реалізацію

проєкту, тому запуск пілотного проєкту є критичним для тестування різних сценаріїв використання та вдосконалення технологічних і правових аспектів перед масштабним упровадженням. В дисертації запропоновано використовувати е-гривню для підвищення прозорості операцій з ВА, що дасть змогу оптимізувати витрати на впровадження процедур комплаєнсу та ПВК/ФТ, що є впровадженням РОП. При цьому важливим є забезпечення спроможності НБУ гарантувати захист персональних даних та стабільність роботи фінансових установ. Співпраця з міжнародними фінансовими організаціями, що мають досвід запуску CBDC, сприятиме зміцненню фінансової стабільності, покращанню доступу до цифрових платежів та інтеграції України у світову фінансову систему.

3. Міжкраїновий регресійний аналіз (індекс сприйняття корупції) із застосуванням підходу від загального до конкретного свідчить, що активніше використання ВА емпірично пов'язане із вищим рівнем корупції та жорсткішим контролем капіталу. Дослідження підкреслює необхідність подальшого удосконалення збору та аналізу даних для більш глибокого розуміння мотивів використання криптовалют.

На основі комплексного аналізу корупційних схем, пов'язаних із використанням криптовалютних операцій для приховування джерел походження активів, сформульовано авторські пропозиції, спрямовані на мінімізацію ризиків декларування цифрових активів як інструменту ВК/ФТ. Визначено, що декларування криптовалют у системі публічного контролю може використовуватися з метою створення видимості легальності походження майна, що особливо актуально у висококорупційних юрисдикціях.

Розроблені автором рекомендації враховують специфіку цифрових активів як високоволатильних і транскордонних інструментів, що ускладнюють їх перевірку й верифікацію. Запропоновано удосконалити механізми контролю за достовірністю декларування шляхом інтеграції ризик-орієнтованого підходу до перевірки джерел походження криптоактивів, а також залучення

автоматизованих засобів блокчейн-аналітики. Це сприятиме підвищенню ефективності державного нагляду, зменшенню корупційних зловживань і забезпеченню прозорості у сфері обігу цифрових активів.

4. У межах дослідження сформульовано авторську концепцію протидії ухиленню від санкцій у сфері обігу ВА шляхом інтеграції РОП до державного та міждержавного регулювання крипторинку. Автором наголошено, що однією з ключових складових цієї стратегії виступає посилення контролю за майнінгом криптовалют у підсанкційних країнах, таких як росія та білорусь, у тому числі через заборону експорту відповідного обладнання. Майнінг, як інструмент перетворення енергетичних ресурсів у фінансові активи, може використовуватись для фінансування злочинних та санкційних режимів, що вимагає його включення до переліку критично контрольованих напрямів.

Серед пріоритетних напрямів також автором визначено запровадження обов'язкового міжнародного ліцензування всіх суб'єктів криптоекосистеми – зокрема, централізованих бірж, P2P-платформ та постачальників послуг з віртуальними активами. Особливу увагу приділено розвитку багатосторонньої координації між юрисдикціями (США, ЄС, Велика Британія), у тому числі в частині обміну інформацією між підрозділами фінансової розвідки, а також застосування вторинних санкцій до компаній-посередників.

На думку автора, запровадження системного моніторингу ризиків та РОП у межах національної системи ПВК/ФТ забезпечить ефективніше виявлення підозрілих криптоопераций, зменшення втрат державного бюджету від злочинної діяльності, а також підвищення спроможності України до протистояння російській агресії. Водночас, за умови правової реалізації, арештовані ВА можуть стати джерелом компенсацій за міжнародну фінансову підтримку, що відкриває нові підходи до економічної відповідальності агресора.

Основні наукові результати розділу опубліковані в працях автора [36; 50; 176; 254; 258; 264; 347; 434].

РОЗДІЛ 4
НАПРЯМИ УДОСКОНАЛЕННЯ ВПРОВАДЖЕННЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В ДІЯЛЬНІСТЬ РИНКУ ВІРТУАЛЬНИХ АКТИВІВ У СФЕРІ ПВК/ФТ

4.1. Фіскально-правові та обліково-звітні аспекти національного регулювання операцій з віртуальними активами відповідно до європейських стандартів: оподаткування, майнінг та бартерні операції

Незважаючи на широкий спектр цифрових фінансових активів, одну з ключових ролей серед них відіграють ВА, що можуть виступати як засіб платежу, а також заощадження й об'єкт інвестування.

З функціональної точки зору ВА – це цифровий вираз вартості, яка може купуватися та продаватися в цифровій формі й функціонувати як засіб обміну, облікова одиниця і/або засіб збереження вартості, але не має законного статусу в будь-якій юрисдикції (тобто не є законним засобом платежу в більшості розвинутих країн і країн, що розвиваються).

З інституційної точки зору ВА можна інтерпретувати як цифровий вираз вартості, при цьому вона випускається нетрадиційними емітентами сучасних форм грошей – банками, кредитними інститутами або спеціалізованими емітентами електронних грошей. Разом із тим віртуальні активи можуть обмежено використовуватись як альтернатива загальновизнаним формам грошей при розрахунках в електронних мережах.

Зростання інтересу до питань розвитку обігу віртуальних валют спостерігається, починаючи з 2015 р. Він продиктований платіжним та інвестиційним потенціалом віртуальних валют як нового цифрового фінансового активу. Протягом 2016–2017 рр. біржові курси віртуальних валют неухильно

підвищувалися. 7 січня 2018 року було відзначено рекордний обсяг капіталізації ринку криптовалют, що становив 813,87 млрд дол. США [262]. Проте проблеми зі швидкістю трансакцій і зростаючі витрати на майнінг зумовили різке падіння курсу основних криптовалют у 2018р., а наприкінці 2020 року відбулося відновлення: у листопаді 2020 року капіталізація біткоїна досягла 342 млрд дол. США при ціні близько 18 500 дол. США за монету [430].

Глибока корекція ринку віртуальних валют, у результаті якої загальна капіталізація криптовалюти із січня по грудень 2018 р. скоротилася на 80 %, була пов'язана з двома факторами – прогалинами в регулюванні віртуальних валют і технологічним недосконалістю більшості рішень на ринку.

Корекція курсів провідних віртуальних валют в 2018р. також обумовлювалася стихійними діями регуляторів, що послабили спекулятивну активність на ринку операцій з віртуальними валютами. При цьому однією з найважливіших проблем, що перешкоджають широкому використанню віртуальних валют як платіжного й інвестиційного інструменту не тільки приватними особами та інвесторами, а й кредитними інститутами та інвестиційними фондами, є відсутність комплексної економіко-правової основи регулювання ВА. Тому своєчасність упровадження регуляторних механізмів, в тому числі і в податковій сфері, яка виступає найважливішим інструментом державного регулювання сфери ВА, надзвичайно актуальна. Інтерес до розвитку ВА з боку учасників фінансового ринку і наглядових органів залишається, як і раніше, високим.

Загалом із 2020 по 2025 р. ринок криптовалют зазнав значного зростання. У березні 2021 р. глобальна капіталізація крипторинку досягла 1,7 трлн дол. США, а ціна Bitcoin становила 54 500 дол. США за монету. Станом на 14 листопада 2024 р. капіталізація ринку зросла до 3,76 трлн дол. США, що на 1,9 % більше, ніж за попередні 24 години. У січні 2025 р. капіталізація стейблкоїнів перевищила 200 млрд дол. США, а до березня досягла 400 млрд дол. США. Ці дані свідчать про стійку тенденцію до зростання ринкової капіталізації

криптовалют, відображаючи їхню зростаючу економічну значущість у глобальній економіці [262]. Однак, як і на будь-якому фінансовому ринку, динаміка курсів криптовалют може бути від'ємною в окремі періоди, що є характерним для всіх життєздатних ринків.

Протягом періоду з 2020 по 2025 р. крипторинок пережив кілька «криптозим», тобто періодів значного падіння вартості криптовалют, що супроводжувалося зниженням капіталізації ринку. Після піка наприкінці 2017 р. ринок криптовалют пережив різке падіння в 2018 р., коли його капіталізація знизилася до менше ніж 100 млрд дол. США. Цю «криптозиму» супроводжувало істотне падіння вартості Bitcoin та інших криптовалют, що створило атмосферу скептицизму щодо цифрових активів. Після рекордного зростання капіталізації крипторинку в першій половині 2021 р. у червні того ж року ринок зазнав суттєвого коригування. Вартість Bitcoin знизилася з понад 60 000 до близько 30 000 дол. США, а ринкова капіталізація всього крипторинку скоротилась на 1 трлн дол. США [262].

Це було спричинено кількома факторами, включно з жорсткими заходами з боку уряду (особливо в Китаї), які запроваджували обмеження на майнінг криптовалют і різко збільшували регуляторний тиск. У 2022 р. ринок криптовалют знову пережив істотну корекцію через різке падіння вартості Bitcoin та інших активів, що було викликано такими факторами, як глобальна економічна невизначеність, підвищення процентних ставок у США та інші макроекономічні обставини. Наприкінці 2022 р. Bitcoin торгувався на рівні близько 16 000 дол. США, а загальна капіталізація ринку знизилася до рівня 2020р. Після важкого 2022 р. ринок почав стабілізуватися, але періодичні падіння продовжувалися, зокрема внаслідок банкрутства кількох криптовалютних платформ та великих компаній, таких як FTX, що створило додаткові труднощі. Хоча криптоактиви пережили кілька важких періодів, ринок виявив стійкість. У 2025 р. ринок ВА, ймовірно, перебуватиме на етапі відновлення, і, попри

можливі періодичні корекції, загальна тенденція до зростання капіталізації та впровадження криптовалютних технологій в економіку зберігається.

Розвиток ВА у зв'язку з їх децентралізацією, з одного боку, та складністю визначення державної належності опосередковуваних ними операцій, з другого боку, являє собою значний виклик у різних фінансових сферах, у тому числі в оподаткуванні. Особливості ВА створюють потенційну можливість використання їх для глобального ухилення від оподаткування [419]. У 2015–2018 рр. податкові органи різних країн здійснювали спроби оподаткування операцій, пов'язаних з віртуальними валютами, причому теоретичне обґрунтування подібних механізмів, як правило, прямувало за практикою (Додаток Д). Необхідність реалізації підходів до оподаткування криптоактивів у теорії та на практиці стало гострим питанням лише після необхідності впровадження міжнародних стандартів FATF і прийняття рішення про легалізацію ринку ВА на національному рівні.

Аналіз стихійно сформованих підходів до оподаткування операцій з ВА в різних країнах в умовах різних інтерпретацій і відсутності уніфікованого підходу до цього оподаткування як на національному, так і на міжнародному рівні викликав безперечний науково-дослідницький інтерес через не тільки введення таких активів у правове поле в рамках сучасної цифрової економіки, а й розроблення політики податкового регулювання ВА в Україні.

Дослідженням підходів до оподаткування ВА передують огляд і обґрунтування вибору їх податкового регулювання в Сінгапурі, США, Великій Британії, Японії та Німеччини узагальнення можливих трактувань цього фінансового активу і їхніх податкових наслідків після 2019 р. (Додаток Д).

Фіскальна політика щодо оподаткування криптоактивів у різних країнах визначається залежно від того, як на законодавчому рівні трактується поняття ВА. Наприклад, у США криптоактиви розглядаються як власність, у Великій Британії — як капітальний актив, а в Італії — як різновид іноземної валюти.

У багатьох країнах фізичні особи повинні сплачувати податок на приріст капіталу з прибутку, отриманого від операцій з ВА. Оподаткування застосовується до таких операцій:

- купівля криптоактивів: зазвичай придбання криптоактивів за фіатні гроші не оподатковується;
- продаж криптоактивів за готівку;
- обмін криптоактивів: коли один криптоактив обмінюється на інший;
- оплата товарів і послуг криптоактивами.

Крім того, фізичні особи зобов'язані сплачувати податок на доходи, якщо отримують винагороду у вигляді криптоактивів.

Для розрахунку суми податку ВА конвертуються в національну валюту за чинним обмінним курсом на момент здійснення операції.

Як зазначалося, у Європейському Союзі в рамках Стратегії цифрових фінансів для ЄС та імплементації Регламенту щодо ринків криптоактивів (MiCA) впроваджуються правила податкової прозорості (Директива ЄС DAC8), оновлена редакція яких поширюються на криптовалютні біржі. Відповідно до них емітенти криптоактивів та професійні оператори крипторинку повинні регулярно звітувати про трансакції, з яких користувачі мають сплачувати податки.

Європейська Директива DAC8 є останнім оновленням Директиви про адміністративну співпрацю у сфері оподаткування (EU Directive 2011/16/EU [435]). Її ухвалення 17 жовтня 2023 р. Європейською Радою знаменує значний крок у напрямі посилення податкової прозорості, особливо у сфері криптоактивів. Вона набрала чинності 13 листопада 2023 р.

Директива встановлює посилені заходи контролю за обігом криптоактивів та електронних грошей. За оцінками, її реалізація сприятиме залученню додаткових 2,4 млрд євро податкових надходжень до бюджету [435].

DAC8 поширюється на постачальників криптопослуг та операторів крипторинків, включно з брокерами, біржами, адміністраторами активів,

операторами криптовалютних банкоматів та гаманців. Вони повинні реєструватися в одній із країн ЄС і подавати щорічну звітність. Вимога також поширюється на компанії за межами ЄС, якщо вони обслуговують клієнтів, що проживають у Євросоюзі.

Звітність охоплює:

- інформацію про оператора (назва, адреса, податковий номер);
- дані клієнтів з ЄС (ім'я, адреса, держава проживання, ІПН);
- інформацію про криптоактиви (назва, ринкова вартість, суми та кількість операцій).

Під регуляцію підпадають як внутрішні, так і транскордонні трансакції, включно з обміном і передачею криптоактивів. Усі оператори повинні забезпечити комплексну перевірку своїх клієнтів, щоб визначити, чи підлягають вони звітності. Хоча передбачено мінімізацію адміністративного навантаження, впровадження нових вимог потребуватиме істотних витрат, а саме близько 300 млн. євро на адаптацію систем і 25 млн євро на їх підтримку [436].

Директива DAC8 інтегрується з Регламентом щодо регулювання ринків криптоактивів (MiCA), який встановлює додаткові вимоги до авторизації постачальників криптопослуг. Це дає змогу краще узгодити податкові вимоги з нормами регулювання ринку.

Наразі упроваджено автоматичний обмін інформацією про клієнтів між податковими органами країн ЄС. Використовуватиметься єдина комунікаційна мережа на основі XML-схем, які розробляються Єврокомісією.

Також оновлена Директива DAC8 враховує стандарти криптозвітності, розроблені OECP (CARF) [437], що впроваджуються у 48 юрисдикціях з 2027 р., а саме:

- впровадження нових інструментів автоматичної перевірки податкових номерів (TIN);
- можливість використання зібраної інформації для антилегалізаційних і антикорупційних цілей;

- мінімальний термін зберігання даних — п’ять років.

Це сприятиме глобальній прозорості у сфері оподаткування криптоактивів. До сфери дії DAC8 належать криптоактиви, що випускаються децентралізовано, стейблкоїни (зокрема токени цифрових грошей, англ. e-money tokens), NFT, цифрові валюти та цифрові гроші центробанків.

Директива DAC8 є важливим кроком у посиленні податкової дисципліни в ЄС, особливо у цифровій сфері. Хоча впровадження вимог потребує значних витрат для операторів, їхня реалізація сприятиме прозорості, запобіганню ухиленню від податків та гармонізації стандартів у ЄС та на міжнародному рівні.

На сьогодні більшість європейських країн вже запровадили податки на операції з криптоактивами, однак умови оподаткування можуть суттєво відрізнятися залежно від держави.

Стосовно оподаткування віртуальних активів, то в Україні розмірковують про можливість використання зарубіжного досвіду оподаткування операцій з ВА за наявності нещодавніх новацій у Цивільному кодексі України (ЦКУ). Треба зазначити, що подібного терміна в зарубіжному законодавстві немає, тому навіть після прийняття змін до ЦКУ продовжуються дискусії правників-цивілістів про виникнення нових правовідносин.

Щодо європейського законодавства, то Директивою (ЄС) 2019/770 Європейського парламенту та Ради від 20.05.2019 про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг [438] введено визначення цифрового контенту та цифрових послуг, але поняття віртуальних (цифрових) активів немає.

Об'єкти цивільних прав можуть існувати як у матеріальному світі, так і в цифровому середовищі. Це визначає форму таких об'єктів, а також специфіку набуття, здійснення та припинення цивільних прав і обов'язків щодо них. Чи є такі правовідносини унікальними? Відповідно до нової статті 179-1 Цивільного кодексу України цифровою річчю визнається благо, яке створюється та існує виключно в цифровому середовищі й має майнову цінність [438]. До цифрових

речей віднесено ВА, цифровий контент та інші блага, зазначені у частині першій цієї статті. Правовий режим цифрових речей встановлюється законом. Якщо інше не передбачено ЦКУ, законом або не випливає із сутності цифрової речі, до неї застосовуються положення ЦКУ, що регулюють речові права.

Встановлено, що поняття ВА, яке є складовою цифрової речі, настільки широке, що охоплює відомі об'єкти цивільного права, зокрема послуги, майнові права, інформацію, результати інтелектуальної та творчої діяльності, оборотоздатні об'єкти особистих немайнових правовідносин тощо. Головною особливістю ВА є те, що вони утворюються й функціонують за допомогою цифрових технологій та інтернет-ресурсів.

Якщо звернути увагу на запропоноване поняття цифрової речі та її склад, може здатися, що це благо є унікальним і новим для цивільного права. Проте детальний аналіз цього поняття дає змогу дійти висновку, що об'єкт, який пропонується визначати як цифрову річ, не є абсолютно новим для цивільного права [438].

Відповідно до Закону України «Про віртуальні активи», «віртуальний актив — це нематеріальне благо, яке має вартість і виражається у вигляді даних в електронній формі» [429]. Це визначення настільки широке, що охоплює вже відомі об'єкти цивільних прав, такі як послуги, майнові права, інформація, результати інтелектуальної чи творчої діяльності, а також оборотоздатні об'єкти немайнових правовідносин. Усі вони є нематеріальними благами, які мають майнову цінність і можуть бути оцінені в грошовому еквіваленті.

Особливістю ВА є те, що вони створюються і використовуються за допомогою інтернет-технологій, телекомунікацій або інтернет-ресурсів. Однак такі об'єкти, як послуги чи результати творчої діяльності, теж можуть бути виражені через сукупність електронних даних, наприклад, інформацію про послугу чи її майнову вартість.

В юридичній літературі зазначено, що поняття «віртуальні активи» може охоплювати й бездокументарні цінні папери або електронні гроші, які існують

виключно в цифровій чи безготівковій формі. Такі об’єкти, як бездокументарні цінні папери чи безготівкові гроші, давно відомі цивільному праву, а їхня цифрова форма не створює суттєвих новацій.

Таким чином, ВА як складова цифрових речей охоплюють не нові, а вже давно відомі об’єкти цивільного права, що отримують додаткову назву, а не замінюють наявні терміни. При цьому термін «актив» має економічне походження й використовується у бухгалтерському обліку, тоді як у цивільному праві існують чіткі поняття «майно», «речі» та «майнові права». Отже, запровадження терміна «актив» у цивільне право здається зайвим з огляду на вже усталені спеціальні терміни [439].

Оскільки цифрова річ має майнову цінність за Цивільним кодексом України, процитуємо відповідну ст. 139 ЦКУ: «Майном у цьому Кодексі визнається сукупність речей та інших цінностей (включаючи нематеріальні активи), які мають вартісне визначення, виробляються чи використовуються у діяльності суб'єктів господарювання та відображаються в їх балансі або враховуються в інших передбачених законом формах обліку майна цих суб'єктів» [438]. Варто розглянути віднесення криптоактивів до нематеріальних активів для бухгалтерського та податкового обліку.

Поняття нематеріального активу визначено у Положенні (стандарті) бухгалтерського обліку 8 «Нематеріальні активи» (далі – П(С)БО8): «Нематеріальний актив – немонетарний актив, який не має матеріальної форми та може бути ідентифікований» [441].

Тобто, щоб вважатися немонетарним активом, криптовалюти повинні відповідати таким ознакам:

- бути немонетарним активом;
- не мати матеріальної форми;
- можуть бути ідентифіковані.

Згідно з Національним положенням (стандартом) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності» (далі – П(С)БО 1), активи – це

ресурси, контрольовані підприємством внаслідок минулих подій, використання яких, як очікується, забезпечить економічні вигоди в майбутньому. Таким чином, криптовалюти відповідають визначенню активів.

За П(С)БО 8, немонетарними активами є всі активи, крім грошових коштів, їх еквівалентів та дебіторської заборгованості у фіксованій сумі. Оскільки криптовалюти не є грошовими коштами чи їх еквівалентами (через значні коливання вартості), вони підпадають під категорію немонетарних активів. Відповідно до МСБО 7, «еквіваленти грошових коштів – це короткострокові, високоліквідні інвестиції, які вільно конвертуються у відомі суми грошових коштів і яким притаманний незначний ризик зміни вартості» [442]. Таким чином, за МСБО 7 криптоактиви теж відповідають критеріям немонетарного активу.

Оскільки криптоактиви існують у формі записів у реєстрах, вони не мають матеріальної форми. Можливість ідентифікації відповідно до МСБО 38 має такі ознаки: «актив є ідентифікованим, якщо він: а) може бути відокремлений, тобто його можна відокремити або відділити від суб'єкта господарювання і продати, передати, ліцензувати, здати в оренду або обміняти індивідуально або разом з пов'язаним з ним контрактом, ідентифікованим активом чи зобов'язанням, незалежно від того, чи має суб'єкт господарювання намір зробити це, або б) виникає внаслідок договірних або інших юридичних прав, незалежно від того, чи можуть вони бути передані або відокремлені від суб'єкта господарювання або ж від інших прав та зобов'язань» [443].

ВА відповідають критеріям, визначеним для ідентифікованих активів. Зазначимо, що облік нематеріальних активів у бухгалтерії здійснюється за такими групами: права користування природними ресурсами, права користування майном, права на комерційні позначення, права на об’єкти промислової власності, авторське право та суміжні права, а також інші нематеріальні активи. Для цілей бухгалтерського обліку доцільно відносити ВА до категорії «інші нематеріальні активи».

Отже, згідно з господарським законодавством ВА класифікуються як нематеріальні активи, а відповідно, є майном. При цьому для бухгалтерського обліку вони належать до групи «інші нематеріальні активи».

У межах податкового законодавства класифікація ВА зазвичай здійснюється з урахуванням їх віднесення до категорій коштів, інвестиційних активів або товарів.

Відповідно до пп. 14.1.93 та п. 14.1 ст. 14 ПКУ «кошти – гривня або іноземна валюта» [444]. Вище ми детально описали, чому ВА не можуть бути віднесені до коштів.

Згідно з пп. а) пп. 170.2.7 п 170.2 ст. 170 ПКУ інвестиційний актив – «пакет цінних паперів, деривативів чи корпоративні права, виражені в інших, ніж цінні папери, формах, випущені одним емітентом» [444]. У своєму первісному вигляді ВА не відповідають наведеному визначенню, а отже, не можуть бути класифіковані як інвестиційні активи. Водночас у межах ICO вони здатні набувати нових характеристик, що буде детальніше розглянуто далі.

Відповідно до пп. 14.1.244 п. 14.1 ст. 14 ПКУ «товари – матеріальні та нематеріальні активи, у тому числі земельні ділянки, земельні частки (паї), а також цінні папери та деривативи, що використовуються у будь-яких операціях, крім операцій з їх випуску (емісії) та погашення» [444]. Як зазначено раніше, ВА класифікуються як нематеріальні активи. Таким чином, для податкового законодавства криптовалюти розглядаються як товари.

Як бачимо, відповідно до цивільного та господарського законодавства ВА визнаються майном, а для податкового законодавства – товарами (нематеріальними активами). На криптоактиви поширюється право власності, вони можуть бути вільно відчужені або передані від однієї особи до іншої.

Для визначення діяльності, пов'язаної з ВА, необхідно встановити, до якої категорії належать ВА згідно з Національним класифікатором України (КВЕД).

Відповідно до Національного класифікатора України:

1) «Товари – це матеріальні об'єкти, на які є попит та щодо яких можна встановити права власності» [445];

2) «Послуги – це результат економічної діяльності, відносно якого не можна встановити права власності» [445].

Як зазначалося, ВА є об’єктами права власності, тому їх не можна класифікувати як послуги. Водночас їх віднесенню до категорії товарів перешкоджає визначення як нематеріальних об'єктів.

Разом із тим, згідно з Методологічними основами та поясненнями до позицій Класифікації видів економічної діяльності, затвердженими наказом Державного комітету статистики України від 23.12.2011 № 396 (далі – Наказ № 396), в описі КВЕД 47.91 «Роздрібна торгівля, що здійснюється фірмами поштового замовлення або через мережу Інтернет» зазначено, що «товар, який купується, може бути або безпосередньо завантажений з інтернет-сайту, або доставлений покупцеві» [445].

Наказ № 396 допускає можливість завантаження товару з інтернет-сайту, що свідчить про те, що товар може мати нематеріальну природу. Таким чином, виявляється розбіжність між визначенням поняття товару та його описом (правова колізія) [440]. Урахування можливості завантаження товару через інтернет дає змогу віднести нематеріальні об'єкти до категорії товарів. З огляду на це ВА можуть вважатися товарами для цілей КВЕД.

На думку експертів, блокчейн застосовуватиметься в найрізноманітніших сферах, таких як грошові перекази, мікроплатежі, розумні контракти (або смарт-контракти), ідентифікація фізичних об’єктів і активів, державне управління, оборона і безпека, міжнародна діяльність тощо. У цілому передбачається, що в майбутньому технології блокчейн можуть стати драйвером радикальних змін у широкому спектрі галузей, бізнес-моделей, соціальних і операційних процесів. Тестування та впровадження технологій блокчейн розпочали в низці країн і у багатьох великих корпораціях [440, с. 75].

Відповідно до чинного законодавства України ВА класифікуються як майно згідно з цивільним законодавством, а як товар (нематеріальний актив) – згідно з податковим. На криптоактиви може виникати право власності, що дозволяє їх вільне відчуження або передачу від однієї особи до іншої.

При створенні ВА в особи автоматично виникає право власності на них. Це стосується також інших бізнес-процесів, пов'язаних із набуттям права власності на ВА, таких як майнінг, купівля-продаж або бартер. Відповідно, виникає питання про необхідність відображення таких активів у балансі.

За Законом України «Про запобігання корупції» суб'єкти декларування (державні службовці, посадові особи місцевого самоврядування та ін.) зобов'язані подавати декларацію, в якій, відповідно до ст. 46, мають зазначатися відомості про нематеріальні активи [40]. У декларації слід вказати вид, характеристики таких активів, їхню вартість на момент виникнення права власності та дату набуття права.

Як зазначалося, ВА відповідають визначенню нематеріальних активів згідно зі стандартами бухгалтерського обліку.

Закон України «Про запобігання корупції» хоч і не дає окремого визначення терміна «нематеріальний актив», проте з 2019 р. ВА включено до переліку активів, які підлягають декларуванню, аналогічно до інших антикорупційних законодавчих актів. Отже, суб'єкти декларування зобов'язані вказувати у своїх деклараціях наявні ВА.

Відповідно до п. 7 П(С)БО 8, нематеріальний актив, створений у результаті розроблення, підлягає відображенню у балансі за умови, що підприємство:

- має намір, технічну можливість і ресурси для приведення нематеріального активу до стану, придатного для реалізації або використання;
- може отримати майбутні економічні вигоди від його реалізації чи використання;
- має достовірну інформацію для визначення витрат, пов'язаних із його розробкою [446].

Таким чином, обов’язок відображення в балансі створених («емітованих») підприємством ВА виникає лише за умови одночасного виконання всіх трьох критеріїв.

Окремо слід розглянути правила обліку придбаних або отриманих ВА (на відміну від тих, що були створені власноруч). Згідно з п. 7 П(С)БО 8, нематеріальний актив (зокрема, криптоактив) відображається в балансі, якщо:

- існує ймовірність отримання майбутніх економічних вигід від його використання;
- його вартість може бути достовірно визначена [443].

Отже, ВА, отримані шляхом придбання чи іншого способу (крім власного видобування), підлягають відображенню в балансі, якщо відповідають наведеним двом умовам. Таким чином, в обліку і звітності суб’єктів господарювання щодо ВА застосовуються вимоги, встановлені для нематеріальних активів.

Відносини, що виникають на ринку ВА за участі суб’єктів господарювання, відповідають визначенню електронної комерції згідно із Законом України «Про електронну комерцію» (далі – Закон про електронну комерцію) [447]. Продаж криптоактивів суб’єктами господарювання вважається електронною торгівлею, яка регулюється цим Законом. В Україні сотні фізичних осіб задекларували свої ВА відповідно до встановлених вимог.

Згідно з п. 2 ч. 1 ст. 3 Закону про електронну комерцію, електронна торгівля визначається як господарська діяльність у сфері дистанційного продажу товарів шляхом укладання електронних правочинів із використанням інформаційно-телекомунікаційних систем.

Стаття 7 цього Закону встановлює перелік інформації, яку продавець товарів чи постачальник послуг у сфері електронної комерції зобов’язаний надавати:

- повне найменування юридичної особи або прізвище, ім’я, по батькові фізичної особи – підприємця;

- місцезнаходження юридичної особи або місце реєстрації й проживання фізичної особи – підприємця;
- адресу електронної пошти;
- ідентифікаційний код юридичної особи або реєстраційний номер платника податків для фізичної особи - підприємця тощо.

Ці вимоги поширюються також на криптовалютні біржі, обмінні пункти та інших учасників ринку ВА.

Права та обов'язки споживачів у сфері електронної комерції регулюються Законом України «Про захист прав споживачів», як визначено у ст. 8 Закону про електронну комерцію [448]. Одне з ключових питань для ринку ВА стосується права споживача на обмін товару належної якості або розірвання договору купівлі-продажу. У разі розірвання договору розрахунок із покупцем проводиться, виходячи з вартості товару на момент його придбання.

На волатильному ринку криптоактивів така можливість може створити ситуацію, коли покупці отримають односторонню перевагу, а господарська діяльність продавців стане неможливою. Однак постанова Кабінету Міністрів України від 19.03.1994 № 172, яка затверджує перелік товарів, що не підлягають обміну (поверненню), не містить згадки про ВА.

Відповідно до ч. 5 ст. 13 Закону України «Про захист прав споживачів», споживач не має права розірвати договір, укладений на відстані, якщо:

1) послугу або товар було поставлено електронними засобами зв'язку за згодою споживача до закінчення строку розірвання договору, про що споживача повідомлено;

2) ціна товару чи послуги залежить від котирувань на фінансовому ринку, що перебувають поза контролем продавця [448].

Оскільки ВА постачаються миттєво та електронними засобами зв'язку, споживач не може вимагати розірвання договору купівлі ВА. Більше того, ціна ВА визначається відкритим ринком, і такий підхід не завжди відповідає ситуації на фінансовому ринку в прямому розумінні, тому продавець не контролює ціну.

Це питання підкреслює важливість імплементації європейського Регламенту MiCA в національне законодавство. Однією з ключових цілей цього документа є захист прав споживачів та інвесторів, а також запобігання шахрайству на ринку ВА.

ВА можуть бути отримані особою як через перехід права власності від іншої особи, так і шляхом майнінгу. Загалом можна виокремити три основні типи бізнес-процесів, що приводять до набуття ВА (рис. 4.1): майнінг (видобуток); купівля-продаж (обмін на гроші); бартер (обмін на товари або послуги).

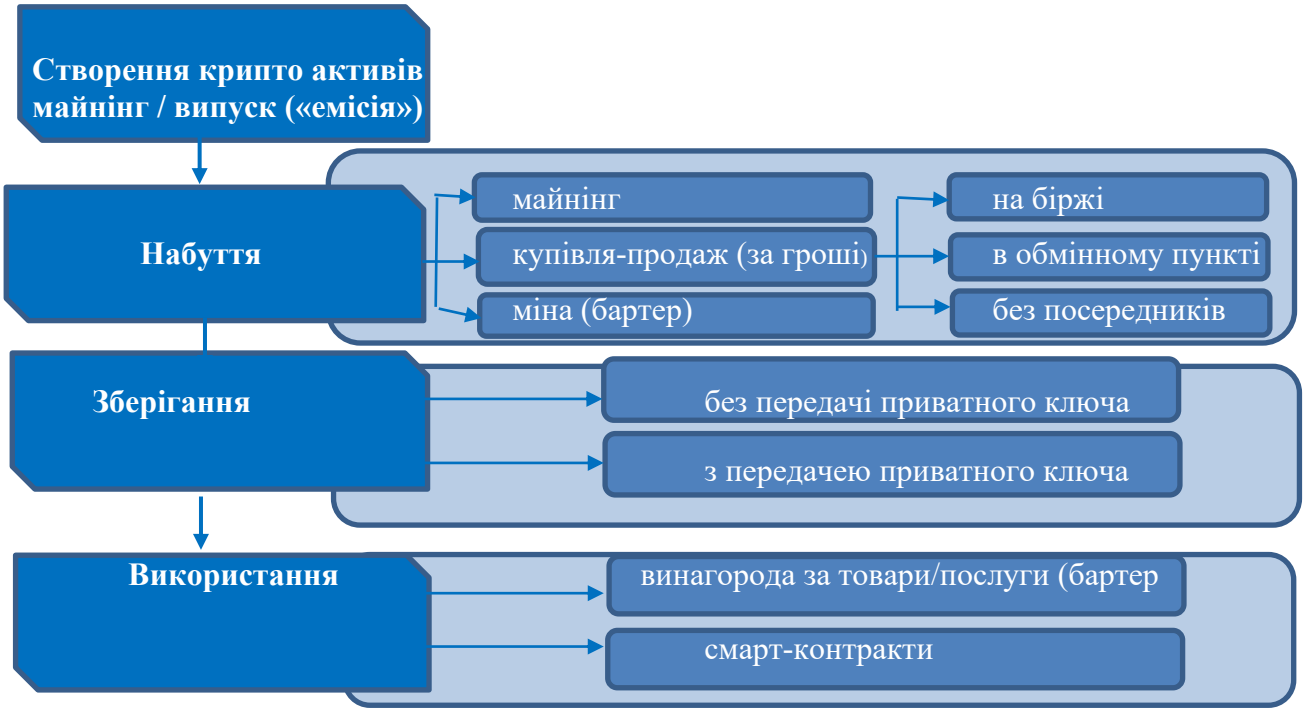


Рис. 4.1. Визначення етапів діяльності суб'єктів господарювання на ринку криптовалют

Джерело: побудовано автором за матеріалами [449]

Далі ми опишемо правове регулювання щодо зазначених бізнес-процесів та окремо розглянемо питання оподаткування операцій з криптоактивами, оскільки воно є одним із найважливіших та найбільш дискусійних.

Поняття «майнінг» в українському законодавстві не визначене. Утім, в українській Вікіпедії наведено таке визначення: «Майнінг, або видобування (від англ. mining — видобуток корисних копалин), — це діяльність із підтримки

розподіленої платформи та створення нових блоків із можливістю отримання винагороди у формі емітованої валюти та комісійних зборів у різних криптовалютах, зокрема біткоїнах» [450].

У рамках цього дослідження детальний опис процесу майнінгу не наводиться, адже важливо зрозуміти його зміст лише з точки зору правової класифікації відносин та економічної сутності бізнес-процесів. Суть майнінгу полягає в тому, що особа використовує своє обладнання для виконання обчислень у межах блокчейн-реєстру, за що отримує криптовалюту.

Під час майнінгу особа отримує винагороду двох типів: від емісії криптовалюти та у вигляді комісійних зборів. Водночас отримання «комісійних зборів» не передбачає жодних переговорів чи договірних відносин із користувачем, чия трансакція обробляється. Усі відносини регулюються автоматично через систему, виключно з будь-яким прямим контактом між сторонами (майнером і стороною трансакції).

Отже, отримання криптовалюти внаслідок майнінгу не можна вважати оплатою за надані послуги. Майнінг доцільно розглядати як окремий вид діяльності — обробку даних у блокчейн-реєстрі, результатом якої є видобуток криптовалюти. Водночас у чинній КВЕД майнінг як окремий вид діяльності не передбачено.

На нашу думку, в рамках чинної класифікації майнінг відповідає класу 63.11 «Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність». Цей клас включає «надання інфраструктури для розміщення (хостингу), оброблення даних і пов'язану із цим діяльність» та «оброблення даних: повне оброблення даних, отриманих від клієнта складання спеціалізованих звітів на основі даних, отриманих від клієнта» [445].

Чинне законодавство не передбачає спеціальної дозвільної системи щодо майнінгу криптовалют. Разом із тим відповідно до постанови Кабінету Міністрів України від 28.07. 2021 № 821 (далі – Постанова № 821) ліцензуванню підлягають такі послуги: «технічне обслуговування (супроводження)...

криптосистем і засобів криптографічного захисту інформації» [451]. Тобто, якщо майнінг стосується технічного обслуговування (супроводження) криптосистем і засобів криптографічного захисту інформації, то надання послуг з майнінгу є ліцензованим видом діяльності.

Відповідно до п. 2 Постанови № 821, «технічне обслуговування (супроводження) криптосистем і засобів криптографічного захисту інформації – операція або комплекс операцій з підтримання криптосистем і засобів криптографічного захисту інформації у справному і придатному для експлуатації стані під час їх використання за призначенням відповідно до вимог експлуатаційної документації розробника (виробника) щодо криптосистем і засобів криптографічного захисту інформації та нормативної документації щодо криптосистем і засобів криптографічного захисту інформації» [451].

Як зазначалося, криптоактиви самі по собі не є засобом захисту інформації. Однак вони можуть вважатися засобом захисту інформації, якщо застосовуються для перетворень інформації з використанням спеціальних даних (ключових даних) із метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Майнінг криптовалют, на наш погляд, може розглядатись як діяльність, спрямована на підтримання засобів криптографічного захисту інформації.

Водночас питання, чи відповідає майнінг вимогам експлуатаційної документації розробника криптовалюти, чи можна ідентифікувати такого розробника, а також наявність нормативної документації щодо криптовалюти потребують детального розгляду в кожному конкретному випадку.

На сьогодні немає інформації про застосування положень Постанови № 821 до майнінгу. Однак це питання є важливим для ринку криптовалют і потребує чіткого правового врегулювання [451].

Слід також зазначити, що ліцензуванню підлягає саме діяльність із надання послуг. У випадку майнінгу відсутні договірні відносини між замовником і виконавцем, а отже, фактично немає надання послуг у звичайному розумінні.

Отже, на нашу думку, майнінг не є ліцензованим видом діяльності. Водночас це питання потребує офіційного роз'яснення Державної служби спеціального зв'язку та захисту інформації України.

Як описано вище, ВА можуть вільно відчужуватися або переходити від однієї особи до іншої. Відповідно до ст. 655 ЦКУ, «за договором купівлі-продажу одна сторона (продавець) передає або зобов'язується передати майно (товар) у власність другій стороні (покупцеві), а покупець приймає або зобов'язується прийняти майно (товар) і сплатити за нього певну грошову суму» [452].

Українське законодавство не встановлює спеціальних обмежень чи вимог щодо відчуження ВА. Тому при здійсненні операцій купівлі-продажу необхідно дотримуватись загальних положень законодавства, зважаючи на правову природу ВА:

- цивільне законодавство класифікує ВА як майно;
- господарське законодавство розглядає їх як майно (нематеріальний актив);
- податкове законодавство визначає ВА як товар (нематеріальний актив).

Як зазначалося, ВА можуть бути класифіковані як товар згідно з КВЕД. Діяльність із їхнього продажу, відповідно, є торгівлею (Розділ 47 КВЕД). Пропонується віднести діяльність із продажу ВА через інтернет до категорії КВЕД 47.91 «Роздрібна торгівля, що здійснюється фірмами поштового замовлення або через мережу Інтернет». Цей клас охоплює роздрібну торгівлю будь-якими товарами через інтернет, що узгоджується з природою операцій із ВА [445].

Договір міни (бартер) відіграє важливу роль у сфері криптоактивів, оскільки обмін одних криптоактивів на інші вважається договором міни (бартеру) та «купівля» товарів чи послуг за криптоактиви теж є міною (бартером), адже криптоактиви класифікуються як товар, а не як грошовий засіб.

Таким чином, її обмін на будь-який інший товар чи послугу формально є бартерною операцією.

Відповідно до ст. 715 ЦКУ, «за договором міни (бартеру) кожна із сторін зобов'язується передати другій стороні у власність один товар в обмін на інший товар»; «Договором може бути встановлений обмін майна на роботи (послуги)» [452].

Відповідно до ч. 5 ст. 293 ГКУ та ст. 716 ЦКУ, до договору міни (бартеру) застосовуються положення, які регулюють договори купівлі-продажу, поставки чи контрактації, якщо це не суперечить законодавству та відповідає суті відносин між сторонами.

Згідно з ч. 2 ст. 715 ЦКУ, кожна сторона договору міни (бартеру) є продавцем того товару, який вона передає в обмін, та покупцем того, що отримує взамін. Таким чином, сторони можуть обмінювати криптоактиви на інші криптоактиви, товари або послуги, і ці операції вважаються бартерними.

Водночас варто враховувати обмеження, які законодавство встановлює для бартерних операцій. Наприклад, відповідно до ч. 4 ст. 293 ГКУ, не може бути об’єктом міни майно з основних фондів державної або комунальної власності, якщо друга сторона договору не є державним чи комунальним підприємством. Однак це обмеження, на нашу думку, не впливає на ринок віртуальних активів.

Операції з бартерного обміну криптоактивів пропонується класифікувати за КВЕД 47.91 «Роздрібна торгівля, що здійснюється фірмами поштового замовлення або через мережу Інтернет», оскільки такі операції фактично відповідають цій категорії діяльності.

ВА широко використовуються для міжнародних розрахунків, зокрема в зовнішньоекономічній діяльності (ЗЕД), де вітчизняне законодавство встановлює низку обмежень для бартерних операцій. Закон України «Про регулювання товарообмінних (бартерних) операцій у галузі зовнішньоекономічної діяльності» (далі – Закон про бартер у ЗЕД) регулює

порядок проведення таких операцій між суб'єктами ЗЕД України та іноземними суб'єктами господарської діяльності [453].

Відповідно до Закону про бартер у ЗЕД суб'єкти зовнішньоекономічної діяльності мають право проводити бартерні операції (ч. 3 ст. 1). Товари, що імпортуються за бартерним договором, мають бути ввезені на митну територію України у строки, зазначені в договорі, але не пізніше 180 календарних днів з дати митного оформлення експортних товарів. Для робіт і послуг цей строк обчислюється з дати підписання акта або іншого документа, що засвідчує виконання робіт чи надання послуг (ч. 1 ст. 2). Суб'єкти зовнішньоекономічної діяльності повинні повідомити органи доходів і зборів про факт здійснення експорту або імпорту за бартерним договором протягом п'яти робочих днів після підписання відповідного документа чи акта. Неподання такої інформації тягне за собою штраф у розмірі 1 % вартості експортованих товарів (робіт, послуг) за кожен день прострочення, але не більше їхньої загальної вартості (ч. 4 ст. 3) [453].

Ці обмеження необхідно враховувати під час обміну ВА на інші криптоактиви, товари, роботи чи послуги.

Окремо слід зазначити, що є перелік товарів, робіт і послуг, імпорт та експорт яких заборонено в обмін на ВА в рамках бартерних операцій. Відповідно до Закону про бартер у ЗЕД Кабінет Міністрів України може встановлювати такі заборони.

Постановою Кабінету Міністрів України від 29.04.1999 № 756 затверджено перелік товарів, експорт чи імпорт яких за бартерними операціями заборонено [454]. Наприклад, це стосується насіння соняшнику, олії, пива солодового, руд і концентратів дорогоцінних металів, шкіряної сировини.

Варто наголосити, що в рамках ЗЕД-операцій із зазначеними товарами використання смарт-контрактів є неприпустимим, оскільки вони передбачають передачу ВА як частини бартерної угоди.

Оподаткування залишається одним із ключових питань для ринку ВА. Надмірні податкові ставки на операції з ВА, зокрема ПДВ, можуть суттєво обмежити його розвиток.

Криптоактиви, як зазначалося, є об'єктом права власності. Отже, їхній продаж класифікується як постачання товарів, оскільки ВА є товаром (нематеріальними активами) і при їх продажу відбувається передача права розпорядження.

Водночас постачання послуг визначається як «будь-яка операція, що не є постачанням товарів, або інша операція, пов’язана з передачею прав на об’єкти права інтелектуальної власності чи інші нематеріальні активи, а також надання послуг, що споживаються в процесі виконання певних дій чи здійснення діяльності» [453]. Таким чином, продаж криптоактивів не може розглядатися як постачання послуг, оскільки є передачею товару з переходом права власності, включно з правом розпорядження.

Отже, операції з продажу, обміну чи дарування ВА є постачанням товарів. При цьому об’єктом оподаткування ПДВ виступають лише операції з постачання товарів, місце постачання яких визначено на території України. Відповідно до п. 186.1 ст. 186 ПКУ місце постачання товарів визначається як:

- фактичне місцезнаходження товарів на момент їх постачання;
- місце початку перевезення і пересилання товарів, якщо такі дії здійснюються;
- місце складання, монтажу чи встановлення товарів, якщо це передбачено.

Криптоактиви не мають фізичного місцезнаходження, не підлягають транспортуванню чи пересиланню, а також не можуть бути зібрані чи встановлені. Це унеможливлює визначення місця постачання ВА згідно з п. 186.1 ст. 186 ПКУ [444]. Таким чином, операції з постачання ВА не підпадають під об’єкт оподаткування ПДВ, оскільки не відповідають критеріям «постачання

товарів, місце постачання яких розташоване на митній території України». Відповідно, продаж ВА не є об’єктом оподаткування ПДВ, але не без винятків.

За європейською таксономією ВА, яку ми розглянули в попередніх розділах, службові (утиліті) токени, ігрові токени та NFT, які нині не є врегульованими, подібні, по суті, до постачання фізичних товарів, які є об’єктом оподаткування ПДВ. Однак, з огляду на виклики затягнутого процесу легалізації ринку ВА в Україні, оподаткування таких ВА не є першочерговим.

Відповідно до пп. 134.1.1 п. 134.1 ст. 134 ПКУ об'єктом оподаткування податком на прибуток підприємств є 134.1.1. «прибуток із джерелом походження з України та за її межами, який визначається шляхом коригування (збільшення або зменшення) фінансового результату до оподаткування (прибутку або збитку), визначеного у фінансовій звітності підприємства відповідно до національних положень (стандартів) бухгалтерського обліку або міжнародних стандартів фінансової звітності, на різниці, які виникають відповідно до положень цього Кодексу» [444].

ВА мають розглядатися для цілей оподаткування податком на прибуток підприємств як нематеріальний актив. Фінансовий результат збільшується та зменшується на суми відповідно до ст. 138 ПКУ.

Згідно з п. 291.6 ст. 291 ПКУ, платникам єдиного податку першої – третьої груп заборонено здійснювати обмін одних ВА на інші або обмінювати свої товари (роботи, послуги) на криптоактиви. Водночас обмеження, встановлені пунктами 291.5 та 291.5-1 ст. 291 ПКУ [444], не виключають можливості для осіб, які здійснюють майнінг криптовалют, бути платниками єдиного податку.

Однак здійснення майнінгу криптовалют платниками єдиного податку може стати предметом дискусії, оскільки результатом майнінгу є отримання криптовалюти (товару), а розрахунки для платників єдиного податку першої – третьої груп мають проводитися виключно у грошовій формі (п. 291.6 ст. 291 ПКУ [444]).

Проте майнінг слід розглядати як процес обробки даних у блокчейн-реєстрі, результатом якого є видобуток криптовалюти. У цьому випадку розрахунків під час майнінгу не здійснюється, оскільки операція не передбачає взаємних платежів чи обміну. Таким чином, платники єдиного податку не обмежені у праві займатися майнінгом криптовалют.

Згідно з п. 292.1 ст. 292 ПКУ доходом платника єдиного податку є:

«1) для фізичної особи – підприємця – дохід, отриманий протягом податкового (звітного) періоду в грошовій формі (готівковій та/або безготівковій)<...>

2) для юридичної особи – будь-який дохід, включаючи дохід представництв, філій, відділень такої юридичної особи, отриманий протягом податкового (звітного) періоду в грошовій формі (готівковій та/або безготівковій) <...>» [444].

Тобто дохід від майнінгової діяльності, пов'язаної з ВА, має бути віднесений до доходу платника єдиного податку, а отже, оподатковуватись за загальними правилами.

Відповідно до п. 164.2. ст. 164 ПКУ, «до загального місячного (річного) оподатковуваного доходу платника податку включаються: <...> 164.2.2. суми винагород та інших виплат, нарахованих (виплачених) платнику податку відповідно до умов цивільно-правового договору» [444]. Тобто, якщо особа здійснила продаж криптоактивів, то відповідна сума буде віднесена до загального місячного (річного) оподатковуваного доходу, що є об'єктом оподаткування ПДФО (пп. 163.1.1 п. 163.1 ст. 163 ПКУ) за поточною ставкою 18 % (п. 167.1 ст. 167 ПКУ).

Об'єктом оподаткування військовим збором за оновленою ставкою 5 % є доходи, визначені ст. 163 ПКУ. Як зазначалося, доходи від продажу криптоактивів включаються до доходів, визначених ст. 163 ПКУ. Тобто фізична особа зобов'язана сплатити військовий збір, з доходу, отриманого від продажу криптоактивів.

Нагадаємо: у США операції з ВА підлягають оподаткуванню податком на доходи фізичних осіб або податком на приріст капіталу, розмір якого варіюється від 0 до 20 %. ВА дозволено використовувати як засіб обміну та зберігання, а також їх визнано цінним папером у цифровій формі.

В Італії в державному бюджету на 2023 р. підвищили податок на приріст капіталу від ВА до 26 %, якщо дохід перевищує 2000 євро. Крім того, запропоновано можливість декларування вартості ВА станом на 1 січня 2023 р. із застосуванням податкової ставки 14 %.

У Великій Британії операції з ВА оподатковуються аналогічно до операцій з іноземними валютами (Додаток Д).

Вперше в 2019 р. на розгляд Верховної Ради було подано проєкт закону «Про внесення змін до Податкового кодексу та інших законів України щодо оподаткування операцій з криптоактивами» [455]. Проект надавав характеристику низці визначень, таких як «криптоактив», «токен-актив», «розподілений реєстр», «віртуальний актив», «токен». Попри п’ятирічну законотворчу діяльність щодо легалізації ВА та запропоновані ще три аналогічні проєкти закону, згаданий проєкт виносився на розгляд засідання народних депутатів Верховної Ради України у вересні 2024 р. (включено до порядку денного: 3939-IX від 03.09.2024).

Відповідно до цього законопроєкту операції з обліку ВА не будуть обкладатися ПДВ, а інвестиційний прибуток у результаті продажу ВА на п’ять років має бути оподатковуваний податком на доходи фізичних осіб, ставка якого становитиме 5 %.

Правові засади процесу регулювання бухгалтерського обліку ВА залишаються відкритими, тому при веденні їх обліку доречніше використовувати міжнародні стандарти фінансової звітності. Залежно від бізнес-моделей суб’єкта господарювання можуть бути застосовані різні методи обліку ВА відповідно до:

– МСБО 38 «Нематеріальні активи» [443];

– МСБО 2 «Запаси» [456].

МСБО 2 визначає запаси як товари, що утримуються для комерційних цілей, виробництва або постачання виробничих матеріалів. Водночас ВА не мають фізичної форми, що викликає питання їхньої класифікації. Якщо компанія чітко вказує, що криптоактиви утримуються для продажу, вона може попередньо визначити їх як запаси. Проте методи оцінки та відсутність фізичної форми ставлять під сумнів цю класифікацію.

Доведено, що найоптимальнішим методом є облік ВА за МСБО 38, оскільки їхня характеристика найбільше відповідає визначенню їх як нематеріального активу. МСБО 38 «Нематеріальні активи» дає змогу визначити собівартість і переоцінку криптоактивів. ВА повинні оцінюватися за собівартістю під час первісного визнання, а згодом – як собівартість за вирахуванням накопиченої амортизації та збитків від зменшення корисності активів. Використовуючи модель переоцінки, ВА можна обліковувати за переоціненою сумою, якщо для них є активний ринок. Однак це може стосуватися не всіх ВА. Для всіх ВА одного класу слід застосовувати однакову модель оцінки. Якщо є активи, для яких немає активного ринку, то ці активи варто оцінювати за собівартістю [443].

Суб’єкт господарювання має визначити, чи термін корисного використання ВА є обмеженим або невизначеним. Невизначений термін використання означає, що період, протягом якого актив здатний генерувати чисті грошові надходження, не має обмежень. З огляду на особливості ВА, їх слід класифікувати як активи з невизначеним строком використання. Такі нематеріальні активи не підлягають амортизації, але їх необхідно щорічно перевіряти на зменшення корисності.

З огляду на численні винятки при визнанні й оцінці ВА важливо надавати повну й зрозумілу інформацію для користувачів. Відповідно до МСБО 1 «Подання фінансової звітності» суб’єкт господарювання має розкривати рішення керівництва щодо обліку активів, зокрема ВА, якщо ці рішення суттєво

вплинули на суми у фінансовій звітності [457]. МСБО 10 «Події після звітного періоду» також зобов'язує суб'єкта господарювання повідомляти про всі істотні події, що не підлягають коригуванню [458].

Для обліку ВА рекомендовано введення окремого субрахунку 128 «Криптоактиви» до синтетичного рахунку 12, що не суперечить чинному Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств та організацій [459, 460]. Запропоновано кореспонденцію рахунків бухгалтерського обліку ВА (табл. 4.1).

Таблиця 4.1

Типові проводки з бухгалтерського обліку криптоактивів

№	Зміст	Дебет	Кредит
1.	Видобуток криптоактивів	154	117,66,65
2.	1) Купівля криптоактивів за грошові кошти 2) Оприбуткування криптоактивів 3) Перераховано кошти за криптоактиви	154 128 «Криптоактиви» 631	631 154 301
3.	1) Придбання віртуальних активів на крипто-валютній біржі 2) Оприбуткування криптоактивів 3)Перераховано коштів за криптоактиви	154 128 «Криптоактиви» 68	68 154 311
4.	Втрата криптоактивів у результаті хакерської атаки	97	128 «Криптоактиви»
5.	1) Придбання товарів у постачальника 2) Розрахунок криптоактивами за отримані товари	28 631	631 128 «Крипт активи»

Джерело: складено автором за [459]

Розрахунки з цифровою валютою виконуються через трансакції, що фіксуються в блокчейні, технологія якого є основою для створення кожного криптоактиву. Блокчейн працює як відкрита мережа, що означає доступність інформації будь-яким користувачам інтернету, хоча також існують приватні блокчейни з обмеженим доступом.

Технологія блокчейну має потенціал змінити майбутнє, впливаючи на всі соціальні інститути, зокрема на бухгалтерський облік. Її зростаюча популярність

зумовлена тим, що вона вирішує проблему довіри між партнерами та дає змогу знизити витрати на посередників, що є важливою умовою ведення бізнесу.

Блокчейн являє собою величезну глобальну базу даних без єдиного власника, яка настільки поширена, що змінити її майже неможливо, навіть для операторів, котрі зберігають ці дані. Кожна трансакція, або «блок», перевіряється майнерами, чиє число не обмежене, що забезпечує надійність системи. Після підтвердження правильності операції всіма майнерами блок приєднується до ланцюга. Він не може бути видалений, оскільки містить дані про попередні трансакції.

Використання блокчейну в бухгалтерському обліку вирішить проблеми приховування незаконних трансакцій, навмисного чи помилкового виправлення здійснених господарських операцій та часткового занесення інформації до облікової системи тощо.

Отже, професійне та наукове обговорення обліку криптоактивів розпочато, а методичні організації та регуляторні органи активно досліджують цю сферу, що вимагає серйозної інституалізації. Зі зростанням інтересу до криптоіндустрії збільшиться і кількість посередників, котрі будуть зацікавлені в купівлі, продажу та зберіганні таких активів. Це підвищує значення впровадження зваженої облікової політики і забезпечення її послідовного застосування для таких операцій, а також відповідного розкриття у фінансовій звітності для інформування користувачів.

Відсутність спеціальних стандартів і директив для ідентифікації ВА, отриманих в обмін на товари чи послуги,, як певного виду активу і його точної оцінки вимагає від суб’єкта господарювання прийняття рішень, керуючись професійним судженням. Без сумніву, кожен ВА повинен оцінюватися з огляду на його специфічні характеристики. Однак наявна практика використання міжнародних стандартів, розроблена до виникнення цифрової економіки, не передбачала облік ВА.

Існує низка важливих аспектів, які потребують подальших досліджень, оскільки облікова наука та практика не були готові до викликів криптоіндустрії, і чинне законодавство досі визначає методику обліку ВА, тоді як цифрові технології та віртуальні ринки динамічно розвиваються та впроваджуються в практичну діяльність суб'єктів господарювання.

Фонд міжнародних стандартів фінансової звітності (МСФЗ) обговорив застосування стандартів щодо зберігання ВА у березні 2019 р. Фонд зазначив, що існує кілька типів ВА і для обговорення розглянув підкатегорію криптоактивів – криптовалюти – з такими характеристиками:

- криптовалюти є цифровими або віртуальними валютами, що реєструються в розподіленому реєстрі та використовують криптографію для забезпечення безпеки;
- криптовалюти не емітовані органом юрисдикції чи іншою стороною;
- володіння криптовалютами не створює контрактних відносин між власником та іншими сторонами [461].

Фонд зробив висновок, що до криптоактивів слід застосовувати МСБО 2 «Запаси», якщо вони утримуються для подальшого продажу в рамках звичайної діяльності. Якщо МСБО 2 не застосовується, то підприємства повинні використовувати МСБО 38 «Нематеріальні активи» для обліку ВА як нематеріальних активів.

Фонд міжнародних стандартів фінансової звітності також підкреслив, що ВА відповідають визначенню нематеріальних активів за МСБО 38, оскільки є ідентифікованими негрошовими активами без фізичної форми.

Пункт 3 МСБО 38 встановлює виняток для нематеріальних активів, які утримуються для продажу в межах звичайної діяльності. Такі активи підпадають під дію МСБО 2 «Запаси» і обліковуються за нижчою із собівартості та чистої вартості реалізації, а не за моделями собівартості чи переоцінки згідно з МСБО 38.11.

Крім того, МСБО 2 не застосовується до оцінки запасів, що утримуються торговими посередниками, які оцінюють свої запаси за справедливою вартістю за вирахуванням витрат на продаж та визнають зміни у справедливій вартості за мінусом витрат на продаж у прибутку або збитку в період змін.

Наразі бракує вказівок щодо обліку нематеріальних активів та товарів, що зберігаються для інвестиційних цілей.

На глобальному рівні уряди й основні бухгалтерські організації не розробили чіткої, уніфікованої та детальної облікової політики або керівних принципів для вирішення бухгалтерських проблем, пов'язаних з ВА. Зі зростанням буму інвестицій у ВА їхні коливання ринкової вартості стають дедалі очевиднішими. Тому створення розумної та вдосконаленої системи бухгалтерського обліку ВА є дуже важливим для фінансових ринків. При створенні майбутньої системи обліку криптоактивів слід звертати увагу на три основні аспекти:

- розрізняти ВА з різними характеристиками залежно від мети їх утримання і визнавати їхні відмінності в ліквідності та ризиках;
- при розробленні або оновленні відповідних рекомендацій повністю враховувати високі коливання ринкової ціни ВА і невизначеність їхньої внутрішньої вартості;
- дотримуватися відповідних керівних принципів для фінансових інструментів, всебічно враховувати, як підприємства керують своїми ВА, а також характеристики грошових потоків, які ці активи можуть генерувати, ретельно класифікувати ВА і детально пояснювати причини та основи цієї класифікації.

У березні 2022 р. Президент України підписав Закон «Про віртуальні активи», який визначив правовий статус ВА та встановив основи для їх регулювання [162]. Однак, для набуття правової сили цим законом необхідно було внести зміни до Податкового кодексу України. Так, у контексті другого українського законопроєкту «Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами» від 13.03.2022

року № 7150 [462] було запропоновано зміни до Податкового кодексу щодо оподаткування ВА. Відповідно до ст. 14.1 ПКУ пропонувалось доповнити ПКУ п. 14.1.196-1, що визначав прибуток від операцій з ВА як позитивну різницю між доходом, отриманим платником податку від таких операцій, та витратами на їх придбання.

Законопроєкт № 7150 передбачав такі правила оподаткування:

1. Для юридичних осіб на загальній системі оподаткування:

- 5 % від доходу від операцій із продажу ВА. Це стосується як прямого доходу від операцій із ВА, так і посередницької діяльності;
- від'ємні значення переносяться на наступні звітні періоди.

2. Для фізичних осіб:

- 5 % податку на доходи фізичних осіб (ПДФО) та 1,5 % військового збору;
- результати операцій із ВА відображаються в річній декларації. У разі від'ємного результату його можна перенести на наступний рік;
- обмін одних ВА на інші не підлягає оподаткуванню.

3. Для фізичних осіб – підприємців (ФОП) на загальній системі:

- оподаткування здійснюється як для звичайних фізичних осіб — податки сплачуються з доходу від операцій із ВА.

4. Для ФОП — платників єдиного податку:

- отримання дозволу на ведення діяльності, пов'язаної з обігом ВА;
- прибуток від продажу ВА декларується, а податок сплачується за ставкою 5 % [462].

З прийняттям та оприлюдненням європейської Стратегії цифрових фінансів [83] постала необхідність прийняття підходів до законотворчої діяльності щодо оподаткування ВА та майнінгу за європейськими стандартами, адже, з огляду на набуття Україною статусу кандидата в члени Європейського Союзу, концепція побудови національного законодавства має відповідати Регламенту ЄС про ринки криптоактивів (MiCA) для забезпечення максимальної

сумісності між українським та європейським ринками ВА. З причин перегляду на відповідність європейських стандартів законопроєкт «Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами» від 13.03.2022 № 7150 було відкликано авторами.

В Україні розроблено і в листопаді 2023 року зареєстровано у Верховній Раді ще два законопроєкти, спрямовані на регулювання ринку ВА. Перший — проєкт закону від Національної комісії з цінних паперів та фондового ринку «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні» (від 07.11.2023 № 10225) [462]. Другий — проєкт закону від Міністерства цифрової трансформації України з аналогічною назвою (від 17.11.2023 № 10225-1) [463].

Головна відмінність між законопроєктами полягає в тому, що проєкт № 10225 акцентує увагу на інтеграції з європейським законодавством, тоді як № 10225-1 переважно зберігає положення попереднього законодавства, пропонуючи менший рівень захисту користувачів і слабші механізми контролю для більш конкурентного розвитку та інвестиційної привабливості (табл. 4.2).

Таблиця 4.2

Порівняльний аналіз проектів законів щодо регулювання, оподаткування та визначення державних регуляторів ринку ВА від 07.11.2023р. №10225 та від 17.11.2023р. №10225-1

	Проєкт закону №10225	**Проєкт закону №10225-1**
Органи контролю	Національна комісія з цінних паперів та фондового ринку (НКЦПФР) і Національний банк України	Міністерство цифрової трансформації та Національний банк України
Ставки оподаткування ВА	Доходи фізичних осіб	
	18% з додатковим військовим збором 1,5%	5% протягом перших трьох років, 9% протягом наступних п'яти років і 18% після восьми років.

Продовження таблиці 4.2

	Доходи юридичних осіб	
	податок на прибуток за стандартною ставкою 18% від приросту на капітал	ППВА надається можливість вибору між стандартним податком на прибуток (18%) або податком на виведений капітал (9%) для резидентів «Дія.City».
	Звільнення від оподаткування операцій з безоплатного отримання ВА - майнінг чи стейкінг	Звільнення від ПДВ на операції з ВА, окрім токенів, які представляють реальні товари або послуги.
Цільове спрямування та фінансова інклюзія	Приділяє увагу впровадженню європейських стандартів для забезпечення прозорості та довіри на ринку ВА.	Надає більшу увагу створенню умов для інновацій та розвитку бізнесу в сфері ВА, особливо через введення спеціалізованої зони для бізнесу в сфері ІТ.

Джерело: складено автором.

Поки що питання оподаткування майнінгу в Україні залишається остаточно не врегульованим. Наразі жоден із законопроєктів не набув чинності, тому операції з ВА регулюються чинними правилами оподаткування.

Повертаючись до ризиків використання ВА в злочинній діяльності, європейські органи державного регулювання насамперед порушують питання обміну інформацією щодо оподаткування, як зазначалося, в оновленій Директиві 2011/16/ЄС, також відомої як DAC8.

На відміну від традиційних фінансових трансакцій, податкові органи наразі усвідомлюють, що їм бракує інформації для моніторингу доходів від ВА, особливо в контексті трансакцій, які проводяться через кордони.

Оскільки оборот ВА може оподатковуватись, існує прогалина між декларованими сумами та тими, що мали би бути сплачені. Для вирішення цієї проблеми ОЕСР розробила Рамкову звітність про криптоактиви (CARF), яка супроводжується поправками до стандарту CRS (Common Reporting Standard) [436]. CARF визначає, як звітувати про трансакції з ВА, а також сприяє дотриманню правил ПВК/ФТ. Завдяки підтримці з боку багатьох країн CARF

забезпечить підвищення прозорості ВА через автоматичний обмін інформацією на щорічній основі, аналогічно до стандартів CRS і FATCA. Основна відмінність у тому, що ця рамкова звітність стосується трансакцій з ВА серед юрисдикцій, чиї податкові резиденти займаються такими операціями.

Для установ, які звикли звітувати про баланси рахунків на кінець року, звітність буде розширено з урахуванням вимог CARF. Для компаній, що працюють виключно з ВА, це буде перший досвід у сфері звітності CRS. Поправки охоплюють електронні гроші, віртуальні активи, цифрові валюти центральних банків (CBDC) і збільшують обсяг інформації про клієнтів, яка підлягає звітності. Також вони гарантують охоплення непрямих інвестицій у ВА через деривативи.

CARF набуде чинності 1 січня 2026 р. ППВА повинні будуть збирати інформацію про клієнтів із цієї дати, а перші звіти за 2026 р. мають бути подані до 31 травня 2027 р. Зміни до CRS також почнуть діяти з 1 січня 2026 р. з аналогічними строками звітності. Уряди продовжуватимуть співпрацювати із зацікавленими сторонами для розроблення відповідних систем, процесів і роз'яснювальної документації.

В оновленому 18 жовтня 2024 р. меморандумі з МВФ за результатом п'ятого перегляду програми Extended Fund Facility (EFF) наголошено на розробленні комплексного пакета заходів на післявоєнний період для реформування оподаткування та визначення принципів оподаткування ВА, узгоджених із правилами ЄС, зокрема щодо обміну інформацією та ініціатив Глобального форуму ОЕСР. Робота в кількох із цих напрямів уже почалася та підтримуватиметься технічною допомогою МВФ та інших партнерів з розвитку [465].

Планується розроблення законодавчих поправок, спрямованих на встановлення вимог до звітності для операторів цифрових платформ та забезпечення міжнародного обміну даними відповідно до Директиви ЄС і модельних правил звітності ОЕСР [466]. Ці заходи дадуть змогу Державній

податковій службі (ДПС) отримувати інформацію від операторів цифрових платформ і міжнародних органів щодо доходів фізичних осіб, які не реєструються як ФОП або користуються спрощеною системою оподаткування. Впровадження таких інструментів забезпечить ефективний контроль за своєчасністю, достовірністю та повнотою декларування доходів, а також сприятиме значному розширенню податкової бази за рахунок оподаткування доходів, які наразі залишаються поза увагою.

Як зазначено в документі, відповідні законодавчі пропозиції планується подати до парламенту до кінця квітня 2025 р. (пропонований структурний контрольний показник). Цей крок сприятиме мобілізації податкових надходжень, гармонізації українського податкового законодавства з нормами ЄС та стандартами ОЕСР, а також стане основою для реформування системи ДПС шляхом запровадження сучасних цифрових інструментів контролю.

Крім того, буде розроблено законодавчі поправки, спрямовані на імплементацію правил запобігання ухиленню від сплати податків. Вони враховуватимуть вимоги Директиви ЄС щодо боротьби з ухиленням від сплати податків (EU ATAD) [467] та найкращі міжнародні практики, забезпечуючи захист податкової бази від ерозії та переміщення прибутку.

4.2. Інтеграція сучасних технологічних рішень у систему управління ризиками обігу ВА у антилегалізаційній сфері

Сучасний світ стрімко змінюється, і в Україні триває активний пошук ефективних рішень як у розвитку ринків, так і в модернізації державного управління. Міністерство цифрової трансформації України, що докладає значних зусиль до забезпечення відповідності міжнародним стандартам, є провідним органом щодо кіберзахисту, цифровізації економіки і державного управління,

упровадження новітніх технологій, а також співпрацює з криптоспільнотою, котра бере активну участь у розробленні законодавства й обговоренні його з органами центральної влади, залучає міжнародних експертів для обміну досвідом та розроблення кращих для України рішень. Національна комісія з цінних паперів та фондового ринку за підтримки та співпраці міжнародних інституцій розробили та представили проєкт закону про регулювання ринку ВА в Україні, який впроваджує за виключенням певних особливостей базові положень Регламенту (ЄС) 2023/1114 Європейського парламенту та Ради від 31 травня 2023 року про ринки криптоактивів (Markets in Crypto-Assets Regulation — MiCA) [78].

Завдяки розробленню спільних нормативних актів Міністерства фінансів України і Державної служби фінансового моніторингу України дедалі більшого визнання й поширення набуває ризик-орієнтований підхід, застосування якого сприятиме створенню оптимальних умов для розвитку нових ринків, запобіганню використанню нових інструментів зі злочинними намірами, ефективному державному регулюванню та діяльності правоохоронної та судової системи. Особливої уваги в контексті врегулювання й визначення ризиків потребує взаємодія криптобізнесу із секторами реальної економіки, так звані шлюзи обміну ВА на фінансові інструменти, цінні папери, нерухомість, майнові права. Важливо забезпечити гармонійну співпрацю державних наглядових органів реальних секторів економіки із наглядовим органом ринку ВА – Національною комісією з цінних паперів та фондового ринку (НКЦПФР), наявність якого рекомендована міжнародними стандартами, та Національним банком України (НБУ) як державним наглядовим органом банківського сектору, фінансових компаній і платіжних систем, які забезпечують обмінні операції грошових коштів та ВА, а отже, головного шлюзу взаємодії фіатного і віртуального ринків.

Також учасники ринку ВА в процесі діяльності потребують відкриття банківських рахунків для комерційної і господарської діяльності. Тобто

взаємодія з банківською спільнотою сприяє розвитку правовому полю функціонування ринку ВА. Водночас співпраця з ринком ВА може збагатити банківський сектор новаціями цифрового світу й допомогти оновленню підходів до оцінки та управління ризиками щодо ПВК/ФТ, інвестиційної та комерційної діяльності.

З огляду на різноманітну природу, ВА намагання наглядових органів інших секторів економіки визначити подібність ВА до інструментів цих секторів доцільно модернізувати підходи до регулювання ринку таких активів, оподаткування операцій з ВА, що сприятиме його транспарентності й доброчесній роботі наглядових органів і приватного сектору, а також створенню інституціональних умов для удосконалення роботи національної системи ПВК/ФТ з урахуванням міжнародних стандартів. У частині забезпечення впровадження та ефективної реалізації механізмів здійснення ПВК-процедур в функціюванні українського ринку ВА, секторальної оцінки ризиків на ринку віртуальних активів та її інтеграції із секторальними оцінками ризиків банківського та небанківського секторів фінансового ринку з метою проведення Національної оцінки ризиків щодо ПВК/ФТ Національна антилегалізаційна система потребує вдосконалення процесу збору загальної статистики та забезпечення її достовірності, системи координації для забезпечення узгодженості й ефективності дій учасників системи, внесення відповідних змін до системи поглибленої перевірки клієнтів та оцінки ризиків на національному і наднаціональному рівнях.

Криптоіндустрія в Україні потребує доступу до банківської системи. Через обмеженість офіційного доступу «сірі» та «чорні» сервіси тіньової економіки використовують банки «в темну». Для цього достатньо відкрити рахунки на певну кількість фізичних осіб, котрі отримують кошти від великих іноземних криптосервісів або переказують до них кошти. Подальші розрахунки з клієнтами в готівці та безготівковими переказами – давно відпрацьована технологія, тому

запитання «Чи використовують конвертаційні центри криптовалюту?» є риторичним.

Якщо банк обслуговує рахунки легального оператора ринку ВА (наприклад, криптобіржі), надавані послуги повністю аналогічні кореспондентським відносинам, ППВА проводить ідентифікацію та верифікацію своїх клієнтів, відстежує їхні трансакції на ризиковість, у тому числі у сфері ВК/ФТ. Банк тільки обслуговує кінцеву ланку цих операцій і може лише покладатися на здійснення ППВА заходів ПВК/ФТ на належному рівні.

З огляду на поточний стан вітчизняної економіки та перспективи її відновлення в умовах війни з рф упорядкування обігу ВА є важливим кроком до побудови ліквідного регульованого ринку ВА в платіжній системі України. Основними проблемними питаннями щодо впорядкування обігу ВА в Україні, які потребують негайного на сучасному етапі вирішення з боку НКЦПФР та НБУ, є:

- аналіз та класифікація ВА, які найбільше вживаються в Україні, відповідно до міжнародних і європейських нормативно-правових актів та стандартів згідно з їхніми основними характеристиками та економічними цілями. Проведення детального аналізу класифікації різних категорій ВА необхідне для забезпечення належного регулювання та контролю відповідно до їхніх характеристик і ризиків. На основі аналізу різних типів ВА доцільно встановити вимоги для ринків тих ВА, які нині не підпадають під дію законодавства України. У міжнародній практиці найпоширеніша класифікація ВА стосується активів, призначених для використання як засіб платежу, для інвестицій та службових токенів, котрі призначені для надання цифрового доступу до програм або послуг;
- визначення характеристик ВА, які регулюються положеннями Закону України «Про ринки капіталу та організовані товарні ринки» [476]. Такий підхід вимагає, щоб усі ППВА, пропонуючи послуги відповідно до законодавства, зокрема пов’язані з випуском цінних паперів, обігом, клірингом

та розрахунками за віртуальними активами, застосовували і повністю дотримувалися відповідних правил незалежно від технологій, які вони використовують;

- адаптація розділеної та децентралізованої книги трансакцій до технології блокчейн, онлайнових однорангових або користувальницьких платформ у платіжній інфраструктурі до законодавства ЄС. Складність технології блокчейн може стати перешкодою для роздрібних інвесторів ВА з третіх країн, які перебувають у різному правовому полі. У зв'язку з цим виникають проблеми, що стосуються насамперед захисту споживачів та інвесторів, цілісності ринку і фінансової стабільності. Такий підхід потребує впровадження пілотного режиму ринкової інфраструктури технологій DLT за аналогією з ЄС та встановлення правил для віртуальних активів, випущених у третіх країнах, і тих, що перебувають в обігу в Україні;
- встановлення вимог до фінансових установ стосовно проведення оцінки ризиків із питань ПВК/ФТ на основі ризик-орієнтованого підходу до впровадження нових технологій, продуктів та практик і застосування відповідних заходів щодо управління та зниження ризиків, які виконують функції державного регулювання та нагляду;
- упровадження суб'єктами первинного фінансового моніторингу аналізу видів діяльності з ВА, зокрема тих, які пов'язані з його клієнтами, географічним розташуванням держави реєстрації клієнта або установи, через яку він здійснює передачу (отримання) активів, видом товарів та послуг. У Звіті Ради фінансової стабільності (FSB) міністрів G20 [477] акцентується увага на впровадженні децентралізованих фінансових технологій, які можуть застосовуватись для підвищення фінансової стійкості в кількох сферах, у тому числі беручи до уваги транскордонні платежі та розрахунки, токенізацію цінних паперів, торгове фінансування й страхування і однорангове кредитування [477]. Така пропозиція охоплює ширше коло питань посилення цифрової операційної стійкості для фінансового сектору та безпеки обігу віртуальних активів;

– посилення транскордонної співпраці й міжсекторальної координації та обміну інформацією щодо розвитку ВА для усунення загроз фінансовій стабільності, що виникають у зв’язку з транскордонним і міжгалузевим характером криптоактивів.

ВК/ФТ є однією з ключових загроз національній безпеці країни, що охоплює різні галузі економіки та негативно впливає на її стабільність. У таких умовах особливого значення набувають своєчасне виявлення загроз, вразливих місць і ризиків, пов’язаних із ВК/ФТ, а також розроблення дієвих заходів для протидії їм. Доведено, що посилення глобалізаційних процесів стимулює злочинну діяльність у цій сфері, а фінансово-банківський сектор залишається найбільш уразливим до таких злочинів.

Проведений економіко-правовий аналіз нормативно-правової бази секторальної оцінки ризиків використання суб’єктів фінансово-банківського сектору для ВК/ФТ дав змогу визначити основні законодавчі акти України у сфері протидії цим загрозам. Це також допомогло дослідити механізми нормативно-правового забезпечення протидії злочинному використанню суб’єктів фінансово-банківського сектору. Отримані результати свідчать про багатогранність і широку охопленість національного законодавства у цій сфері, а також підкреслюють необхідність подальшої гармонізації українських нормативних актів із міжнародними стандартами.

Зокрема, необхідно привести у відповідність до 6-ї Директиви ЄС щодо боротьби з відмиванням коштів (6AML), Регламенту MiCA та оновленої 15-ї та 1-ї Рекомендацій FATF щодо РОП національне законодавство, а саме: з метою зміцнення механізмів ПВК/ФТ розширити список зобов'язаних суб'єктів, зокрема включити ППВА, запровадити обов'язкову перевірку кінцевих бенефіціарів для всіх активів і видів діяльності.

Потребує вдосконалення національне кримінальне законодавство шляхом посилення відповідальності за фінансові злочини, у тому числі шляхом

розширення застосування фінансових санкцій, упровадження обов'язкової конфіскації незаконних активів у разі доведення їх злочинного походження.

Для підвищення ефективності національної оцінки ризиків (НОР) у сфері ПВК/ФТ необхідно включити до оцінки криптовалютні операції, цифрові активи та фінансові послуги, що надаються онлайн, запровадити динамічний підхід до оновлення системи «червоних прапорців» для операцій з ВА, запровадити автоматизовані системи аналізу фінансових операцій, пов'язаних з оборотом ВА, у державних установах та банках.

Загрози, вразливості та ризики використання суб'єктів фінансово-банківського сектору для ВК/ФТ негативно впливають на соціально-економічний розвиток України. Зокрема, ці ризики сприяють зростанню обсягів тіньового ВВП, тіньової зайнятості та ухилення суб'єктів господарювання від сплати податків, що зумовлює дестабілізуючий вплив на економіку країни. Вони вимагають посилення контролю за цифровими активами та онлайн-фінансовими послугами шляхом упровадження державного регулювання крипторинку, реєстрацію ППВА як суб'єктів первинного фінансового моніторингу, запровадження вимоги FATF щодо ідентифікації сторін криптотрансакцій. Також потребує посилення контроль за фінансовими технологіями (FinTech) та платіжними системами, а саме йдеться про реєстрацію постачальників фінансових технологій (FinTech) та визначення їхніх регуляторних зобов'язань, встановлення вимог щодо ідентифікації клієнтів у фінансових онлайн-сервісах.

Позитивно на вдосконалення функціонування Національної системи ПВК/ФТ вплине посилення міжнародної співпраці шляхом інтенсифікації обміну інформацією з міжнародними регуляторами, створення ефективних механізмів контролю за транскордонними трансакціями.

За результатами аналізу стратегічних пріоритетів протидії ризикам використання фінансово-банківського сектору для ВК/ФТ встановлено важливість оцінки наслідків, викликаних зростанням ризиків. Ключовими напрямами протидії визначено зменшення обсягу використання готівкових

коштів, зниження рівня тіньової економіки та вдосконалення відповідальним за стратегію та політику діяльності Національної системи ПВК/ФТ в Україні органом (МФУ) та координатором цієї національної системи (ДСФМУ) методології проведення НОР.

Щодо проведення секторальної оцінки ризиків ринку віртуальних активів як складової НОР необхідно використати наявні методології проведення оцінки ризиків Світового банку та МВФ. У 2023 р. експертами МВФ на базі їхньої загальної методики оцінки ризиків щодо ВК/ФТ розроблено методику оцінки ризиків використання ВА щодо ВК/ФТ [474], яка може бути взята за основу для проведення секторальної оцінки ринку ВА в Україні.

Крім того, після консультацій з організаціями громадянського суспільства та іншими зацікавленими сторонами, МВФ наприкінці 2023 р. опублікував нову стратегію, спрямовану на ПВК/ФТ [479]. Ця стратегія стане основою взаємодії МВФ із країнами в межах усіх його функцій: моніторингу, програм оцінки фінансового сектору, кредитування та розвитку спроможностей. До публікації стратегії додавалися п’ять аналітичних документів, що висвітлювали такі питання, як незаконні фінансові потоки та фінансова стабільність, а також запуск вебсайту МВФ із питань ПВК/ФТ і блогу, в якому б обґрунтовувалося та доводилось, що фінансові злочини завдають шкоди економікам і потребують кращого розуміння та стримування.

Мережа податкової справедливості (Tax Justice Network) брала активну участь у процесі консультацій, які привели до ухвалення нової стратегії, і відстоювала амбітні політики під час весняних і щорічних зустрічей МВФ / Світового банку у 2023 р.

Однією з головних переваг нової стратегії є намір МВФ використовувати свої сильні сторони та мандат для досягнення цілей у ПВК. Фонд планує наголошувати на макроекономічних наслідках фінансових злочинів через фіскальні, монетарні та структурні канали, включно з транскордонними незаконними фінансовими потоками.

Це, ймовірно, свідчить про зміну акцентів: замість суворого підходу до країн із низьким рівнем доходу та поблажливого ставлення до великих фінансових центрів МВФ тепер має зосереджуватися на податкових гаванях та юрисдикціях, що сприяють секретності. До таких належать компанії, зареєстровані на Британських Віргінських островах, банки у Швейцарії та США, нерухомість у Великій Британії та Дубаї (ОАЕ), а також хедж-фонди на Каймановых островах. Це є успіхом адвокації, базованої на підходах Індексу фінансової секретності (Financial Secrecy Index) та Індексу корпоративних податкових гаваней (Corporate Tax Haven Index) [480].

Нова стратегія передбачає уникнення так званої перехресної умовності в рекомендаціях МВФ. Це означає, що Фонд більше не буде автоматично орієнтуватися на списки FATF, які переважно фокусуються на країнах, що розвиваються, і рідко націлюються на безпечні гавані для злочинців. Натомість МВФ покладатиметься на власну оцінку критичності ризиків. Фонд має вимагати публічного доступу до інформації про бенефіціарну власність і реєстрацію трастів, особливо в юрисдикціях, чия непрозорість становить глобальний ризик. Уже тепер МВФ вимагає доступу до цієї інформації в контексті державних закупівель під час COVID-19, але очікується, що це стане загальноприйнятою практикою для секторів із високим рівнем ризику, таких як видобувна промисловість та нерухомість.

МВФ наголосив на посиленні взаємодії між місцевими органами влади, зокрема податковими органами та структурами, що займаються ПВК/ФТ. МВФ повинен регулярно співпрацювати з громадянськими організаціями при розробленні міжнародних стандартів, щоб забезпечити їхню ефективність і перспективність.

Нова стратегія МВФ щодо боротьби з відмиванням коштів [481] має перспективу, і факт залучення громадянського суспільства до її розроблення є позитивним кроком. Проте справжнім викликом стане її ефективне впровадження. МВФ повинен зробити свої умови прозорішими та посилити

участь ключових зацікавлених сторін у процесі прийняття рішень. Мережа податкової справедливості продовжуватиме стежити за реалізацією стратегії та сприяти обміну знаннями.

МВФ вже почав реалізовувати нову стратегію в міжнародних документах, що стосуються співпраці з Україною. У квітні 2024 р. Фонд представив структурні орієнтири нової програми Механізму розширеного кредитування EFF, у рамках якої у 2023 р. було передбачено два транші кредиту по 0,9 млрд дол. США після отриманих 2,7 млрд дол. США. Загалом Україна взяла на себе 19 ключових зобов'язань перед МВФ, з яких 10 стосуються фіскальної сфери, одне — монетарної, одне — енергетичної, три — фінансового сектору, та чотири — антикорупційної діяльності [482].

Основними структурними маяками стали усунення недоліків, виявлених у рамках опитування платників податків, як внесок до дорожньої карти Національної стратегії доходів та затвердження цієї Стратегії до кінця грудня 2023 р. Також вимоги торкались бюджетного процесу, а саме відновлення та посилення ст. 52 Бюджетного кодексу України для мінімізації одноразових змін до бюджету, відновлення дії статей Кодексу про ліміти державних гарантій із чіткими критеріями їх надання, прозорості та підзвітності спеціальних рахунків через консолідацію в рамках державного управління як спеціального фонду бюджету.

Певні вимоги було висунуто до Національного банку України, а саме щодо розроблення стратегії переходу до гнучкішого валютного курсу, зняття валютних обмежень і таргетування інфляції. Також НБУ мав посилити управління та нагляд у банківській сфері через створення окремих наглядових органів і відновлення планових перевірок. До кінця березня 2023 р. НБУ мусив розробити «рамку» для реабілітації банків спільно з ФГВФО, а до кінця червня 2024 р. – запровадити методологію оцінки наглядових ризиків для визначення пріоритетів власної діяльності.

Виокремлено було вимоги щодо антикорупційної політики. Так, у 2024 р. прийнято закон про відновлення декларування майна державних службовців, які не брали участі у воєнних діях, та повернення функцій НАЗК щодо перевірки декларацій. На сьогодні необхідно оптимізувати систему декларування активів державних службовців через інтеграцію з іншими базами даних та внести зміни до закону про ПВК/ФТ для посилення перевірок політично значущих осіб відповідно до стандартів FATF.

Влітку 2024 р. було додано ще два структурних маяки, один з яких спрямований на розроблення концептуальної записки щодо програми «Доступні кредити 5-7-9%» із пропозиціями націлити її на малі та середні підприємства, поступово відмовляючись від участі великих компаній, посилити моніторинг та підтримувати адекватні запобіжні заходи зі строком виконання до кінця вересня 2023 р. До кінця жовтня 2023 р. ДПСУ та ДМСУ мали підготувати плани дій щодо коротко- й середньострокових заходів, що охоплюватимуть ключові сфери реформ визначені майбутньою діагностикою, які будуть інтегровані в загальну Національну стратегію доходів [483].

У грудні 2024 р. в Україні було запроваджено методологію оцінки ризиків при здійсненні нагляду з метою прийняття поінформованих рішень про пріоритети наглядової діяльності.

У рамках співпраці з МВФ у листі про наміри від 11.03.2024 з боку України було взято зобов’язання до кінця грудня 2024 р. привести чинне законодавство щодо віртуальних активів у відповідність до найкращих міжнародних практик, враховуючи цілі економічного розвитку та пом'якшуючи ризики для цінової та фінансової стабільності, але строки виконання намірів за погодженням сторін було продовжено до кінця грудня 2025 р.

Врегульована діяльність на ринку віртуальних активів відповідно до Національної стратегії доходів сприяла б додатковим надходженням до Державного бюджету України. Замороження та конфіскація таких активів також можуть збільшити ці надходження за умови ухвалення законодавства, що

легалізує діяльність ринку віртуальних активів і сприятиме поверненню капіталів в Україну. Серед таких активів можуть бути репатрійовані кошти українських інвесторів завдяки запровадженню прогресивного оподаткування та ефективного регулювання ринку, а також віртуальні активи, заморожені у зв'язку із санкціями ЄС, США та інших держав.

Серед структурних маяків МВФ, визначених у 2023 р., окремими пунктами є посилення антикорупційної діяльності в Україні, а саме доброчесного декларування доходів, утому числі ВА, швидкого й ефективного реагування на корупційну діяльність з використанням криптоактивів. В окремому розділі дисертації надано пропозиції щодо підвищення механізмів аналізу декларування ВА та запобігання їх використанню в корупційних злочинах.

В умовах повномасштабної збройної агресії рф проти України, що триває, та у зв'язку з реальними на цій підставі загрозами національним інтересам і національній безпеці, а також діями, що порушують права та свободи людини і громадянина з боку держави-агресора, яке, зокрема, проявляється у використанні ВА з метою обходу раніше накладених обмежувальних заходів (санкцій), фінансування терористичної, розвідувальної та диверсійної діяльності виникає необхідність подальшого розширення санкцій. Їх упровадження безпосередньо пов'язане з легалізацією ринку ВА. У врегульованому ринку моніторинг діяльності, взаємодія з правоохоронними та судовими органами влади стають значно ефективнішими.

Для ефективного управління ризиками та впровадження механізмів ПВК/ФТ у сфері діяльності крипторинку основні кроки Верховної Ради України, НКЦПФР, НБУ, Мінцифри, МФУ, Держфінмоніторингу України повинні відбуватися в таких напрямах.

1. *Законодавча та нормативно-правова база*. Внесені зміни до закону про ПВК/ФТ, підписаного Президентом України Закону «Про віртуальні активи» потребують завершення процесу легалізації ринку ВА, а саме внесення за ініціативою НКЦПФР та Мінцифри змін до Податкового кодексу України щодо

оподаткування операцій з ВА та діяльності ППВА. Для забезпечення впровадження процедур ПВК/ФТ у сфері обороту віртуальних активів НКЦПФР та НБУ потрібно доповнити наявні інструкції з фінансового моніторингу специфічними вимогами для ВА.

2. *Система нагляду.* Механізми контролю за дотриманням банками вимог ПВК/ФТ можуть бути майже без змін поширені на операції з криптоактивами. Однак, з огляду на високу технологічність діяльності крипторинку, процедури комплаєнсу та ПВК/ФТ потребують технологічного вдосконалення з використанням сучасних підходів до управління та оснащення програмним забезпеченням. Система нагляду за фінансовим та крипторинком має включати нові функції:

- моніторинг ринку ВА та виявлення нелегальних операторів;
- ідентифікація клієнтів банків, які проводять інтенсивні трансакції з великими зарубіжними криптооператорами;
- контроль за операціями банків із нерезидентами, що працюють на крипторинку.

Для цього як в органах нагляду, так і в банках потрібні фахівці, котрі:

- розуміють принципи роботи криптоактивів;
- знають ризики, пов’язані з відмиванням коштів і фінансуванням тероризму за участю криптоактивів;
- знають поширені схеми шахрайства та інші фінансові злочини, що використовують ВА;
- володіють навичками аналізу операцій із ВА;
- здатні виконувати процедури комплаєнсу та ПВК/ФТ щодо діяльності крипторинку;
- розуміють механізми замороження та конфіскації криптоактивів, задіяних у злочинній діяльності.

3. *Інструменти аналізу та моніторингу операцій із ВА.* Для аналізу операцій з ВА необхідні спеціалізовані бази даних, які дають змогу визначати

належність криптовалютних гаманців (публічних адрес) до реальних об’єктів, таких як біржі, обмінники, онлайн-майданчики в Даркнеті або кримінальні сервіси.

Ці заходи є основою для підвищення ефективності діяльності у сфері ПВК/ФТ та зміцнення контролю над операціями з криптоактивами. Сьогодні правоохоронні та наглядові органи, а також суб’єкти фінансового моніторингу в усьому світі активно використовують бази даних провідних приватних компаній, таких як Chainalysis Reactor, Elliptic, Crystal, CipherTrace, Certik, Global Ledger, AMLbot, Lukka Data Solutions, Coinfirm, Purifi та Slowmist [424-428; 287-290]. Крім доступу до баз даних, ці компанії пропонують програмне забезпечення для аналізу трансакцій у ВА.

1. *Інформаційний обмін між учасниками Національної системи ПВК/ФТ та міжнародними партнерами.* Важливою складовою ефективного державного регулювання є розбудова інформаційного обміну між ППВА, іншими суб’єктами первинного фінансового моніторингу, визначеними нефінансовими установами та професіями (ВНУП) і державними регуляторними органами, правоохоронною та судовою системами, тобто між учасниками Національної системи ПВК/ФТ шляхом упровадження інтегрованої платформи, що створює зв'язок між реєстрами та їх інформаційними системами, реалізує механізми захищеного обміну даними. Додатковим аргументом щодо важливості впровадження такої системи є наявність кількох державних регуляторів ринку ВА, призначених відповідно до сутності ВА та запобігання корупційним проявам у координації взаємодії публічного й приватного секторів.

Єдину державну інформаційну систему у сфері запобігання та протидії легалізації (відмиванню) доходів і фінансуванню тероризму (ЄДІС) було створено 15 вересня 2009 р. Державним комітетом фінансового моніторингу України, правонаступником якого стала теперішня служба Держфінмоніторингу відповідно до вимог Закону України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом”. На виконання вимог

антилегалізаційного Закону від 06.12.2019 № 361-IX (набув чинності 28 квітня 2020 р.) Уряд затвердив нову редакцію Положення про Єдину державну інформаційну систему у сфері запобігання та протидії відмиванню коштів [469]. Документом встановлено оновлені засади визначення інформаційних ресурсів і використання технологій інформаційного обміну ЄДІС та порядок надання суб'єктами ЄДІС інформаційних ресурсів, необхідних для проведення Держфінмоніторингом оперативного й стратегічного аналізу.

Інформаційний обмін ЄДІС запропоновано базувати на Системі електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» [470].

Уряд, виконуючи вимоги зазначеного Закону, оновив порядок формування Переліку осіб, причетних до терористичної діяльності або щодо яких застосовано міжнародні санкції. Згідно з новою редакцією документа, підставами для включення або виключення осіб із Переліку можуть бути рішення адміністративного суду щодо осіб, котрі відповідають критеріям, визначеним резолюціями Ради Безпеки ООН, та дані міжнародних організацій про осіб, пов'язаних із терористичними організаціями або під міжнародними санкціями.

Відомості про громадян, іноземців, юридичних осіб і трасти подаються до Держфінмоніторингу, СБУ та МЗС для внесення до Переліку. Ті самі органи розглядатимуть запити про виключення з нього. МЗС, у свою чергу, забезпечуватиме комунікацію осіб зі спеціальним комітетом Ради Безпеки ООН [420]. Також передбачено оперативне інформування суб'єктів первинного фінансового моніторингу про відповідну інформацію. Реалізація цих положень сприятиме технічному узгодженню українського законодавства з міжнародними стандартами FATF.

За результатами проведеного дослідження автором визначено, що у сфері проведення розслідувань та моніторингу руху криптоактивів необхідно максимально ефективно застосовувати наявні технологічні та правові інструменти для адресного впровадження санкцій, зосереджуючись на нагляді

без необхідності змінювати чинну нормативну базу. Пріоритетом має стати оперативне впровадження добровільних зобов'язань криптовалютними і FinTech-компаніями у вигляді кодексів поведінки, розроблених у співпраці з регуляторами та наглядовими органами фінансових ринків. Водночас зловживання у сфері ліцензованих послуг фіатних платежів становить більшу загрозу, ніж операції з криптоактивами, які загалом забезпечують кращі можливості для відстеження трансакцій [470].

Російські та білоруські юридичні особи й особи, які постраждали від фінансових санкцій, накладених на них унаслідок вторгнення російської федерації в Україну, обходять їх за допомогою криптоактивів, включно з NFT, послуг із фінансових технологій (і традиційних фінансових), приховування особи та/або організації, котра постраждала від санкцій, використовують інші організації, переважно бізнес-корпорації, часто зареєстровані в податкових гаванях на членів їхніх родин та інших пов'язаних із ними осіб, зловживають SWIFT для обходу санкцій за допомогою посередників, що надають їм доступ через власні системи, використовують небанківські платіжні послуги як альтернативи для проведення операцій у разі недоступності традиційних платіжних інструментів, придбають ліквідні державні цінні папери через конвертаційні майданчики (нелегальні утворення фінансових груп для конвертації готівкових коштів у безготівкові й навпаки), вкладають в інструменти страхового і товарного ринків, зловживають організаціями, ліцензованими в ЄС, Європейській економічній зоні (ЄЕЗ) або США, також шляхом їх придбання.

Однак переважно це стосується суб'єктів, котрі вже мають зв'язки з російськими або білоруськими компаніями чи функціонують у сірій зоні. Для цієї мети доцільно використовувати Директиву ЄС про бенефіціарне володіння [476], яка імплементована в українське законодавство, але потрібне розроблення механізмів її реалізації. Водночас корисним може бути глибший аналіз, зокрема інвесторів таких організацій.

Упровадження суворіших заходів ПВК/ФТ і ухилення від санкцій вимагають проведення профілактичних перевірок суб'єктів і осіб, пов'язаних із санкційними суб'єктами. Це передбачає перевірки осіб, які мають зв'язки з тими, хто зазначений у санкційних списках. Для цього, а також для запобігання помилковій ідентифікації трансакцій як підозрілих доцільно звертатися до державних органів із Національної системи ПВК/ФТ.

Автором надано рекомендації стосовно посилення процедур оцінки ризику у сфері ВК/ФТ криптовалютних трансакцій, у тому числі тих, що здійснюються через криптовалютні банкомати. Трансакції в більшості криптовалют утворюють зв'язаний ланцюжок, який можна простежити за джерелами походження коштів та подальшим їхнім рухом. Такий аналіз може виявити зв'язки коштів із програмами-вимагачами, шахрайством, крадіжками, тіньовими ринками тощо. Для цього можуть використовуватись як публічні інструменти дослідження блокчейну, так і власні аналітичні рішення [39].

Механізм реалізації посилення процедур оцінки ризику у сфері ВК/ФТ криптовалютних трансакцій має включати: визначення критеріїв ризику шляхом розроблення та впровадження системи оцінки ризику цих трансакцій на основі міжнародних стандартів (FATF, ЄС); визначення параметрів ризику, а саме походження коштів (чисті чи сумнівні джерела), взаємодія ППВА з високоризиковими гаманцями, біржами або сервісами (наприклад, міксери, даркнет-маркети); протидію використанню користувачами криптовалютних банкоматів для анонімних операцій та аномальній активності (раптові великі перекази, дроблення сум) крипторинку. Також необхідні інтеграція аналітичного ПЗ для моніторингу криптовалютних трансакцій (Chainalysis Reactor, Elliptic, Crystal, CipherTrace, Certik, Global Ledger, AMLbot, Lukka Data Solutions, Coinfirm, Purifi та Slowmist) [424-429; 287-290], використання публічних блокчейн-сканерів (Etherscan, Blockchain.com Explorer) [472, 473] для перевірки підозрілих адрес, розроблення власних алгоритмів та систем аналітики для аналізу трансакцій і виявлення аномалій.

З боку державних регуляторів діяльності крипторинку доцільно запровадити механізми контролю за криптовалютними банкоматами, зобов'язати їх операторів реєструвати свої пристрої в державних реєстрах. Для ідентифікації користувачів перед здійсненням операцій у крипто-АТМ через аналітичні системи необхідно впровадити моніторинг і перевірку джерел коштів.

Упровадження механізму швидкого реагування для блокування підозрілих адрес або трансакцій шляхом обміну інформацією з фінансовими розвідками та поліцією для виявлення підозрілих схем можливе через співпрацю з міжнародними регуляторами і правоохоронними органами з метою запобігання транскордонному ВК.

Організація тренінгів для фінансових аналітиків, правоохоронців і операторів криптовалютних сервісів, розроблення методичних рекомендацій щодо оцінки ризику та розслідування підозрілих трансакцій сприятиме ефективнішому виявленню та запобіганню фінансовим злочинам у сфері криптовалютних трансакцій.

2. *Публічно приватне партнерство (ППП)*. Ключовим аспектом ефективного впровадження міжнародних та європейських стандартів ПВК/ФТ у сфері ВА є тісна взаємодія з наглядовими та правоохоронними органами, зокрема шляхом подання звітів про підозрілі дії та операції, що здійснюються постачальниками фінансових послуг та ППВА на ринках ЄС і США.

Офіс генерального прокурора створив оперативну групу для виявлення та арешту активів осіб, причетних до організації, забезпечення та провокування агресивної війни РФ проти України. Ці заходи спрямовані на подальшу передачу вилучених активів до Державного бюджету України з метою відновлення зруйнованої інфраструктури [474].

Департамент кіберполіції Національної поліції України ініціював створення механізму ефективної взаємодії для протидії кіберзлочинності. Основними завданнями цієї ініціативи є реалізація державної політики у сфері кібербезпеки, своєчасне інформування населення про новітні види

кіберзлочинів, а також упровадження програмних засобів для систематизації та аналізу даних про кіберінциденти, кіберзагрози і злочини.

Такий механізм повинен включати впровадження централізованої платформи для обміну інформацією між Департаментом кіберполіції, іншими підрозділами Національної поліції, фінансовими установами, державними органами та приватним сектором, створення єдиної системи координації, а саме формування спеціалізованих підрозділів у регіонах для оперативного реагування на кіберзагрози та визначення ключових партнерів у сфері кібербезпеки, таких як CERT-UA, СБУ, НБУ, міжнародні правоохоронні органи (Європол, Інтерпол, ФБР).

Упровадження системи раннього виявлення загроз та збору інформації про потенційні кібератаки, використання штучного інтелекту та великих даних (Big Data) для аналізу кіберзлочинних схем, інтеграція відкритих джерел (OSINT) та закритих баз даних для швидкої ідентифікації підозрілих дій сприятиме ефективному вдосконаленню роботи правоохоронних органів України у сфері функціонування цифрової економіки. Оперативне реагування на кіберзлочини шляхом створення цілодобового ситуаційного центру для відстеження атак та координації дій правоохоронних органів, розроблення алгоритмів швидкого блокування підозрілих фінансових операцій, доменів, IP-адрес та серверів, пов’язаних із кіберзлочинністю, взаємодії з хостинг-провайдерами та телекомунікаційними компаніями для миттєвого відключення ресурсів, що використовуються для атак, підвищить рівень національної економічної безпеки.

Удосконалення законодавчої бази щодо відповідальності за кіберзлочини, розроблення рекомендацій для бізнесу та громадян щодо захисту від кібершахрайства, використання цифрових доказів у судах, укладання угод про міжнародну співпрацю для обміну даними і проведення спільних операцій із боротьби з кіберзлочинністю, адаптація стандартів ЄС та НАТО у сфері кібербезпеки сприятимуть ефективному запобіганню,

виявленню та розслідуванню кіберзлочинів, а також підвищенню рівня цифрової безпеки в Україні. Координація такої системи має здійснюватися під егідою Ради національної безпеки та оборони України.

Спільна взаємодія органів центральної влади, правоохоронних і судових установ, підрозділів фінансової розвідки, державних наглядових органів із відповідними повноваженнями та доступом до інформації, разом із експертами криптоспільноти, розробниками програмного забезпечення для аналізу операцій із ВА, а також фахівцями банківського сектору та платіжних систем, стане ключовим фактором у створенні ефективного механізму протидії обходу санкцій, накладених на російські фінансові установи, причетні до агресії проти України.

Аналіз сучасних тенденцій у сфері оцінки ризиків використання суб'єктів фінансово-банківського сектору в ВК/ФТ засвідчує, що фінансово-банківський сектор загалом має достатньо глибоке розуміння цих ризиків. Водночас існують певні проблеми, пов'язані зі статистичною базою, проведенням оцінок зовнішніх загроз, виявленням фактів незаконних фінансових операцій злочинних угруповань, а також з обміном інформацією з фінансовими розвідками інших країн.

Блокчейн-технології, які забезпечують обіг ВА, використовуються для ВК/ФТ шляхом підтримки анонімних переказів активів у особливо великих обсягах. Без легалізації ринку ВА з упровадженням вимог щодо ідентифікації та верифікації клієнтів, застосування політики ЗСК та процедур ПВК/ФТ знизити ризики анонімності переказів не вдасться.

Структурні маяки МВФ загострюють увагу на побудові публічно-приватного партнерства Раніше ми вже зазначали, що майже всі міжнародні організації працюють над законодавством, особливо тим, що стосується новітніх технологій, цифрової економіки, штучного інтелекту, в робочих групах, до яких запрошені представники приватного сектору, науковці, представники

громадськості. Для гармонійного розвитку необхідно вибудовувати взаєморозуміння, спільні цілі на основах партнерства та взаємної поваги.

Публічно-приватне партнерство може стати ключовим інструментом стимулювання економічного зростання та відновлення країни. Завдяки співпраці між державою і приватним сектором можна прискорити процес відновлення економіки та реалізації соціальних інфраструктурних проєктів. Наприклад, поєднання державного фінансування за участю приватних інвесторів у відновленні інфраструктури може стати основою для повного відновлення країни після війни. Таким чином, у воєнний час ППП може як переживати труднощі, так і виходити на якісно новий рівень завдяки оптимізації процесів і модернізації механізмів співпраці. Важливо приділяти належну увагу розвитку таких партнерств як під час війни, так і після її завершення, забезпечуючи сталість економічного зростання та розвитку країни.

Щоб зрозуміти механізми функціонування ППП та його правову природу, органам влади, професійним асоціаціям та громадським організаціям необхідно ознайомитися з основними принципами, покладеними в його основу. Закон України «Про державно-приватне партнерство» визначає такі ключові принципи його здійснення:

- рівність сторін перед законом і заборона дискримінації;
- узгодження інтересів із метою досягнення взаємної вигоди;
- забезпечення ефективності реалізації;
- стабільність умов співпраці, спільне визнання прав та обов’язків відповідно до чинного законодавства;
- справедливий розподіл ризиків і дотримання конкурсних засад [488].

У науковій літературі пропонуються додаткові принципи ППП:

- раціональність бюджетних витрат;
- пріоритетність інтересів публічного сектору;
- соціальна відповідальність учасників;
- прозорість партнерства;

– забезпечення контролю державними органами [485].

Таким чином, основними принципами ППП для органів державної влади є раціональність використання бюджетних коштів, пріоритетність публічних інтересів і прозорість діяльності. Приватні партнери можуть використовувати власні ресурси та залучати різні форми інвестицій для реалізації проєктів, що дає змогу зменшити навантаження на державний бюджет. Зекономлені кошти можуть бути спрямовані на виконання інших завдань державної влади, що відповідає принципу ефективного використання бюджетних ресурсів.

Проєкти ППП спрямовані на задоволення публічних інтересів, адже діяльність державних органів має сприяти вирішенню потреб суспільства. Тому пріоритет публічних інтересів є одним із основоположних принципів. Прозорість партнерства також відіграє важливу роль, забезпечуючи громадянам доступ до інформації про діяльність органів влади, що сприяє підвищенню довіри до державних інституцій.

Особливу увагу слід приділити вивченню можливостей застосування ППП у сфері безпеки в Україні, оскільки більшість інших збитків певною мірою пов'язані з нестачею ресурсів і можливостей для забезпечення безпеки. Останнім часом у суспільстві активно обговорюється необхідність переосмислення філософії безпекового сектору, суттєвого вдосконалення основ державної політики в цій галузі та перегляду концепції безпекових відносин.

Воно потребує стратегічного оновлення державної політики шляхом розроблення нової Концепції кібербезпеки України, що враховуватиме сучасні загрози, виклики гібридної війни, розвиток штучного інтелекту та цифрових фінансових інструментів, синхронізації політики з міжнародними стандартами, зокрема NIST Cybersecurity Framework, Директивою ЄС NIS 2 та рекомендаціями НАТО щодо кіберзахисту, та створення єдиного оперативного центру з кібербезпеки, який координуватиме взаємодію державних органів, приватного сектору та міжнародних партнерів.

Перегляд підходів до безпекових відносин між державою і бізнесом, зокрема через створення Національного альянсу кібербезпеки, який включатиме урядові структури, фінансові установи та IT-компанії, запровадження державного регулювання для критичної інфраструктури, включно з обов'язковим моніторингом кіберзагроз, аудитом безпеки та сертифікацією кіберзахисту відповідно до Стратегії розвитку цифрових активів в ЄС, зміцненням захисту від інформаційних та кібератак, шляхом упровадження ефективних механізмів протидії дезінформації та кібершпигунству інтегрує кібербезпеку в систему національної безпеки.

Для підвищення рівня міжнародної співпраці необхідно посилити інтеграцію з кіберструктурами НАТО, зокрема участь у програмах спільних навчань та обмін інформацією про загрози, розширити співпрацю з ЄС у сфері кібербезпеки через програми кіберзахисту фінансових операцій, боротьбу з кібератаками та розслідування злочинів (Регламент DORA).

Укладання міжнародних угод про спільну боротьбу з кіберзлочинністю, зокрема в рамках Глобальної конвенції ООН про кіберзлочинність та Глобального форуму з кібереконономічної безпеки, є механізмами концепції безпекових відносин.

На національному рівні необхідно розробити і впровадити державну програму підвищення цифрової грамотності, яка навчить громадян захищати персональні дані та протидіяти кібератакам, запровадити нові стандарти кіберзахисту для малого та середнього бізнесу, щоб убезпечити їх від хакерських атак і фінансових махінацій, сформувати єдиний центр реагування на інциденти (SOC) для бізнесу, що дасть змогу підприємствам оперативно отримувати аналітику й рекомендації стосовно кіберзахисту.

Актуалізація законодавства щодо відповідальності за кібератаки, шахрайство та зловживання у сфері цифрових технологій, запровадження обов'язкової сертифікації державних органів та компаній у сфері кіберзахисту, впровадження механізму кіберстрахування допоможе підприємствам і

державним установам компенсувати збитки від атак. Ці заходи забезпечать системне вдосконалення державної політики у сфері кібербезпеки, посилять захист критичної інфраструктури, зміцнять міжнародні безпекові відносини та сприятимуть підвищенню цифрової стійкості країни.

Традиційно сектор безпеки монополізований державою і не враховує можливості застосування ППП. Проте в умовах війни та зростання ролі приватного й громадського секторів, зокрема в забезпеченні військових потреб, виникає потреба у формуванні нових підходів до організації безпекової діяльності. Значна частина громадян підтримує ідею залучення приватного сектору до сфери безпеки, високо оцінюючи соціально-правову концепцію такого партнерства. Вони схвально ставляться до впровадження моделі ППП у цій сфері на основі відповідного законодавчого врегулювання [486].

Одним із ключових напрямів розвитку ППП є співпраця у сфері диджиталізації соціально-економічного та культурно-ідеологічного простору України. Важливість новітніх технологій стала очевидною ще у 2020 р., коли під час жорсткого карантину у зв'язку з пандемією коронавірусу суспільство масово перейшло на онлайн-формат взаємодії. Однак за рік війни питання цифровізації публічно-приватних відносин та спрощення процедур стало ще актуальнішим. Це зумовлено тим, що швидкість реагування дедалі частіше визначає можливість збереження людських життів і забезпечення матеріально-фінансових потреб.

Серед переваг ППП в інформаційному просторі можна виокремити:

- вирішення проблем комунікації та покращання інформаційного обміну;
- сприяння створенню нових механізмів для задоволення інтересів громадян;
- формування бази для оперативного відновлення інфраструктури після війни;

- збереження досягнень у цифровій сфері навіть за умов значних руйнувань, оскільки інформація здатна швидко відновлюватися, копіюватися та поширюватися;
- підвищення рівня кібербезпеки, що особливо важливо в умовах гібридної війни;
- позитивний досвід розвинутих країн, який доводить істотну роль ППП у побудові сталої цифрової інфраструктури [487].

Таким чином, диджиталізація через ППП має потужний потенціал для зміцнення як державних, так і громадських інституцій, а також для швидкого відновлення країни після війни.

Новітні технології забезпечили активну громадянську позицію людей з різних країн світу. З початком повномасштабного вторгнення російської федерації в Україну оперативну та дієву допомогу країні було організовано через збір коштів благодійними криптофондами. Водночас така активність, пов’язана з підтримкою українського народу, активізувала злочинний світ, трансакції в якому видавалися за благодійну діяльність. Тому потрібне підвищення стандартів та оперативності у сфері оцінки й управління ризиками та комплаєнсу.

Державне регулювання нових інноваційних індустрій вимагає і реформування підходів державного регулювання шляхом їх цифрової трансформації та впровадження новітніх фінансових технологій. Операції з управління ризиками і дотримання норм є критично важливими для успішного функціонування фінансово-технічних організацій, однак вибір і впровадження відповідних рішень RegTech можуть виявитися непростим завданням.

Підмножина фінансових технологій у сфері регулювання (Regulatory Technology, RegTech) описує інформаційні технології, що забезпечують більш легке, швидке й ефективне виконання регуляторних вимог учасниками фінансових ринків. Суб'єктами RegTech є як учасники фінансового ринку, так і

державні органи, що можуть застосовувати RegTech-контроль за виконанням регуляторних вимог.

Фінансові установи стикаються з численними викликами при інтеграції програмного забезпечення регуляторних технологій [488]. Ці труднощі посилилися в умовах пандемії COVID-19, яка спричинила масовий перехід до мобільного та онлайн-банкінгу, а також через швидкі зміни в регуляторному середовищі. Це створило значні бар'єри для ефективного розгортання таких рішень, що вплинуло на процеси закупівель і операцій організацій.

Попри ці виклики, у контексті постпандемічних ризиків, активного використання регуляторами штучного інтелекту (AI) та аналізу великих даних (Big Data), впровадження інноваційних рішень RegTech є необхідним. Ці технології нового покоління стали ключовим інструментом у забезпеченні відповідності фінансовим вимогам у сучасних умовах.

Починаючи з 2008 р., стрімко зростає кількість регуляторних повідомлень, які організації з дотримання нормативних вимог змушені опрацьовувати. Це зростання супроводжується посиленням ризиків фінансових злочинів, особливо кіберзлочинів, що активізувалися під час пандемії (наприклад, шахрайство в романтичних стосунках). У таких умовах масове впровадження Regtech стало невід'ємною складовою діяльності фінансової індустрії.

Відповідно до звіту Thomson Reuters Regulatory Intelligence за 2021 р. 16 % із приблизно 720 опитаних компаній у всьому світі «впровадили рішення Regtech, а ще 34 % повідомили, що рішення Regtech впливають на управління відповідністю» [489].

Серед основних напрямів використання Regtech можна виокремити: регуляторну звітність, перевірку санкцій, управління ризиками, ідентифікацію, дотримання норм боротьби з відмиванням грошей (ПВК), а також моніторинг трансакцій. Крім того, епоха громіздкого локального впровадження Regtech залишилася в минулому. Ці технології також придатні для криптовалютних

платформ, забезпечуючи відповідність нормативним вимогам для їх користувачів.

Сучасні рішення Regtech майже завжди розгортаються як рішення програмного забезпечення у вигляді послуг (англ. Software as a service, SaaS), повністю розміщених у хмарі, причому багато хто стверджує, що пропонує компонування за принципом «підключай і працюй», доступ до високоякісних даних про ризики та ефективний продукт на основі AI.

Чотири ключові практики, які автор дослідження пропонує фінансовим організаціям для успішної трансформації та інтеграції Regtech:

1. Прогнозування трансформації. Успішна трансформація є міжфункціональним процесом, що передбачає активну участь усіх зацікавлених сторін організації.

2. Розроблення ефективної стратегії управління даними, що має враховувати вимоги сучасних технологій штучного інтелекту (AI) та машинного навчання (ML), щоб оптимізувати функціональність як наявних, так і перспективних IT-інфраструктур. Наприклад, рішення на основі машинного навчання значно полегшують прогнозну оцінку комплаєнс-сповіщень, заощаджуючи час і ресурси.

3. Інвестування в навчання та розвиток персоналу. Фінансовим установам важливо залучати фахівців із відповідними навичками та забезпечувати їх підготовку для ефективного використання Regtech-рішень.

4. Стратегічне планування. Впровадження Regtech вимагає чіткого стратегічного бачення та задокументованого плану дій для досягнення довгострокових результатів.

Сучасні Regtech-рішення здатні перетворювати необроблені дані на значущу аналітику та прогнози, що автоматично інтегруються в діяльність підприємства. Тому фінансові установи повинні оптимізувати свої IT-інфраструктури та хмарні конфігурації для роботи з програмним забезпеченням SaaS.

Для реалізації прогнозування трансформації в управлінні необхідно провести внутрішній аудит поточних процесів та технологій, щоб визначити слабкі місця та можливості для впровадження Regtech, організувати робочі групи за участю керівництва, IT-фахівців, відділів комплаєнсу та ризик-менеджменту для обговорення майбутніх змін, упровадити механізми зворотного зв'язку з персоналом для адаптації трансформаційних процесів у режимі реального часу та використовувати моделювання сценаріїв впливу Regtech на операційну діяльність для оцінки потенційних ризиків і вигід.

У сфері розроблення національними суб'єктами фінансового моніторингу ефективної стратегії управління даними необхідно: визначити ключові джерела даних і вдосконалити єдину платформу їх централізованого збору, обробки та аналізу (ЄДІС) шляхом упровадження технології AI/ML для автоматизації обробки великих масивів даних та ідентифікації підозрілих трансакцій у режимі реального часу; використати API-інтеграції для безперебійного обміну даними між Regtech-рішеннями та внутрішніми системами організації; запровадити автоматичне управління якістю даних (Data Governance), щоб уникнути помилок і знизити ризики регуляторного недотримання.

У сфері стратегічного планування державним регуляторам, національним правоохоронним органам та учасникам фінансових ринків слід мати детальний дорожній план упровадження Regtech, включно з ключовими етапами, відповідальними особами та критеріями оцінки успіху, визначити ключові KPI для оцінки ефективності Regtech-рішень (наприклад, зниження часу на обробку трансакцій або покращання якості комплаєнс-перевірок), інвестувати в хмарні технології (SaaS) для швидкої масштабованості Regtech-рішень та підвищення їхньої продуктивності, регулярно переглядати стратегію відповідно до змін у регуляторному середовищі й технологічних трендах.

Організаціям важливо розробити сучасну стратегію управління даними, яка враховуватиме всі аспекти роботи з ними: приймання, обробку, трансформацію, передачу, зберігання та захист. Глибоке розуміння цих процесів

допоможе уникнути труднощів під час упровадження та експлуатації Regtech-рішень. Крім того, організації повинні враховувати ймовірні проблеми з даними, впроваджувати регулярні процеси очищення та форматування даних, а також створювати структури та команди для управління переміщенням даних між системами і регулятивними юрисдикціями.

Важливим є людський фактор: навіть найкращі технології можуть зазнати невдачі, якщо персонал не вміє ними користуватися. Організації повинні інвестувати в навчання співробітників і залучення фахівців, здатних працювати з Regtech-рішеннями. Наприклад, Goldman Sachs оновив свої процеси, найнявши команду професіоналів для реалізації бізнес-моделі нового покоління. За даними Європейського банківського управління (EBA), фінансові установи повинні залучати науковців та інженерів з обробки даних для ефективного використання й підтримки рішень Regtech. Однак висока конкуренція за таких фахівців на ринку є значним викликом [490].

Інновації у сфері наглядових і регулятивних технологій є ключем до сталого розвитку фінансового ринку, оскільки дають змогу фінансовим установам та регуляторам безперервно вдосконалювати наявні процеси, розширювати коло клієнтів і піднаглядних суб’єктів, а також виявляти й попереджати потенційні ризики у фінансовому секторі.

RegTech-інструменти, спочатку розроблені для банків, почали активно використовуватись і регуляторами. Яскравим прикладом є платформа Abacus від консалтингової компанії BearingPoint, призначена для стандартизації звітування як у банках, так і в регуляторних органах [491]. Цей підхід демонструє, як спільне прагнення спростити й підвищити ефективність регуляторної звітності трансформує програмні рішення із суто банківських у двосторонні. Інструменти, спочатку створені для полегшення роботи банків, отримують інтерфейси для регуляторів, що дає їм можливість не лише отримувати належним чином верифіковані дані, а й користуватися потужними інструментами для аналізу та консолідації.

Одним із найуспішніших рішень у сфері RegTech сьогодні є комерційна платформа AuRep, яка об’єднує 90 % банків Австрії. Вона побудована на основі платформи Abacus. Основний принцип її роботи полягає у створенні спільного інтерфейсу звітності для банків і регуляторів. Замість численних таблиць система оперує безпосередньо даними, що значно підвищує зручність і ефективність звітності.

Щороку зростає кількість регуляторів, які вже розробили або активно розробляють стратегії у сфері SupTech та RegTech. Окремі з них уже мають офіційні платформи для створення та тестування інструментів SupTech і RegTech, а також спеціалізовані підрозділи для підтримки їхнього розвитку. Обмін досвідом на міжнародному рівні сприятиме швидкому впровадженню новітніх технологій управління, що є стратегічною метою діяльності Міністерства цифрової трансформації та Кабінету Міністрів України загалом.

Наглядові технології (англ. Supervisory technologies, SupTech) спрямовані на оптимізацію, спрощення та вдосконалення процесів нагляду відповідними органами. Ці інструменти допомагають ефективно виконувати свої функції та адміністративні завдання.

SupTech, як і RegTech, виникли внаслідок швидкого розвитку фінансових технологій (FinTech), оскільки цей сектор вимагає від регуляторів адаптації своїх підходів до нових умов (контролювати інноваційні продукти складніше). Варто зазначити, що SupTech є рішенням для більш автоматизованого й алгоритмізованого нагляду та регулювання діяльності у сфері ПВК/ФТ наявних фінансових установ та їхніх продуктів. Таким чином, розвиток наглядових технологій традиційно не випереджає, а йде слідом за FinTech-сферою.

Уявімо, що регулятор отримує дані від одного банку, деталізовані по 100 відділеннях за 30 днів і трьох валютах. Наприклад, інформацію про стан виявлення ризиків злочинного використання ВА (обмінні криптовалютні операції) подають у вигляді не 1800 таблиць (100 х 30 х 3), а одного масиву, що містить 18 тисяч чисел. Кожне число має унікальний ідентифікатор (номер

відділення, день, валюта, категорія ВА та сума), що дає змогу миттєво аналізувати динаміку будь-якого відділення, регіону чи їх сукупності у будь-якому часовому проміжку та для будь-якої категорії клієнтів. Завдяки цьому більше немає потреби вручну відкривати тисячі таблиць або будувати складні алгоритми для вилучення даних: інформація подається в максимально деталізованому форматі, що дає змогу створювати різноманітні зрізи та комбінації.

Орієнтований на дані підхід відомий як data-centric, на відміну від template-based методів звітності, що базуються на використанні шаблонів таблиць і є значно складнішими для обробки. Усі дані проходять перевірку й накопичуються у так званому базовому кубі (basic cube), який можна «обертати» у будь-яких проєкціях для аналізу. Основні переваги такого підходу — єдиний стандарт звітності для всієї системи, контроль якості вхідних даних та можливість спільно з регулятором визначати єдиний стандарт подання фінансової інформації. Чистота даних, швидкість їх обробки, висока якість та значне скорочення витрат як для банків, так і для регуляторів — ключові переваги цих систем.

У Національному банку України data-centric підхід застосовується з 1999 р., коли було докорінно переосмислено систему банківської статистики та звітності. Тож український регулятор уже багато років упроваджує ініціативи, які відповідають концепції SupTech/RegTech. Водночас аналіз міжнародного досвіду показав, що на сьогодні не існує готових універсальних рішень зі стратегії впровадження таких технологій для центральних банків. У грудні 2018 р. НБУ розпочав проєкт упровадження наглядових технологій, який наразі перебуває на пілотному етапі.

Регулятори, зокрема Національний банк, вважають, що одночасне сприяння розвитку SupTech та RegTech повинне ґрунтуватися на постійній взаємодії та співпраці з піднаглядними суб’єктами і RegTech-компаніями. Це є необхідною умовою формування єдиного бачення щодо застосування цих технологій, визначення їхньої ролі та пріоритетності в реалізації.

Упровадження SupTech і розвиток RegTech також є однією з ключових цілей Національного банку, визначених у Стратегії розвитку фінансового сектору до 2025 року [492], Стратегії розвитку FinTech в Україні до 2025 року [493] та Стратегії Національного банку України до 2025 року [494], які були оновлені у зв'язку з введенням воєнного стану у 2022 р. через неспровоковану російську агресію в Україні [495].

Розвиток FinTech вимагає від регуляторів фінансових ринків і наглядових органів перегляду підходів та методів оцінки ризиків, оскільки нові фінансові продукти часто є складними для розуміння і контролю. SupTech, можна сказати, виник як відповідь на виклики, що супроводжують розвиток FinTech. Проте таке твердження є лише частково точним, адже наглядові органи та регулятори застосовують SupTech/RegTech рішення переважно для автоматизації й оптимізації процесів регулювання та контролю наявних фінансових продуктів і установ (рис. 4.2).

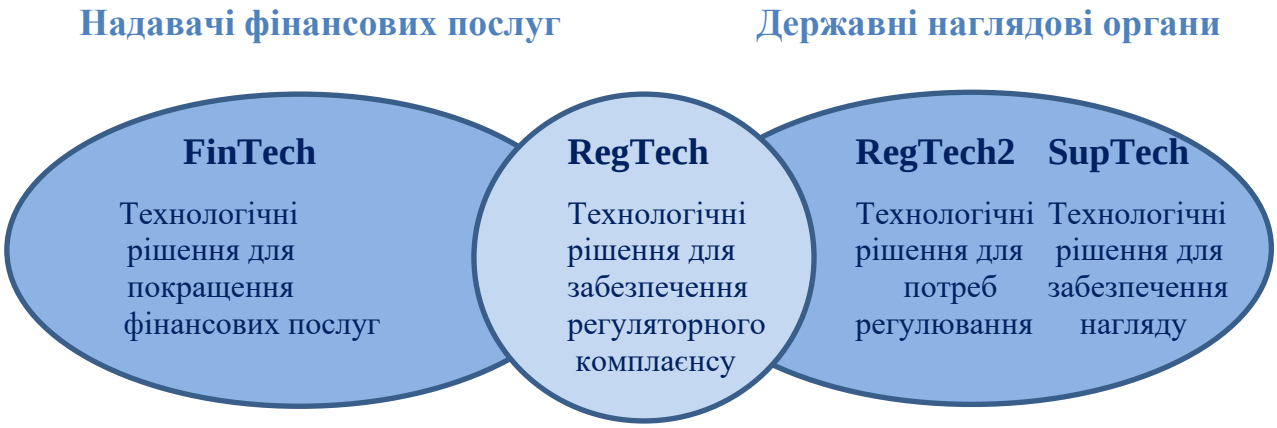


Рис 4.2. Співвідношення застосування фінансових технологій публічним і приватним сектором.

Джерело: складено автором

SupTech можна охарактеризувати як сукупність технологій, що використовуються регуляторами для виконання своїх функцій і виконання адміністративних завдань. Найчастіше SupTech асоціюють із упровадженням рішень сучасних аналітичних платформ (Business Intelligence) для потреб

нагляду, але його застосування не обмежується лише цим. Наприклад, є SupTech-рішення, які завдяки використанню технологій розподіленого реєстру, таких як блокчейн, запобігають шахрайству шляхом цифровізації певних реєстрів і процесів.

Ефективне управління ризиками, використання кваліфікованих інструментів комплаєнсу та боротьби з відмиванням грошей (ПВК) дають змогу забезпечувати безпеку даних, виявляти підозрілу активність і запобігати шахрайству, що є критично важливим у сучасному фінансовому середовищі [496].

Управління ризиками та дотримання законодавства про ПВК/ФТ є ключовими елементами діяльності будь-якої FinTech-компанії. Вони не лише обов'язкові, а й сприяють істотному зменшенню втрат від шахрайства, що, у свою чергу, підвищує загальний дохід компанії.

Швидке зростання FinTech-сектору за останні роки створило конкурентне середовище для впровадження рішень, що ідеально підходять для тих, хто прагне вдосконалити свої FinTech-платформи. Сучасні інструменти управління ризиками та дотримання нормативних вимог стали більш комплексними, забезпечуючи швидку й безперебійну інтеграцію.

Далі наведено основні причини, чому управління ризиками та дотримання нормативних вимог є критично важливими для успіху FinTech-бізнесу:

1. *Захист даних.* Забезпечення безпеки клієнтів і всієї платформи є першочерговим завданням. Вкрай важливо гарантувати, що всі дані, зокрема користувацькі, залишаються захищеними від будь-яких загроз.

2. *Дотримання законодавства про ПВК/ФТ.* Установи повинні суворо дотримуватись ПВК-вимог, щоб попередити випадки відмивання коштів і забезпечувати відповідність чинному фінансовому законодавству.

3. *Протидія підозрілій діяльності.* Своєчасне виявлення, обробка та подання звітів про підозрілі трансакції до відповідних органів є надзвичайно

важливими. Затримка в цьому процесі може призвести до значних штрафів і свідчити про недотримання регулятивних норм.

4. *Підготовка до кризових ситуацій.* Ефективне управління ризиками передбачає готовність до наймасштабніших та найруйнівніших атак, а також здатність швидко реагувати на порушення безпеки, що можуть вплинути на роботу платформи чи дані клієнтів.

5. *Зміцнення довіри клієнтів*. Забезпечення безпеки, прозорості та надійного захисту від шахрайства позитивно впливає на лояльність клієнтів і їхню довіру до платформи, що є ключовим фактором для довгострокового успіху.

Бездоганну інтеграцію з наявними FinTech-технологіями, що дає змогу швидко розширювати можливості платформи, забезпечують такі рішення для управління ризиками та дотримання нормативних вимог:

1. Моніторинг трансакцій є критичним для виявлення та запобігання ризикам. Такі рішення допомагають отримувати доступ до різних джерел даних для виявлення підозрілої активності. Завдяки автоматичним сповіщенням і зупинкам у реальному часі вдається швидко реагувати на спроби шахрайства. Ці рішення забезпечують дотримання стандартів боротьби з відмиванням коштів і надають гнучкі налаштування для моніторингу трансакцій, що дає можливість вчасно виявляти підозрілі операції для подальшого перегляду. Технології, які дозволяють тестувати та налаштовувати ці правила в ізольованому середовищі, допомагають зменшити кількість помилкових спрацьовувань після розгортання.

2. З огляду на велику кількість повідомлень та розслідувань, важливо мати централізовану систему управління загальною кількістю справ. Програмне забезпечення для управління справами ПВК забезпечує зручний доступ до всіх необхідних даних через єдину панель керування, автоматизує подання електронних Звітів про підозрілі операції (англ. Suspicious Transaction Report, STR), а також дозволяє дослідникам швидко переглядати інформацію та приймати рішення завдяки візуалізації даних і контрольним журналам, що

допомагає забезпечити відповідність вимогам і запобігає пропуску важливих подань, знижуючи ризик штрафів та санкцій.

Додаток goAML — це повністю інтегроване програмне рішення, що розроблене спеціально для використання ПФР і є одним зі стратегічних заходів відповіді УНП ООН на фінансові злочини, включно з ВК/ФТ [497]. Підрозділи фінансової розвідки відіграють провідну роль у будь-якому режимі боротьби з відмиванням грошей, оскільки зазвичай відповідають за отримання, обробку та аналіз звітів, наданих фінансовими установами чи іншими організаціями згідно з національним законодавством про боротьбу з ВК. Такі звіти та інша інформація, зібрана ПФР, часто є основою для розслідування відмивання грошей, фінансування тероризму та інших серйозних злочинів. goAML спеціально розроблено для задоволення потреб будь-якого підрозділу фінансової інформації щодо збору даних, управління, аналітики, документообігу, документообігу та статистики. Додаток goAML розроблено Службою інформаційних технологій УНП ООН у партнерстві з Глобальною програмою УНП ООН проти відмивання грошей, доходів від злочинів і фінансування тероризму (GPML UNODC).

Національним органам із реалізації стратегії та політики ПВК/ФТ (МФУ) і координації роботи Національної системи ПВК/ФТ (Держфінмоніторинг України) доцільно впровадити в діяльність учасників системи новітні технологічні розробки міжнародних організацій шляхом посилення взаємодії та співпраці з установами, що опікуються реалізацією політики ПВК/ФТ.

3. Належне управління ризиками є ключовим для успішного комплаєнсу всіх учасників фінансового та крипторинків – суб’єктів первинного фінансового моніторингу і ВНУП. Воно передбачає налаштування порогових значень для моніторингу трансакцій та оцінки ризиків, які можуть виникнути під час операцій. Адаптивні рішення повинні збалансувати ризики при верифікації нових користувачів, забезпечуючи одночасно ефективний контроль за шахрайськими акаунтами та мінімізацію відмов для легітимних користувачів. Це

важливо для синхронізації інших рішень і забезпечення ефективної оцінки ризиків.

4. Надійне рішення для виявлення та запобігання шахрайству повинне забезпечувати швидку реакцію на шахрайську діяльність, припиняти її на ранніх етапах і сповіщати про будь-яку підозрілу активність, що не була зупинена автоматично.

5. Для забезпечення успішного функціонування платформи необхідна ефективна команда, здатна швидко адаптуватися до змін. Для сприяння розвитку бізнесу потрібне рішення, яке не лише відповідає вимогам боротьби з відмиванням коштів, а й оптимізує взаємодію з користувачами, зокрема для нових клієнтів. Це важливо, оскільки при реєстрації користувачів повинна здійснюватися належна перевірка за допомогою джерел ЗСК і ЗСТ. Це дає змогу забезпечити відповідність вимогам ПВК і знижує ймовірність шахрайської діяльності на платформі.

6. Попри всі зусилля щодо мінімізації ризиків шахрайства та відмивання коштів на платформі, спроби шахрайства залишаються неминучими. Звіти про підозрілу діяльність STR є невід'ємною частиною процесу моніторингу, і відповідні рішення мають на меті відстеження підозрілої активності, сповіщення фінансової установи про потенційні загрози та автоматизацію процесу управління справами та подання документів. Це важливо, оскільки неможливо уникнути подання звітів STR, і доцільно зводити процес до максимальної автоматизації. Високоякісні рішення для моніторингу в поєднанні з ефективними інструментами управління справами полегшують виявлення підозрілої діяльності, скорочують час на розслідування та покращують аналіз даних через передові методи візуалізації. Крім того, автоматичне подання електронних файлів істотно заощаджує час співробітників.

7. Незважаючи на те, що керівник комплаєнсу не є фізичною частиною технічного рішення, він повинен мати змогу взаємодіяти з такими рішеннями, сприяючи реалізації потреб управління ризиками та комплаєнсу. Керівник

комплаєнсу є невід'ємною частиною системи, сполучною ланкою, що забезпечує інтеграцію всіх компонентів і сприяє ефективному функціонуванню організації. Це важливо, оскільки досвідчений фахівець із ПВК гарантує, що підрозділ, відповідальний за боротьбу з відмиванням коштів, буде проінформований про всі нормативні акти, застосовувані до конкретного бізнесу, та впроваджуватиме робочі процеси, які забезпечують дотримання вимог при розробленні нових продуктів і послуг.

8. Ризик та комплаєнс є взаємопов'язаними, але не ідентичними поняттями, і вони вимагають постійного аналізу ринкових умов та оновлення технічного забезпечення організації. Оскільки нормативні вимоги до боротьби з відмиванням коштів і схеми шахрайства постійно змінюються, фінансові установи повинні постійно оновлювати свої стратегії для ефективного управління ризиками та забезпечення відповідності законодавству. Це важливо, оскільки зміни в регуляторному середовищі можуть створювати нові загрози, що вимагають негайної адаптації. Тому компанія повинна мати професіонала, котрий відстежує ринкові тенденції, або використовувати автоматизовані рішення, що регулярно оновлюються, для відповідності актуальним вимогам боротьби з ВК і шахрайством.

Фінансові установи та ППВА повинні звітувати перед кількома сторонами, включно зі своїми клієнтами, які користуються банківськими послугами, а також державні органи, що здійснюють нагляд та регулювання їхньої діяльності (і, у разі потреби, можуть притягнути до відповідальності). У певних випадках, особливо коли йдеться про можливу злочинну діяльність, це може призвести до конфлікту інтересів.

Таким чином, фінансові установи несуть «подвійну відповідальність». Дотримання високих стандартів конфіденційності покращує відносини з клієнтами, тоді як співпраця з правоохоронними органами та подання звітів STR зміцнюють їхні зв'язки з урядом. У кінцевому підсумку пошук оптимального

балансу між цими «конкуруючими» обов'язками принесе користь усім сторонам, що беруть участь.

Фінансові установи можуть захищати своїх клієнтів, співпрацювати з державними органами та підтримувати організаційну цілісність, застосовуючи найкращі методи, зазначені вище, і поліпшуючи декларування STR.

Розвинута цифрова економіка разом з ефективним наглядом важливі для подолання перешкод до фінансової інклюзії та відкриття нових шляхів економічного та фінансового розвитку для підтримки зростання і зменшення бідності. Приклади містять розширення доступу до фінансів із одночасним зниженням витрат, створення нових шляхів залучення капіталу, надання нових інформаційних послуг для оцінки ризиків і стимулювання бізнесу. Для досягнення цих цілей питання FinTech мають бути частиною національних стратегій фінансової інклюзії та цифрової грамотності з активним обміном знаннями між державним і приватним секторами, громадянським суспільством та іншими учасниками.

Швидкий розвиток FinTech вимагатиме покращання моніторингу для досягнення цілей державної політики та уникнення збоїв у фінансовій системі. Допоможуть мінімізувати ризики збоїв у фінансовій системі, посилять довіру до FinTech-рішень та забезпечать стабільність державної фінансової політики упровадження автоматизованих систем аналізу та моніторингу трансакцій у реальному часі для виявлення аномальних фінансових операцій і шахрайства, розвиток механізмів міжвідомчої взаємодії органів державної влади, впровадження гнучких нормативних вимог, що дають змогу швидко адаптуватися до змін у FinTech-середовищі та забезпечити прозорість FinTech-компаній, використання блокчейн-технологій для створення надійних механізмів підтвердження фінансових операцій, упровадження вимог до відкритої звітності та аудитів для компаній, що працюють із цифровими активами та платіжними системами, регулярне тестування систем безпеки й підготовка до сценаріїв потенційних кіберзагроз.

Варто забезпечити постійний діалог з індустрією — як з новаторами, так і з традиційними гравцями — для своєчасної реакції на можливості та ризики.

4.3. Посилення фінансово-цифрової інклюзії в умовах розвитку ринку цифрових активів як складова ПВК/ФТ

У попередніх розділах дисертації автором наголошено на стрімкому зростанні фінансових ризиків, які виникають через недостатню обізнаність користувачів. Проаналізовано ключові аспекти інвестиційної грамотності, необхідні для ефективної роботи на криптовалютному ринку, включно з розумінням природи криптовалют, основних механізмів торгівлі, управління ризиками та безпеки, проведено докладний огляд літератури, пов'язаної з інвестиціями, фінансовою й цифровою грамотністю на ринку криптовалют. Аналіз виявив, що в Україні наукові дослідження щодо розвитку крипторинку є фрагментарними, а питання інвестиційної грамотності на ньому поки що не розглядаються вітчизняними дослідниками. Однак, з огляду на стрімкий розвиток крипторинку та поширення на ньому шахрайських схем, дослідження в цій сфері стають дедалі актуальнішими. Особливу увагу автором приділено необхідності вивчення технічних і фундаментальних аспектів криптовалютних активів, а також розвитку навичок критичного мислення для оцінки потенційних інвестицій. Регуляторні заходи, спрямовані на захист інвесторів і створення прозорих правил на ринку криптовалют, також мають вирішальне значення. Освітні програми й підвищена доступність навчальних матеріалів є важливими для мінімізації ризиків для новачків. Таким чином, дослідження підкреслює ключову роль інвестиційної грамотності у формуванні стабільної фінансової поведінки учасників крипторинку та посиленні їхньої здатності досягати успіху в ринкових умовах, що швидко змінюються.

Превентивна діяльність у сфері ПВК/ФТ є складовою впровадження ризик-орієнтованого підходу до операцій з ВА (Рекомендації 1, 15 FATF), що значно оптимізує ресурси шляхом запровадження освітніх заходів порівняно з витратами, необхідних для розслідування злочинної діяльності.

Тому для успішної роботи органів нагляду та фінансових і криптоустанов необхідно підготувати працівників до роботи з криптоактивами через постійне вдосконалення їхніх компетенцій. З урахуванням кількості банківських установ та афілійованих із ними фінансових організацій, актуалізується необхідність оперативної підготовки щонайменше тисячі профільних спеціалістів.

Враховуючи досвід автора в реалізації навчальних програм у межах проєктів Програми розвитку ООН та Організації з безпеки і співробітництва в Європі, обґрунтовано доцільність використання практико-орієнтованої моделі підвищення кваліфікації. Така модель передбачає інтеграцію практичних завдань із застосуванням реальних криптовалютних активів та професійного програмного забезпечення, що забезпечує формування прикладних компетентностей, необхідних для здійснення ефективного фінансового моніторингу в умовах цифровізації фінансового сектору. Це дасть змогу фахівцям набути необхідних навичок для ефективного моніторингу та управління ризиками у сфері криптоактивів.

Міжнародні та державні організації дедалі більше співпрацюють із представниками приватного сектору, а саме фахівцями криптоіндустрії, у сфері аналізу ризиків використання криптоактивів у злочинних операціях. Це міжнародні аналітичні компанії, котрі розробляють і вдосконалюють безперервно в часі програмні продукти дослідження операцій у блокчейні. Серед визнаних компаній за останні п’ять років відзначені Chainalysis Reactor, Elliptic, Crystal, CipherTrace, Certik, Global Ledger, AMLbot, Purifi, Lukka Data Solutions (Coinfirm), Slowmist [287 -290, 424-428].

Не можна однозначно віддати належне одній із перелічених компаній, тому що всі вони мають свої переваги в певний час і в конкретній ситуації. Для

досконалого дослідження (розслідування) часто необхідно використовувати не один програмний продукт. Але з огляду на значну вартість (100–300 тис. дол. США на рік) отримати ліцензії на певну кількість програмних продуктів часто проблематично, особливо для державних органів влади, правоохоронної та судової системи.

Наявність програмного забезпечення вимагає обізнаного персоналу, що викликає потребу в додаткових ресурсах на навчання та підвищення кваліфікації. Саме завдяки проведенню розслідувань збирається доказова інформація для правоохоронних і судових органів, здійснюється регуляторний нагляд за постачальниками послуг, пов’язаних з оборотом віртуальних активів. Інструменти аналізу блокчейну підтримали та використовують успішні правоохоронні органи [424].

Європол також пропонує правоохоронним органам розробити стандартні операційні процедури для роботи з цифровими доказами та захисту конфіскованих активів, а засоби візуалізації можуть допомогти прокурорам стежити за грошима [230]. Однак пом’якшення ризиків, пов’язаних із незаконним використанням криптовалют, вимагає від країн не лише зусиль для підвищення обізнаності, а й суттєвих заходів для прийняття відповідного законодавства у сферах внутрішнього та міжнародного кримінального права.

Як працівники органів нагляду у сфері ПВК/ФТ суб’єктів державного та первинного фінансового моніторингу, представники правоохоронних та судових органів, які входять в Національну систему ПВК/ФТ, повинні знати, як працювати з процедурами комплаєнсу та ПВК/ФТ у сфері ВА. З огляду на масштаб охоплення персоналу, залученого до реалізації процедур на всіх рівнях регулювання ринку віртуальних активів, виникає об'єктивна потреба у забезпеченні цільової підготовки близько тисячі фахівців у стислі часові рамки. Такий підхід є критично важливим для належного функціонування системи регулювання та нагляду в умовах стрімкого розвитку цифрових фінансових інструментів. Зазвичай питаннями навчання певних секторальних суб’єктів

фінансового моніторингу займаються державні регулятори. Однак у випадку з оборотом ВА та ризиками, які вони спричиняють у сфері ВК/ФТ та іншої злочинної діяльності, доцільно не тільки розробити освітні програми для державних правоохоронних, наглядових, судових органів, а й забезпечити навчанням заклади середньої та вищої освіти, освіти для дорослих. Отже, це має бути розроблення освітніх програм Міністерством освіти і науки України разом з відповідальним за стратегію і політику розвитку Національної системи ПВК/ФТ органом (Міністерство фінансів України), координатором роботи системи – Державною службою фінансового моніторингу України, суб'єктами державного фінансового моніторингу – НКЦПФР та НБУ, які є державними наглядовими органами ринку ВА, Міністерством цифрової трансформації України, яке відповідальне за стратегію розвитку цифрової трансформації держави, в якому освіта є невідокремлюваною складовою.

Необхідно зазначити, що Мінцифри активно та постійно займається просвітницькою роботою у сфері діяльності крипторинку з 2020 р. На платформі «Дія. Освіта» викладено кілька проєктів щодо діяльності крипторинку, професій у Web3 різних років. У рамках співпраці з УНП ООН за результатами серії виконаних проєктів УНП ООН та ОБСЄ для представників державних наглядових та правоохоронних органів України з 2019 по 2024 р. було організовано передачу онлайнової тренінгової платформи з протидії використання ВА в злочинній діяльності [468; 502].

Тренінг включає практичні вправи з блокчейном із використанням аналітичних програм (індивідуальні навчальні ліцензії Chainalysis, Crystal, Global Ledger, AML-bot [424; 286–288]) у режимі реального часу на навчальній онлайн-платформі УНП ООН. Курс триває п'ять днів, складається переважно з практичних завдань із реальними об'єктами, навчання проводиться з 2016 р.

Власне програмне забезпечення є відносно простим, багатьом установам достатньо отримати доступ через інтернет-браузер («software as a service»). З досвіду тренінгових програм УНП ООН випливає, що вистачає кількох днів

навчання для самостійного аналізу криптоактивів за допомогою програмного забезпечення (рис. 4.3).

Навчання може проводитись як очно, так і дистанційно. Усі навчальні матеріали розміщені на електронній платформі та доступні учасникам у режимі онлайн. Курс, протестований на невеликій групі українських банкірів, працівників НБУ, Держфінмоніторингу та правоохоронців, отримав схвальні відгуки.

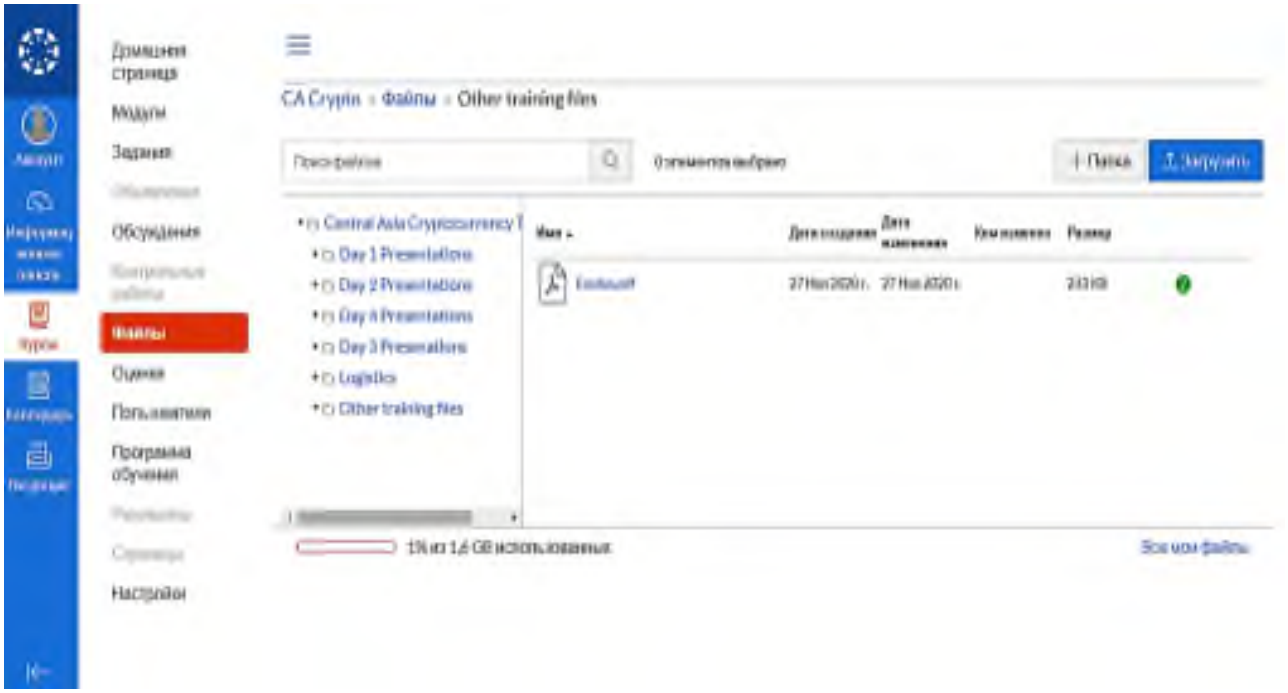


Рисунок 4.3 Навчальний електронний курс УНП ООН з протидії використання криптоактивів в злочинних операція

Джерело: за матеріалами [468; 502]

Успішний проєкт потребує координації з боку органів нагляду – НБУ та НКЦПФР, а також участі Держфінмоніторингу. Найефективнішим підходом є створення національного курсу:

УНП ООН проводить пілотне навчання та навчання групи національних тренерів;

національні тренери за допомоги УНП ООН проводять початкове навчання;

у подальшому основний обсяг навчання здійснюється національними

тренерами та на базі національної навчальної установи;

УНП ООН періодично оновлює зміст власного курсу та допомагає національним тренерам внести відповідні зміни до національного курсу.

Окрім підвищення обізнаності правоохоронних органів у країнах-партнерах про ризики, пов'язані з криптовалютами, агенції з розвитку можуть привернути увагу урядів-донорів до необхідності регулювання галузі, щоб запобігти шкідливим наслідкам у країнах із низьким і середнім рівнем доходів. Нарешті, агенції розвитку також можуть розглянути можливість фінансування інформаційних кампаній у країнах-партнерах, щоб підвищити знання громадян про ризики інвестування своїх заощаджень у криптовалюту.

Часовий тиск для розслідувачів помітно посилюється при роботі з ВА, оскільки трансакції можуть бути здійснені протягом кількох хвилин, що вимагає швидких дій для обмеження або заморожування активів [230].

Щоб полегшити процедури та підвищити ефективність заморожування та конфіскацію ВА, Робоча група з кримінальних фінансів і криптовалют Базельського інституту управління, Європол та Інтерпол рекомендують розглядати криптовалюти як традиційні активи, такі як ювелірні вироби чи твори мистецтва [247]. Міжнародні експерти підкреслили, що впровадження вже встановлених практик повернення активів, таких як планування перед конфіскацією та державно-приватна співпраця, було дуже ефективним у кількох юрисдикціях, надавши змогу повернути значні суми криптовалют, які в подальшому можна конвертувати у фіатну валюту через аукціони чи біржі [248].

На думку автора, такий підхід не тільки допомагає відновити вкрадені кошти, а й діє як стримуючий фактор для потенційних злочинів з використанням ВА у сфері ВК/ФТ. Крім того, автор рекомендує усунути розбіжності між державними установами, які працюють з традиційними фіатними грошима та ВА, щоб підвищити ефективність заходів ПВК/ФТ. Ефективна співпраця між державним і приватним секторами може виявитися важливою для запобігання зникненню активів під час поточного

розслідування.

Згідно із заявою згаданої Робочої групи з кримінальних фінансів і криптовалют, приватний сектор має потенціал стати союзником правоохоронних органів, допомагаючи в розробленні та використанні інноваційних технологій для відстеження коштів у криптоактивах. У цьому плані криптобіржі та інші ППВА мають потенціал для підтримки розслідувань правоохоронних органів шляхом обміну інформацією, технічними можливостями, а також інструментами для аналізу даних і моніторингу в реальному часі. Наприклад, вони можуть створювати спеціальні відділи для координації запитів від національних органів влади, обмежувати доступ злочинців до активів або блокувати підозрілі злочинні активи.

Міжнародні організації розвитку, правоохоронні органи та неурядові організації можуть відігравати важливу роль у активних пошуках створення механізмів для співпраці та обміну інформацією, використовуючи існуюче публічно-приватне партнерство як платформу для обміну інформацією та зміцнення довіри. Для прикладу наведемо організовані заходи з видалення сайту експлуатації дітей «Welcome to Video» і численні міжнародні арешти, які стосувалися понад 1,3 млн біткоїн-адрес і тисячі біткоїн-платежів, що підкреслює успішний результат співпраці між державним і приватним секторами, оскільки Міністерство юстиції США використовувало програму Chainalysis у своєму дослідженні [423].

Упровадження превентивних заходів у сфері ПВК/ФТ є ключовим інструментом для зниження ризиків незаконного використання криптоактивів та економії ресурсів держави, фінансових установ і учасників ринку. Одним із найефективніших механізмів у цьому контексті є розроблення та впровадження освітніх програм фінансової та цифрової інклюзії, які сприяють підвищенню рівня знань про фінансові технології, механізми ризик-орієнтованого підходу та вимоги законодавства.

Превентивна діяльність зменшує потребу в ресурсозатратних процесах виявлення порушень та реагування на них. Навчання учасників ринку дає їм можливість уникати ризиків ще на початковому етапі, що скорочує кількість випадків фінансових злочинів та необхідність розслідувань. Розуміння ризиків і відповідних механізмів їх мінімізації допомагає ефективніше впроваджувати заходи з ПВК/ФТ, що робить фінансову систему стійкішою.

Освітні заходи допомагають учасникам крипторинку виявляти та запобігати шахрайським схемам, нелегальному використанню криптоактивів, а також сприяють зменшенню кількості випадків фінансових злочинів. Поширення знань про безпечне використання криптовалют і відповідальне ведення бізнесу сприятиме підвищенню довіри з боку інвесторів та міжнародних партнерів, що допоможе подальшій інтеграції України у світовий фінансовий простір.

Однак треба зазначити, що прискорення розвитку цифрових технологій виявило непідготовленість громадян до життєдіяльності в цифровій реальності. За даними дослідження EU4Digital 2019 р., цифрова грамотність 53 % громадян України була нижчою від базового рівня, проблеми виникали навіть з офісним програмним забезпеченням (робота у Word, Excel, редагування фотографій і відео, створення презентацій тощо). Також у менше ніж 50 % громадян України є навички оплати комунальних послуг, поповнення рахунку мобільного телефону, переказу грошей із картки на картку онлайн, перегляду відео, прослуховування музики, купівлі товарів через інтернет, проходження онлайн-курсів та інші навички, які стали необхідними в сучасному світі. Згідно з тим самим дослідженням, упродовж року 34 % українців стали жертвами шахрайських дій через інтернет та лише 11 % можуть розпізнати неправдиву інформацію в мережі [500].

Рівень фінансової грамотності в Україні теж залишається невисоким (58,6 % можливого максимуму), що спричиняє чималі грошові втрати домогосподарств на ринку фінансових послуг. Зокрема, дослідження в рамках

проєкту USAID «Трансформація фінансового сектору», виявило вразливі групи споживачів фінансових послуг. За віком це молодь і особи похилого віку; за рівнем доходу – особи з нижчим за середній рівень доходу; за рівнем освіти – особи з неповною середньою та середньою освітою [501].

У свою чергу, здійснення трансакцій на ринку ВА (криптовалюти) передбачає для учасників поєднання навичок фінансової й цифрової грамотності. Тому нагальним питанням є фінансова та цифрова інклюзія населення, що зумовлює пошук підходів і механізмів розв'язання окреслених проблем. Саме цьому питанню присвячено публікацію, метою якої є пошук підходів та механізмів підвищення рівня освіти у сфері кібербезпеки, фінансової й цифрової грамотності як чинник зменшення ризиків діяльності крипторинку [501].

Огляд наукової літератури з питань фінансової грамотності свідчить про інтерес науковців до зазначеної проблематики, а також про розуміння ними важливості проведення відповідних досліджень, особливо в країнах, що розвиваються. Передусім наукові публікації мають на меті оцінювання взаємозв'язку фінансової грамотності та поведінки споживачів фінансових послуг, зокрема на інвестиційних ринках (у т. ч. інвестицій у криптоактиви).

Так, індійські дослідники підкреслюють складність оцінки впливу фінансової грамотності на фінансові результати інвестування. Проте вони намагаються визначити рівень такої грамотності роздрібних інвесторів у Делі та з'ясувати, чи є якась істотна різниця в її оцінках між тими, хто відвідував тренінги/програми з підвищення фінансової грамотності, й тими, хто цього не робив. За результатами статистичного аналізу, середній показник фінансової грамотності тих, хто відвідував такі програми, значно відрізняється від показника тих, хто не брав участі в них [502]. Також індійські дослідники наголошують, що фінансова грамотність є життєво важливою навичкою для молоді. Її рівень серед учнів середньої школи в Індії виявився нижчим за стандартні показники. Частка правильних відповідей із базового рівня фінансової грамотності становить 45 %, а з просунутого – 44 %. Виявилося, що

рівень фінансової грамотності в Індії нижчий, ніж у розвинутих країнах світу [503]. Зауважимо, що в Україні таких досліджень серед учнів закладів загальної середньої освіти не проводилося, хоча, на нашу думку, вони мають велике значення.

Досить цікавими є дослідження поведінкових і культурних особливостей у сфері альтернативних фінансів, які спонукають людей до використання криптоактивів у електронній комерції. Справді, незважаючи на те, що використання ВА для електронної комерції поширюється по всьому світу швидкими та зростаючими темпами, серед їхніх користувачів є як прихильники, так і противники. Аналіз відмінностей між цими двома групами фундаментальний для розуміння їхніх намірів щодо використання криптоактивів для електронної комерції. Відповідне опитування було проведено серед 2532 користувачів криптоактивів у США й Китаї, при цьому збиралися дані про їхні поведінкові схильності та культурні особливості. Результати показали, що ставлення, суб'єктивні норми, уявний контроль поведінки й стадна поведінка впливають на намір використовувати криптоактиви для електронної комерції, а рівень фінансової грамотності – ні [504].

Учені зазначають, що в перетворенні глобальної валютно-фінансової системи виникла точка біфуркації, пов'язана з її подальшою цифровою трансформацією, що великою мірою залежить від бажання економічних агентів використовувати віртуальні активи. Зокрема, автори дослідження щодо ролі фінансової грамотності поставили мету проаналізувати чинники, котрі визначають ставлення суб'єктів господарювання до цифрових активів і вплив такої грамотності на застосування цих інструментів як об'єкта інвестування й засобу платежу. Це дослідження одним із перших виявило відмінності в оцінці знань та готовності до використання цифрових активів студентами фінансового й нефінансового профілю, а також підтвердило адекватну оцінку ризиків і можливостей ВА різних типів, якщо студенти мають фінансові знання. Автори дійшли висновку, що низька фінансова та цифрова грамотність населення може

створити психологічний бар'єр для використання цифрових активів, ускладнюючи їх легалізацію в національних грошових системах. Водночас відсутність фінансової грамотності призводить до перебільшення сприйняття своїх знань учасниками ринку криптоактивів [505].

Становить інтерес стаття, у якій розглядаються характеристики індонезійських криптоінвесторів, а також досліджується вплив їхньої впевненості та фінансової грамотності на ймовірність здійснення таких інвестицій. Вибірка охоплювала 339 інвесторів, котрі вкладають кошти в різні фінансові активи, включно з цифровими криптоактивами. Авторами застосовано пробіт-регресію для аналізу зв'язку між довірою і грамотністю інвесторів щодо інвестицій в інструменти крипторинку. Отримані результати свідчать про те, що «середні» криптоінвестори в Індонезії, ймовірно, є надто самовпевненими та нехтують ризиками, пов'язаними з інвестуванням у ці інструменти. Крім того, результати показали, що «середні» інвестори в криптоактиви – це, як правило, молоді люди зі ступенем бакалавра [506].

Інші науковці теж вивчають питання фінансової грамотності, а саме те, наскільки поведінка криптоінвестора залежить від інвестиційного досвіду, який фактор більше впливає на прийняття рішень щодо інвестування. Так, дослідження з використанням вибірки індивідуальних інвесторів США показало: хоча й фінансова грамотність, й інвестиційний досвід позитивно впливають на прийняття рішень щодо інвестування в криптоактиви, інвестиційний досвід усе-таки має більшу вагу. Отримані дані теж засвідчили, що особи, котрі мали досвід інвестування, особливо ті, що володіли середньоризиковими активами, були схильні інвестувати без фінансових посередників, попри суб'єктивні фінансові знання стосовно інвестицій у криптоактиви. Щодо практичного застосування фінансової та інвестиційної грамотності, то вважаємо обґрунтованою рекомендацію авторів зазначеної праці, адресовану дослідникам, глибше усвідомлювати детермінанти інвестицій у криптоактиви в Сполучених Штатах. Також у цьому дослідженні детально описано наслідки відсутності фінансової й

цифрової інклюзії для діяльності фінансових установ, професійних учасників і державних регуляторів у частині управління раціональною інвестиційною поведінкою на ринку криптоактивів. Вказане дослідження стало однією з перших спроб виокремити визначальні фактори прийняття рішень про інвестиції у криптоактиви – сферу, яка динамічно змінюється та стрімко розвивається [507].

Такі висновки авторів свідчать про наявність високих ризиків залучення населення до шахрайських схем на ринку віртуальних активів, адже відсутність фінансової грамотності не зупиняє людей у прийнятті рішення про здійснення криптотрансакцій. Підкреслимо важливість подібних досліджень з огляду на схильність неосвічених осіб перебільшувати свої знання, що зумовлює потенційні ризики залучення їх до злочинних схем на ринку ВА. Також це є сигналом для українських державних регуляторів (центральних органів виконавчої влади) стосовно необхідності розвитку програм фінансової та цифрової грамотності, у тому числі з питань кібербезпеки.

Основною проблемою в Україні в окресленій галузі залишається низький рівень фінансової грамотності й обізнаності споживачів фінансових та інвестиційних послуг щодо захисту своїх прав та інвестицій від шахраїв. Їм бракує знань про альтернативні фінанси, які стосуються фінансових каналів, процесів та інструментів, що виникли поза традиційною фінансовою системою.

На жаль, використовують населення з низькою фінансово-цифровою інклюзією не тільки в шахрайстві, а й у злочинній діяльності ВК/ФТ. Останніми роками, особливо під час російського вторгнення в Україну, населення дедалі частіше залучають до злочинних схем ВК з використанням ВА як осіб, котрі відкривають гаманці або рахунки на своє ім’я для трансакцій (дропи) і виступають посередниками для переміщення нелегальних коштів (мули). Ці схеми активно використовуються міжнародними злочинними угрупованнями, оскільки Україна є однією з найбільш криптоактивних країн світу, а населення має низький рівень цифрової грамотності, але просунутий у використанні Fintech-технологій.

Найчастіше людей залучають зловмисники для штучного підвищення обсягу торгівлі новими токенами: щоб створити ілюзію їхньої популярності, «дропи» відкривають рахунки на криптобіржах та виконують фіктивні покупки, збільшуючи ліквідність проєкту. Учасники таких схем отримують доступ до закритої інформації про майбутні лістинги на біржах або великі трансакції, їхнє завдання — поширювати чутки у криптоспільнотах, підштовхуючи трейдерів до вигідних для злочинців угод.

Наймані «мули» проводять невеликі транзакції через P2P-біржі, криптомати та навіть звичайні банківські перекази, щоб роздрібнити великі суми нелегальних коштів. Вони також можуть використовувати свої акаунти для отримання й пересилання криптовалюти, створюючи складну мережу трансакцій. Окремі зловмисники залучають українців до переведення криптовалюти у готівку через нелегальні обмінники та доставлення цих коштів іншим учасникам схем. Часто таких «кур'єрів» використовують без розуміння ними повної картини злочинної діяльності.

Багато людей, котрих залучають до таких схем, не усвідомлюють, що стають частиною фінансових злочинів. Однак участь у подібних операціях може призвести до кримінальної відповідальності за відмивання грошей та фінансування незаконної діяльності (ст. 209 Кримінального кодексу України), замороження коштів та блокування акаунтів на криптобіржах і в банках, юридичних проблем під час виїзду за кордон, якщо особу внесено до міжнародних списків санкцій чи розшуку [418].

З початку 2021 р. близько 46 тис. осіб повідомили про втрату криптовалюти на суму понад 1 млрд дол. США через шахрайство – це приблизно один із кожних чотирьох втрачених доларів, більше, ніж будь-який інший спосіб оплати. Найпопулярнішими криптовалютами, якими люди платили шахраям, були Bitcoin (70 %), Tether (10 %) та Ethereum (9 %). За словами майже половини тих, хто повідомив про втрату криптовалюти через шахрайство у 2021 р., усе починалося з реклами, публікації чи повідомлення в соціальних мережах

(Instagram – 32 %, Facebook – 26, WhatsApp – 9 і Telegram – 7 %). Зареєстровані збитки мають тенденцію до збільшення (рис. 4.4). Винятком був 2022 р., що передусім пов’язано із загальним зниженням активності на крипторинку.

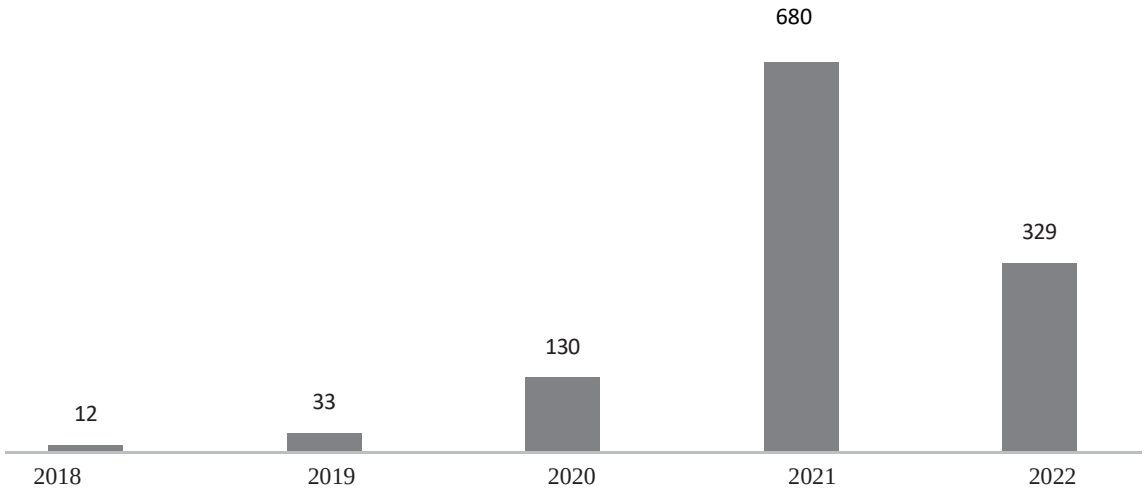


Рис. 4.4. Обсяги фінансових втрат громадян США на крипторинку через шахрайство протягом 2018–2022 рр., млн дол. США

Джерело: побудовано автором за матеріалами [508]

Зауважимо, що на сьогодні немає жодного банку чи іншого централізованого органу, який позначав би підозрілі трансакції та намагався зупинити шахрайство, перш ніж справу буде доведено до кінця. Тобто уникнути шахрайства на крипторинку можна тільки шляхом підвищення компетентності потенційних учасників.

З 2021 р. 575 млн дол. США з усіх збитків від криптовалютного шахрайства, про які було повідомлено Федеральною торговою комісією (FTC), стосувалися фіктивних інвестиційних можливостей, і ця цифра набагато більша, ніж обсяги збитків унаслідок будь-яких інших типів шахрайств. Розповіді осіб, котрі зазнали такого шахрайства, описують ідеальний шторм: помилкові обіцянки легких грошей у поєднанні з обмеженим розумінням і досвідом у сфері криптовалют людей, котрим ці обіцянки адресовано. Інвестиційні шахраї стверджують, що вони можуть швидко й легко отримати величезні прибутки для інвесторів. Але такі «інвестиції» в криптовалюту потрапляють просто до гаманця

шахрая. Хоч інвестиційні вебсайти та програми нібито дають змогу інвесторам відстежувати зростання своїх криптовалют, насправді все це підробка.

Наразі на крипторинку застосовується чимало схем, за допомогою яких шахраї обкрадають необізнаних громадян (рис. 4.5).

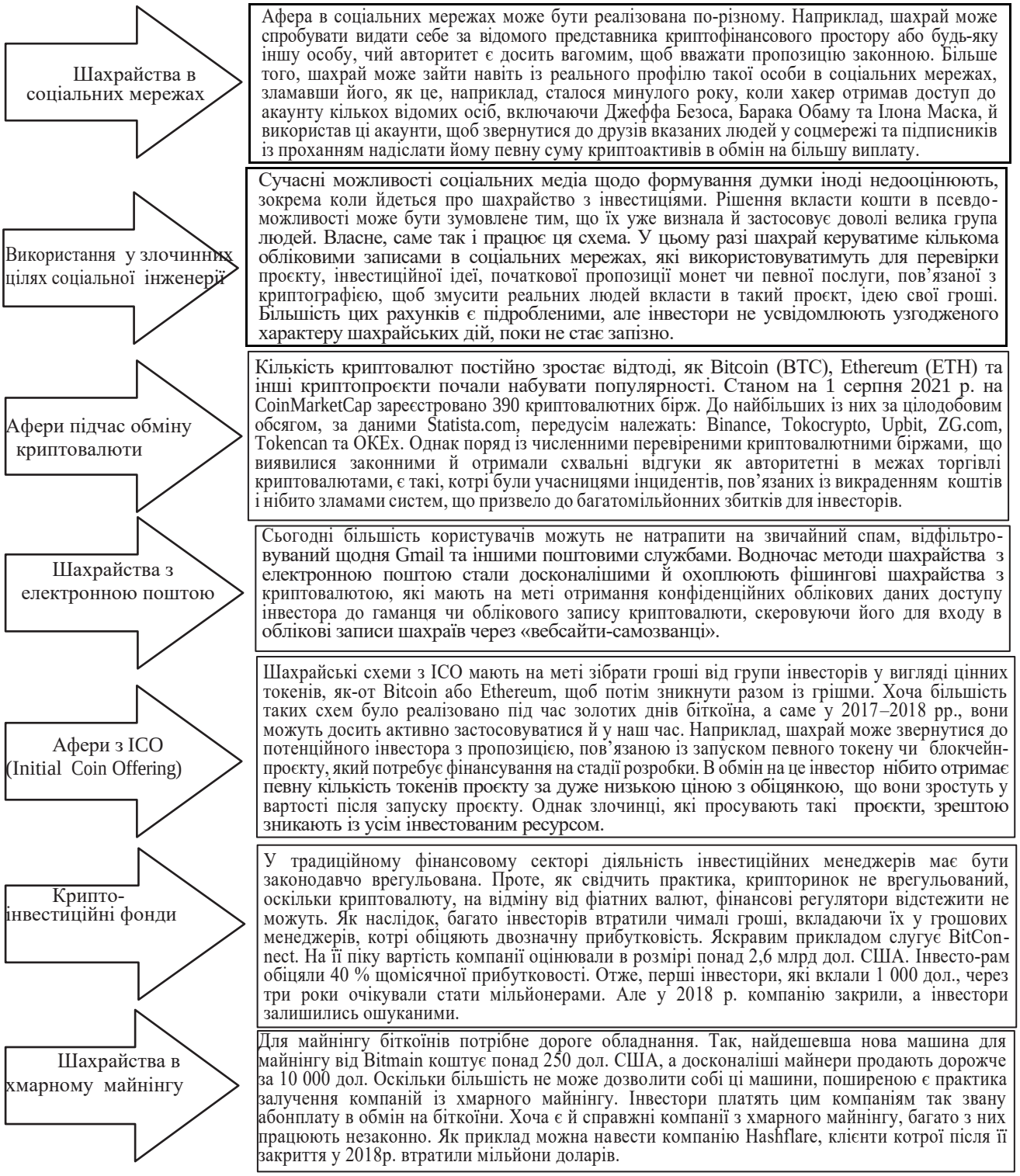


Рис. 4.5. Шахрайські схеми на крипторинку

Джерело: побудовано автором за матеріалами [509]

Також є факти залучення підлітків до шахрайських схем із використанням криптоактивів. Таких схем досить багато, серед основних – шахрайство в соціальних мережах, шахрайства соціальної інженерії, афери під час обміну криптовалюти, шахрайство з використанням розсилок електронною поштою, шахрайство з ICO (Initial Coin Offering – первинне розміщення токенів), шахрайські криптоінвестиційні фонди, шахрайство в хмарному майнінгу (щодо підтримки роботи мережі біткоїна чи іншої криптовалюти за винагороду у вигляді токенів) [510].

Зазначене дає підстави стверджувати, що для підвищення фінансової й цифрової грамотності доцільно запровадити курс для учнів 5–9-х класів базової середньої освіти, спрямований на вивчення особливостей крипторинку, напрямів інвестування в криптоактиви, шляхів оцінки інвестиційних ризиків, методів захисту від шахрайства, що в результаті допоможе здобути базові знання про альтернативні фінанси. На думку автора, такий курс має бути розроблено у вигляді комбінованої навчальної програми, яка включатиме курси «фінансова грамотність», «цифрова грамотність» і «кібербезпека». Поєднання цих напрямів дасть змогу учням набути необхідних компетенцій у сфері обігу віртуальних активів.

Зауважимо, що в цій сфері є низка напрацювань, зокрема розроблено численні навчальні курси з підвищення фінансової грамотності [511] і правил платіжної безпеки [512]. Утім, немає освітніх програм для середньої школи, що стосуються ринку ВА. Разом із тим ми бачимо досить масову й агресивну рекламу різноманітних сайтів і телеграм-каналів, які пропонують «вигідні» інвестиції в криптовалюту.

У свою чергу, щодо цифрових компетентностей треба зазначити, що Мінцифри розроблено концептуальний документ «Опис рамки цифрової компетентності для громадян України» [513]. За його основу було взято європейську концептуально-еталонну модель цифрових компетентностей, яку

адаптовано до української практики із залученням експертів Міністерства освіти і науки України. Розроблена рамка містить 4 виміри, 6 сфер, 30 компетентностей та 6 рівнів володіння цифровими компетентностями. Логічно, що запропонований навчальний курс має ґрунтуватися, зокрема, й на вказаному концептуальному документі.

Також, з огляду на те, що обсяги операцій із криптоактивами стрімко зростають і проводяться в кіберпросторі, набуття компетентностей із кібербезпеки є важливим аспектом. Підкреслимо, що правові й організаційні засади забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства й держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначено в Законі України «Про основні засади забезпечення кібербезпеки України». Відповідно до положень цього Закону, кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Важливість кібербезпеки підтверджується також положеннями Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»» від 26.08.2021 № 447/2021 [514], де, зокрема, зазначається, що частка кіберзагроз зростає й ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Кіберпростір разом з іншими фізичними просторами визнано одним із можливих театрів воєнних дій. На сьогодні цю тезу доведено в процесі повномасштабної агресії рф проти України, коли через низький рівень знань із питань кібербезпеки

українці своїми діями призводили до ракетних ударів по об’єктах цивільної інфраструктури, будинках тощо.

Підсумовуючи викладене, доцільно спрямувати зусилля освітніх управлінців на забезпечення підвищення фінансової грамотності, цифрових компетентностей і навичок із кібербезпеки для учнів середніх класів закладів загальної середньої освіти України. Навчальний контент теж має бути розроблено відповідно до Державного стандарту базової середньої освіти Нової української школи (НУШ) у частині набуття ключових компетентностей та наскрізних умінь.

Наголосимо, що навчальний контент повинен бути націлений на реалізацію концепції освіти впродовж життя щодо забезпечення навчальної діяльності людей різного віку (дітей, молоді, дорослих і людей похилого віку) в будь-якому життєвому середовищі (сім’ї, школі, спільноті, на роботі тощо) та за допомогою різноманітних методів (формальних, неформальних, інформальних), які разом задовольняють широке коло навчальних потреб. Такий підхід відповідає концепції реформи НУШ, а також Цілям сталого розвитку (Ціль 4 «Забезпечення всеосяжної та справедливої якісної освіти та заохочення можливостей навчання протягом усього життя для всіх»).

Імплементація в освітній процес закладів загальної середньої освіти України навчального курсу з фінансової грамотності, цифрових компетентностей і кібербезпеки відповідно до Державного стандарту базової середньої освіти НУШ допоможе учням:

– критично й системно мислити під час прийняття фінансових та інвестиційних рішень, що забезпечить майбутній добробут і фінансову стійкість домогосподарства;

– розв’язувати проблеми широкого спектра із застосуванням різних цифрових технологій;

– оцінювати ризики роботи в кіберпросторі, широко використовуючи навички з кібербезпеки, набуті під час проходження курсу;

– підвищувати рівень набутих знань у дорослому житті в контексті розвитку освіти впродовж життя.

Окремо варто підкреслити, що запровадження такого комбінованого навчального курсу забезпечить превентивну діяльність і потенційно зменшить навантаження на правоохоронні органи в частині розслідування фінансових, крипто- й кіберзлочинів, які насамперед пов’язані з необізнаністю громадян.

В Україні восени 2021 р. Служба безпеки України викрила мережу з шести кол-центрів у Львові, яку шахраї використовували для обману інвесторів у криптовалюту по всьому світу. Зловмисники використовували VoIP-номери для приховування свого місцезнаходження, обманюючи тисячі іноземних інвесторів. Під час обшуків правоохоронці вилучили електронні пристрої та документи, що підтверджували незаконну діяльність. У листопаді 2023 р. Департаментом кіберполіції України закрито шахрайські кол-центри у Львові, Одесі, Дніпрі та Кривому Розі, в яких працювало понад 800 осіб. Ці кол-центри підозрюються у крадіжці даних та переконанні жертв «інвестувати» в криптовалютні схеми. Під час операції було вилучено близько 900 одиниць цифрової техніки, мобільні телефони, SIM-карти, жорсткі диски та документи [515].

Окрім шахрайства, Департаментом кіберполіції Національної поліції України зібрано докази того, що в рф зростає кількість криптовалютних операторів (ППВА), які допомагають конвертувати гроші, що зберігаються у фінансових установах під санкціями, у криптоактиви з метою виведення капіталу з російської федерації та обходу санкцій Європейського Союзу й окремих держав.

Наведені випадки демонструють активну роботу українських державних правоохоронних органів у виявленні та припиненні злочинної діяльності, пов'язаної з криптовалютами, що сприяє підвищенню безпеки фінансового середовища в країні, однак саме превентивна діяльність щодо залучення громадян до такої протиправної діяльності й псевдоінвестування може значно скоротити витрати Державного бюджету України на розслідування такої

злочинності та покарання. Це вкотре обґрунтовує необхідність запровадження ризик-орієнтованого підходу щодо ПВК/ФТ та іншої протиправної діяльності до регулювання обігу ВА та діяльності ППВА, однак процес легалізації крипторинку в Україні істотно затягнувся в часі, що і надає підстави для використання ВА злочинцями без відповідного покарання.

В Україні вже впроваджуються нові регуляторні механізми для боротьби з кіберзлочинністю у криптосекторі, однак найкращий захист — це обізнаність громадян та їхня обережність у фінансових операціях. Цікаво, що особи віком від 20 до 49 років утричі частіше повідомляли про втрату криптовалюти через шахрайські дії, ніж люди старшого віку. Отже, навчання фінансової й цифрової грамотності необхідно запровадити ще в школі.

Таким чином, підвищення інвестиційної грамотності є важливим інструментом у боротьбі з шахрайськими схемами та ВК/ФТ на крипторинку. Освітні програми, інформаційні кампанії, розвиток критичного мислення та співпраця з регуляторами можуть істотно знизити ризики для інвесторів і сприяти здоровому розвитку криптовалютної екосистеми.

Висновки до розділу 4.

1. В підрозділі 4.1 автором обґрунтовано, що визначення правового статусу майнінгу, розробка ефективних обліково-звітних стандартів з застосуванням РОП дозволить регуляторам та фінансовим установам чіткіше оцінювати ризики кожної операції та концентрувати зусилля і ресурси на моніторингу саме тих транзакцій і операцій, що мають найвищий ризик незаконного використання, тим самим оптимізуючи контрольні процедури. Отже, зазначені напрями регулювання не лише забезпечують прозорість економічних операцій із ВА, а й створюють фундамент для впровадження ризик-

орієнтованого підходу в системі ПВК/ФТ, дозволяючи точніше визначати, аналізувати та мінімізувати відповідні ризики.

Тому впровадження ефективної податкової політики щодо ВА має забезпечити баланс між фіскальними інтересами держави та стимулюванням розвитку цифрової економіки. В дослідженні обґрунтовано, що розбудова національної системи контролю за ВА відповідно до вимог Директиви DAC8, яка передбачає розвиток прозорої та надійної фінансової системи для забезпечення стабільності економіки, залучення іноземних інвестицій може посилити позиції України на міжнародному рівні. Надані автором рекомендації щодо податкової політики з оподаткування ВА та інтеграції України в систему автоматичного обміну податковою інформацією направлені на виконання ключових вимог для гармонізації законодавства України з нормами ЄС. Це сприятиме підвищенню податкової дисципліни, боротьбі з фінансовими злочинами та зміцненню довіри.

2. РОП у процедурах комплаєнсу та ПВК/ФТ потребують використання моделей машинного навчання (AI), що дозволяє бізнесу більш ефективно прогнозувати фінансові ризики та виявляти шахрайські схеми. Викладені автором положення в корелюють з положеннями економічної теорії регулювання ризиків Стіглера – Пельцмана.

Для ефективної боротьби з фінансовими злочинами ВК/ФТ надані пропозиції з посилення публічно-приватного партнерства у сфері ПВК/ФТ, що сприятиме створенню безпечного фінансового середовища, мінімізує ризики ухилення від санкцій та ВК, а також зміцнить репутацію України як прозорої та технологічно розвиненої фінансової юрисдикції.

Автором обґрунтовано на прикладі співпраці FATF з представниками блокчейн-аналітичних програм в постійно-діючій робочій групі зазначених учасників, що взаємодія між НБУ, НКЦПФР, Держфінмоніторингом та ліцензованими криптооператорами сприятиме ранньому виявленню фінансових злочинів. Регулятори мають залучати учасників ринку до обговорення законодавчих змін та нових вимог щодо ПВК/ФТ.

Автором запропоновано створення Центру кіберфінансової безпеки, який може координувати дії між урядом, банківським сектором, криптобіржами та правоохоронними органами у сфері ПВК/ФТ. Також, надані пропозиції з використання FinTech та SupTech-рішень для забезпечення належного контролю трансакцій у криптоекосистемі сприятиме інтеграції криптоіндустрії у Національну систему ПВК/ФТ.

3. У дослідженні автором обґрунтовано, що впровадження освітніх ініціатив у сфері фінансової та цифрової інклюзії є не лише важливим інструментом підвищення рівня фінансової обізнаності учасників крипторинку, а й стратегічним елементом ризик-орієнтованого підходу до ПВК/ФТ. Автор зазначає, що ефективна комунікація базових знань про ризики, пов'язані з обігом цифрових активів, а також формування навичок безпечної участі у криптоекосистемі здатні зменшити кількість неусвідомлених правопорушень і зловживань.

Автор підкреслює, що належна фінансова грамотність знижує навантаження на систему державного нагляду, оптимізує витрати на ПВК/ФТ та забезпечує проактивну протидію фінансовим злочинам за рахунок саморегуляції на рівні учасників ринку. Таким чином, автор дійшов висновку, що освітні ініціативи у сфері фінансової та цифрової інклюзії мають бути інтегровані в національну систему ПВК/ФТ як довгостроковий інструмент зменшення ризиків, підвищення інституційної спроможності та зміцнення довіри до ринку віртуальних активів в Україні.

Основні наукові результати розділу опубліковані в працях автора [39; 50; 173; 398; 432; 433; 450; 502; 515].

ВИСНОВКИ

У результаті проведеного дисертаційного дослідження, виконаного на основі аналізу чинного вітчизняного й зарубіжного законодавства, узагальнення теоретико-методологічних основ ризик-орієнтованого підходу та обігу цифрових активів, розвитку інфраструктури фінансового та крипторинку і аналізу сучасного стану імплементації міжнародних стандартів ПВК/ФТ, автором сформульовано низку висновків, пропозицій та рекомендацій щодо розвитку методології ризик-орієнтованого підходу у сфері ПВК/ФТ, цивілізованого розвитку крипторинку та цифрових валют центральних банків, запропоновано новий спосіб розв'язання наукового завдання оцінки віртуальних активів як інструментів, що використовуються в легалізації злочинних доходів, тіньовій економіці, ухилення від санкцій, корупційній злочинності. Проведене дослідження дозволило сформулювати такі висновки:

1. Ризик-орієнтований підхід у сфері ПВК/ФТ став сучасним стандартом регулювання фінансової системи. Він передбачає фокусування зусиль на найбільш серйозних загрозах та гнучке управління новими ризиками в міру їх виникнення Однак фундамент цього підходу закладено задовго до цифрової доби – у класичних економічних теоріях ризику середини XX століття. Автором проаналізовані принципи теорії ризику та невизначеності Френка Найта, теорії очікуваної корисності фон Неймана–Моргенштерна, портфельна теорії Гаррі Марковіца та економічна теорії регулювання ризиків Стіглера–Пельцмана трансформації для їхньої до обороту цифрових активів. У сфері ПВК/ФТ в умовах функціонування крипторинку та цифрової економіки спостерігається еволюція цих теорій, а саме від найтівського усвідомлення невизначеності – до прийняття гнучких стратегій на випадок появи невідомих загроз; від теорії очікуваної корисності – до вдосконалення стимулів і покарань, що змінюють раціональний розрахунок злочинця, і включення поведінкових чинників; від портфельної теорії – до бачення цілісного «портфеля ризиків» і

оптимізації зусиль проти фінансових злочинів у різних напрямах одночасно; від економічної теорії регулювання – до вироблення збалансованих, стійких до обхідних маневрів правил для нових фінансових технологій.

Автором зазначено, що розвиток цифрових фінансів приніс нові проблеми, яких не було за часів Найта чи Марковіца, на стику класичних теорій та сучасних реалій виникає низка міждисциплінарних викликів та наголосив на доцільності об'єднання зусиль різних дисциплін. Автор пропонує розглядати ризик-орієнтований підхід ПВК/ФТ як міждисциплінарний продукт: він ґрунтується на економічній ідеї оптимального розподілу ресурсів (МРТ Марковіца), враховує ймовірності та корисності (фон Нейман–Моргенштерн), розрізняє вимірювані та невимірювані чинники (Найт), і прагне ефективного регулювання попри поведінкові реакції (Стіглер–Пельцман). Цей підхід закріплений у методах оцінки ризиків в сфері ПВК/ФТ.

Таким чином, класичні теорії ризику не втрачають значення – вони перетворюються. Автором обґрунтовано, сьогоднішні виклики на кшталт криптовалют чи DeFi спонукають науку і практику оновити ці теорії, додавши до них багатовимірність та технологічну оснащеність. Полеміка між традиційним і новим зрештою веде до синтезу: виникають нові теоретичні конструкції (як-то поведінкова теорія регулювання або моделі ризику, керовані ШІ), що спираються на класичні засади, але здатні відповісти на питання XXI століття. В дисертації зазначено, що ефективна ПВК/ФТ значною мірою буде залежати від того, наскільки ефективно інтегрується економічна мудрість минулого з науково-технічним прогресом сучасності. Така інтеграція забезпечить сталий міждисциплінарний розвиток теорій ризику на благо безпеки фінансової системи й суспільства.

3. У межах дисертаційної роботи автором обґрунтовано, що розвиток ринку ВА та цифрових технологій стали ключовими детермінантами оновлення міжнародних та європейських стандартів у сфері ПВК/ФТ. Автор зазначив, що така нормативна еволюція стала відповіддю на глобальні виклики, пов'язані з

динамікою інновацій у сфері фінансів і використанням ВА в трансзлочинній діяльності, та зумовила необхідність адаптації регуляторної бази до нових форм ризиків.

На думку автора, концептуально важливим у цьому контексті є європейський підхід до регулювання ВА, реалізований через Регламенти ЄС у поєднанні з Директивами. Це, як зазначено автором, забезпечує уніфікацію правових норм та термінології у сфері цифрової економіки на рівні Європейського Союзу, що є важливою передумовою для гармонізації регуляторної практики в державах-членах. Застосування таких правових інструментів дозволяє ефективніше реалізовувати ризик-орієнтований підхід у практиці ПВК/ФТ та забезпечувати належну координацію між національними та наднаціональними регуляторами.

Крім того, в дослідженні акцентовано, що розробка та тестування CBDC стало предметом глибоких макроекономічних досліджень. Зокрема, центральні банки аналізують вплив цифрових валют на інфляцію, грошову масу, банківську систему та кредитування. Такі дослідження, на думку автора, є основою для оновлення теоретичних підходів у регулюванні грошового обігу в умовах цифровізації, зокрема розширення економічної теорії регулювання ризиків і формування інституційних моделей, які враховують специфіку цифрового середовища.

4. У результаті проведеного ґрунтовного аналізу термінологічного апарату та таксономії цифрових активів в дисертаційній роботі було сформульовано узагальнене авторське визначення, яке врахувало їхню фінансово-економічну природу. Цифрові активи доцільно трактувати як цифрове представлення вартості, зафіксоване у криптографічно захищеному розподіленому реєстрі (зокрема, блокчейні), що існує виключно в цифровому середовищі та має майнову цінність. У структурному поділі таких активів виокремлено суверенні (CBDC) і приватні криптоактиви (ВА), що включають різноманітні форми цифрової вартості. Відособлення таких категорій, як

стейблкоїни та інвестиційні токени, дало змогу більш глибоко дослідити економічну поведінку користувачів та механізми збереження і передачі цифрової вартості.

Ключовим аспектом запропонованого автором підходу є інтеграція ризик-орієнтованої парадигми оцінки цифрових активів у контексті ПВК/ФТ. Через призму ризик-орієнтованого підходу цифрові активи постають не лише як інноваційні інструменти, а й як потенційні вектори фінансових зловживань. Встановлення чіткої ідентифікації активів, оцінки пов'язаних із ними ризиків і вразливостей дозволяють забезпечити більш цільову ПВК/ФТ. В дослідженні запропоновано зміщення фокусу регуляторної політики – від універсального контролю до адресного управління ризиками, пов'язаного зі злочинною діяльністю, зокрема ВК/ФТ.

Таким чином, уточнення сутності цифрових активів і їх класифікація крізь призму ризик-орієнтованого підходу не лише розширюють межі економічної науки, а й формують методологічне підґрунтя для розробки ефективних регуляторних стратегій у цифровій економіці. Це сприяє побудові безпечного, прозорого та стійкого до зловживань середовища обігу цифрових активів у відповідності до міжнародних стандартів FATF, ЄС та Базельського комітету.

5. Ризик-орієнтований підхід є ефективним інструментом управління та оцінки ризику, оскільки ґрунтується на системному аналізі потенційних загроз, їхньому впливі на економічні процеси та забезпечує оптимальний розподіл ресурсів, концентруючись на найбільш критичних загрозах, знижувати регуляторне навантаження для низькоризикових суб'єктів і забезпечувати гнучкість у реагуванні на нові виклики.

З огляду на класифікацію ризиків у економічній теорії, автором сформульовано визначення сутності ризик-орієнтованого підходу до регулювання обігу цифрових активів у сфері ПВК/ФТ, що полягає в забезпеченні систематичного здійснення оцінки ризиків використання цифрових активів у легалізаційних операціях та операціях маніпулювання віртуальними активами

уповноваженими державними органами й учасниками обігу цифрових активів і особами, котрі обслуговують операції з цифровими активами, а також застосування широкої сукупності методів фінансового контролю за обігом цифрових активів з метою виявлення операцій щодо легалізації (відмивання) доходів, ухилення від сплати податків, корупційної діяльності, фінансування тероризму, уникнення санкцій, шахрайства для забезпечення фінансової цілісності та резилієнтності економічної системи.

Запропоноване визначення поєднало в собі основні чинники ризик-орієнтованого підходу, методи ідентифікації ризиків та дозволило систематизувати процеси управління ризиками.

6. Результати проведеного дослідження засвідчили актуальність і необхідність впровадження ризик-орієнтованого підходу до оцінки операцій з віртуальними активами в контексті ПВК/ФТ через один із ключових його інструментів так звані «червоні прапорці» – індикатори підвищеного ризику, які сигналізують про потенційно підозрілу діяльність.

У рамках дослідження було поглиблено аналіз схем кримінального використання віртуальних активів і сформульовано авторську систему з 13 критеріїв ризиковості, що дозволяє ідентифікувати операції з високою ймовірністю причетності до процесів легалізації злочинних доходів. Особлива увага приділялася децентралізованим платформам, анонімним монетам (наприклад, Monero, Zcash), міксерам, криптобанкоматам та операціям, пов’язаним із неліцензованими біржами. Усі ці фактори були класифіковані як високоризикові, що значно підвищують вірогідність обходу стандартних механізмів ПВК/ФТ.

Автор зазначає, що використання системи «червоних прапорців» як інструмента ризик-орієнтованого підходу значно посилює ефективність національної системи ПВК/ФТ. Це дозволяє не тільки своєчасно реагувати на сучасні загрози цифрового середовища, а й формувати прозоріші умови для обігу

віртуальних активів, що, своєю чергою, підвищує інвестиційну привабливість країни та знижує витрати держави на боротьбу з економічною злочинністю.

7. Розроблені в дисертації критерії стали основою для побудови математичних моделей оцінки ризиків, орієнтованих на експертну оцінку поведінкових і трансакційних патернів користувачів цифрових активів. Застосування таких моделей дає змогу фінансовим установам, провайдерам криптопослуг та державним регуляторам не лише вчасно ідентифікувати ризиковані трансакції, але й оптимізувати ресурси, зосереджуючи контроль саме на тих операціях, які мають найвищу ймовірність зловживань.

Так, використані автором моделі класифікації допомагають ранжувати трансакції за рівнями ризику та виявляти підозрілі операції на ранніх стадіях. Регресійний аналіз сприяє встановленню зв'язків між факторами ризику та волатильністю віртуальних активів. Баєсові мережі дають змогу прогнозувати ймовірнісні сценарії ризиків ВК/ФТ на основі даних бухгалтерського обліку операцій з ВА, а гравітаційне моделювання аналізує транскордонні потоки нелегальних коштів у глобальному масштабі. Методи SEER (System for Evolutions and Review) та статистичні метрики (наприклад, метрики Мінковського) додатково уточнюють оцінку ризиків операцій із віртуальними активами. Зокрема, проведений аналіз 65 глобальних криптобірж підтвердив, що найбільші ризики пов'язані з анонімізацією трансакцій та обходом міжнародних санкцій.

8. Міжкраїновий регресійний аналіз (індекс сприйняття корупції) із застосуванням підходу від загального до конкретного свідчить, що активніше використання ВА емпірично пов'язане із вищим рівнем корупції та жорсткішим контролем капіталу. Дослідження підкреслює необхідність подальшого удосконалення збору та аналізу даних для більш глибокого розуміння мотивів використання криптовалют.

На основі комплексного аналізу корупційних схем, пов'язаних із використанням криптовалютних операцій для приховування джерел походження

активів, сформульовано авторські пропозиції, спрямовані на мінімізацію ризиків декларування цифрових активів як інструменту легалізації доходів, одержаних злочинним шляхом. Визначено, що декларування криптовалют у системі публічного контролю може використовуватися з метою створення видимості легальності походження майна, що особливо актуально у висококорупційних юрисдикціях.

Розроблені автором рекомендації враховують специфіку цифрових активів як високоволатильних і транскордонних інструментів, що ускладнюють їх перевірку й верифікацію. Запропоновано удосконалити механізми контролю за достовірністю декларування шляхом інтеграції ризик-орієнтованого підходу до перевірки джерел походження криптоактивів, а також залучення автоматизованих засобів блокчейн-аналітики. Це сприятиме підвищенню ефективності державного нагляду, зменшенню корупційних зловживань і забезпеченню прозорості у сфері обігу цифрових активів.

9. У межах дослідження сформульовано авторську концепцію протидії ухиленню від санкцій у сфері обігу ВА шляхом інтеграції ризик-орієнтованого підходу до державного та міждержавного регулювання крипторинку. Автором наголошено, що однією з ключових складових цієї стратегії виступає посилення контролю за майнінгом криптовалют у підсанкційних країнах, таких як росія та білорусь, у тому числі через заборону експорту відповідного обладнання. Майнінг, як інструмент перетворення енергетичних ресурсів у фінансові активи, може використовуватись для фінансування злочинних та санкційних режимів, що вимагає його включення до переліку критично контрольованих напрямів.

Серед пріоритетних напрямів також автором визначено запровадження обов’язкового міжнародного ліцензування всіх суб’єктів криптоекосистеми – зокрема, централізованих бірж, P2P-платформ та постачальників послуг з віртуальними активами. Особливу увагу приділено розвитку багатосторонньої координації між юрисдикціями (США, ЄС, Велика Британія), у тому числі в

частині обміну інформацією між підрозділами фінансової розвідки, а також застосування вторинних санкцій до компаній-посередників.

На думку автора, запровадження системного моніторингу ризиків та РОП у межах національної системи ПВК/ФТ забезпечить ефективніше виявлення підозрілих криптоопераций, зменшення втрат державного бюджету від злочинної діяльності, а також підвищення спроможності України до протистояння російській агресії. Водночас, за умови правової реалізації, арештовані віртуальні активи можуть стати джерелом компенсацій за міжнародну фінансову підтримку, що відкриває нові підходи до економічної відповідальності агресора.

10. В підрозділі 3.1. дисертації автором наголошено на необхідність в найкоротші строки легалізувати український крипторинок шляхом розроблення комплексного законодавства, відповідного європейським стандартам, із встановленням вимог до операторів і сервісів криптоіндустрії щодо ліцензування, звітності, безпеки та оподаткування, а також із забезпеченням постійного моніторингу ринку і впровадженням ризик-орієнтованого підходу до управління ризиками. Надані пропозиції з регулювання крипторинку щодо залученню як внутрішніх, так і іноземних інвестицій, стимулювання економічне зростання, розвитку інноваційних технологій, забезпечення захисту прав споживачів і підвищення безпеки фінансових операцій, будуть сприяти загальному економічному розвитку країни.

Автором проаналізовані ризики затримки легалізації, що вказують на можливе зниження рейтингу України в 6-му раунді взаємних оцінок MONEYVAL щодо впровадження 15-ї Рекомендацій FATF (категорія «не впроваджено»). Це може ускладнити доступ до міжнародних фінансових ринків, обмежити можливості українських підприємств у залученні інвестицій та веденні бізнесу з іноземними партнерами, а також спричинити скорочення обсягів міжнародної торгівлі через побоювання партнерів щодо недотримання міжнародних стандартів протидії ВК/ФТ. Для банківського сектору особливо критичним є ризик потрапляння до списку країн з підвищеним моніторингом, що

може призвести до припинення операцій за кореспондентськими рахунками з іноземними фінансовими установами та вплинути на стабільність фінансової системи.

11. Розвиток пілотного проєкту е-гривні є необхідним кроком модернізації фінансової системи України в контексті глобальних тенденцій упровадження CBDC. Запровадження е-гривні сприятиме підвищенню ефективності внутрішніх та міжнародних платежів, забезпеченню прозорості операцій і зниженню корупційних ризиків. У дисертації наголошено, що повноцінна реалізація е-гривня має відповідати вимогам ПВК/ФТ – зокрема, необхідно впровадити ліміти на баланс електронних гаманців та обсяги транзакцій згідно з міжнародними стандартами ПВК/ФТ. Це фактично означає застосування ризик-орієнтованого підходу: невеликі суми можуть використовуватися анонімно або напіванонімно, тоді як для здійснення більших платежів користувачі повинні пройти ретельнішу перевірку та ідентифікацію.

Крім того, впровадження CBDC у цьому контексті розглядається не лише як інструмент підвищення ефективності фінансових операцій, а й як засіб уніфікованого контролю в межах національної системи ПВК/ФТ. Йдеться про потенціал автоматизації перевірок, вбудованого моніторингу транзакцій та обмеження операцій із підвищеним ризиком завдяки вбудованим технічним механізмам.

Як загрози запуску в оборот е-гривні існують виклики, пов’язані з конфіденційністю платежів, кібербезпекою та забезпеченням операційної стійкості фінансових установ. Автор вважає, наявність неповного законодавчого регулювання цифрових валют уповільнює практичну реалізацію проєкту, тому запуск пілотного проєкту є критичним для тестування різних сценаріїв використання та вдосконалення технологічних і правових аспектів перед масштабним упровадженням.

В дисертації запропоновано використовувати е-гривню для підвищення прозорості операцій з ВА, що дасть змогу оптимізувати витрати на впровадження

процедур комплаєнсу та ПВК/ФТ, що є впровадженням РОП. При цьому важливим є забезпечення спроможності НБУ гарантувати захист персональних даних та стабільність роботи фінансових установ. Співпраця з міжнародними фінансовими організаціями, що мають досвід запуску CBDC, сприятиме зміцненню фінансової стабільності, покращанню доступу до цифрових платежів та інтеграції України у світову фінансову систему.

12. В підрозділі 4.1 дисертації автором обґрунтовано, що визначення правового статусу майнінгу, розробка ефективних обліково-звітних стандартів з застосуванням РОП дозволить регуляторам та фінансовим установам чіткіше оцінювати ризики кожної операції з ВА та концентрувати зусилля і ресурси на моніторингу саме тих операцій, що мають найвищий ризик незаконного використання, тим самим оптимізуючи контрольні процедури.

Тому впровадження ефективної податкової політики щодо ВА має забезпечити баланс між фіскальними інтересами держави та стимулюванням розвитку цифрової економіки. В дослідженні обґрунтовано, що розбудова національної системи контролю за ВА відповідно до вимог Директиви DAC8, яка передбачає розвиток прозорої та надійної фінансової системи для забезпечення стабільності економіки, залучення іноземних інвестицій може посилити позиції України на міжнародному рівні. Надані автором рекомендації щодо податкової політики з оподаткування ВА та інтеграції України в систему автоматичного обміну податковою інформацією направлені на виконання ключових вимог для гармонізації законодавства України з нормами ЄС. Це сприятиме підвищенню податкової дисципліни, боротьбі з фінансовими злочинами та зміцненню довіри.

13. РОП у процедурах комплаєнсу та ПВК/ФТ потребують використання моделей машинного навчання (AI), що дозволяє бізнесу більш ефективно виявляти шахрайські схеми та прогнозувати фінансові ризики. Викладені автором положення корелюють з положеннями економічної теорії регулювання ризиків Стіглера – Пельцмана.

Для ефективної боротьби з фінансовими злочинами ВК/ФТ автором надані пропозиції з посилення публічно-приватного партнерства у сфері ПВК/ФТ, які будуть сприяти мінімізації ризиків ухилення від санкцій та ВК, а також зміцнять репутацію України як прозорої та технологічно розвиненої фінансової юрисдикції.

Автором обґрунтовано на прикладі співпраці FATF з представниками блокчейн-аналітичних програм в постійно-діючій робочій групі зазначених учасників, що взаємодія між НБУ, НКЦПФР, Держфінмоніторингом та ліцензованими криптооператорами сприятиме ранньому виявленню фінансових злочинів. Регулятори мають залучати учасників ринку до обговорення законодавчих змін та нових вимог щодо ПВК/ФТ.

Автором запропоновано створення Центру кіберфінансової безпеки, який може координувати дії між урядом, банківським сектором, криптобіржами та правоохоронними органами у сфері ПВК/ФТ. Також, надані пропозиції з використання FinTech та SupTech-рішень для забезпечення належного контролю трансакцій у криптоекосистемі, що сприятиме інтеграції криптоіндустрії у Національну систему ПВК/ФТ.

14. У дисертаційному дослідженні автором обґрунтовано, що впровадження освітніх ініціатив у сфері фінансової та цифрової інклюзії є не лише важливим інструментом підвищення рівня фінансової обізнаності учасників крипторинку, а й стратегічним елементом ризик-орієнтованого підходу до ПВК/ФТ. Автор зазначає, що ефективна колаборація базових знань про ризики та ризики, пов’язані з обігом цифрових активів, а також формування навичок безпечної участі у криптоекосистемі здатні зменшити кількість неусвідомлених правопорушень і зловживань.

Автор дійшов висновку, що освітні ініціативи у сфері фінансової та цифрової інклюзії мають бути інтегровані в національну систему ПВК/ФТ як довгостроковий інструмент зменшення ризиків, підвищення інституційної спроможності та зміцнення довіри до ринку віртуальних активів в Україні.

Основні результати дослідження використовуються у діяльності Національної комісії з цінних паперів та фондового ринку України, Робочої групи при Раді національної безпеки і оборони України, Національного антикорупційного бюро України, Міністерства цифрового розвитку, інновацій та аерокосмічної промисловості Республіки Казахстан у співпраці з Департаментом по боротьбі з організованою злочинністю та відмиванням незаконних грошей Управління ООН з наркотиків і злочинності (UNODC), Комітету цифрової трансформації Верховної Ради України, Кременчуцької міської ради Кременчуцького району Полтавської області України, ДНУ «Інститут освітньої аналітики» Міністерства освіти та науки України, а також у навчальному процесі Інституту економіко-правових досліджень НАН України ім. Мамутова та ДВНЗ «Чернівецький торговельно-економічний інститут» Державного торговельно-економічного університету (Додаток Є).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ubezpieczenia majątkowe. Wydanie IV uzupełnione aneksem. Praca zbiorowa / pod redakcją W. Warkallo. Warszawa: PWE, 1971. S. 34.
2. Danhel J. Üloha kategorie nahodilosti v defmici pojisteni. *Pojistne rozpravy*. 1989. No. I. S. 24.
3. Neumann J., Morgenstern O. Theory of Games and Economic Behavior. Princeton, NJ: Princeton University Press, 1953.
4. Jensen M., Meckling W. Theory of the Firm Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economics*. Vol. 3 (4). P. 305–360. DOI: https://doi.org/10.1016/0304-405X(76)90026-X.
5. Kenneth R. French, Eugene Fama. The Cross-Section of Expected Stock Returns. The Journal of Finance. 1992. Vol. 47 (2). P. 427–465. DOI: https://doi.org/10.2307/2329112
6. Tetens J. N. Philosophische Versuche über die menschliche Natur und ihre Entwickelung. 2 Vols. Leipzig, 1777.
7. Finley M. I. The Ancient Economy. Berkeley: University of California Press, 1974. 222 p.
8. Lange O. Optymalne decyzje. *Dzieła*. T. 6. Wyd. 2. Warszawa: PWE, 1977. S. 204.
9. Willett A. H. The Ekonomie Theory óf Risk and Insurance. Philadelphia, 1951. P. 3—6. DOI: https://doi.org/10.9783/9781512808995.
10. Catastrophe theory: Selected papers, 1972-1977, by E. C. Zeeman, Addison-Wesley, London, Amsterdam, Ontario, Sydney, Tokyo, 1977. URL: https://projecteuclid.org/download/pdf_1/euclid.bams/1183541477?utm_source=chatgpt.com
11. Haddon W. Jr. Energy damage count errneasure and the ten strategies insurance institute for hghway safety. Human Factors. 1973. Vol.. 15(4). P. 355–366. DOI: https://doi.org/10.1177/001872087301500407

12. Nietzsche F. Twilight of the Idols; and the Anti-Christ. Harmondsworth: Penguin, 1977. P. 40–55.
13. Knight H. Fr., Risk, Uncertainty and Profit. Boston; New York: Houghton Mifflin Company, 1921. P. 381.
14. Galbraith J. K. Economics in Perspective: A Critical History. Houghton Mifflin Harcourt, 1987. 324 p.
15. Гері Стенлі Беккер. Лауреати Нобелівської премії / КНУДТ. URL: http://nobel.knute.edu.ua/in-dex.php/nobelivski-laureati/geri-stenli-bekker.
16. Поведінкова економіка: від теорії до практики : міждисц. навч, посіб. / за наук. ред. Татомир І. Л., Квасній Л. Г. Трускавець: ПОСВІТ, 2022. 408 с.
17. Almeida D., Dionísio A., Vieira I., Ferreira P. Uncertainty and Risk in the Cryptocurrency Market. Journal of Risk and Financial Management. 2022. Vol. 15 (11). DOI: https://doi.org/10.3390/jrfm15110532.
18. Mueller L., Langenegger I., Kem S. Blockchain Based Assets and Anti-Money Laundering: A Law and Economic Analysis. 2020. July 30. DOI: http://dx.doi.org/10.2139/ssrn.4279475
19. Markowitz H. M. Portfolio Selection. *Journal of Finance.* 1952. Vol. 7 (1). P. 77–92. DOI: https://doi.org/10.2307/2975974.
20. William F. Sharpe. Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk. *The Journal of Finance*. 1964. Vol. 19, No. 3. P. 425–442. DOI: https://doi.org/10.1111/j.1540-6261.1964.tb02865.x.
21. Lintner J. The Valuation of Risk Assets and the Selection of Risky Investments in Stock Portfolios and Capital Budgets. *Review of Economics and Statistics*. The Review of Economics and Statistics. 1965. Vol. 47, No. 1. P. 13–37. DOI: https://doi.org/10.2307/1924119.
22. Mossin J. Equilibrium in a Capital Asset Market. *Econometrica.* 1966. Vol. 34. No. 4. P. 768–783. DOI: https://doi.org/10.2307/1910098.
23. Фінтех-пісочниця як платформа інноваційного розвитку: досвід інших країн та перспективи в Україні. FinTechInsider. URL:

https://fintechinsider.com.ua/finteh-pisochnyczya-yak-platforma-innovaczijnogo-rozvytku-dosvid-inshyh-krayin-ta-perspektyvy-v-ukrayini/

24. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843.
25. Mnuchin S. The Remaking of Global Finance. *World Economic Forum.* 2018. URL: https://www.weforum.org/meetings/world-economic-forum-annual-meeting-2018/sessions/the-remaking-of-global-finance/.
26. Virtual Currencies Key - Definitions and Potential AML/CFT Risks / FATF-GAFI. 2014. URL: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
27. Guidance for a Risk-Based Approach to Virtual Currencies / FATF. 2015. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.inline.pdf.
28. Резолюція 1267 (1999), прийнята Радою Безпеки на його 4051 засіданні 15 жовтня 1999 року. URL: https://ips.ligazakon.net/document/MU99039.
29. Резолюція 1373 (2001), прийнята Радою Безпеки на його 4385 засіданні, 28 вересня 2001 року. URL: https://zakononline.com.ua/documents/show/225509___225574.
30. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers / FATF. 2019. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.
31. Recommendation 16: Wire transfers / FATF. URL: https://www.cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers.

32. A Bank Secrecy Act (BSA) rule [31 CFR 103.33(g)] / Treasury Department's Financial Crimes Enforcement Network (FinCEN). URL: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act.
33. What is Know Your Transaction (KYT) / Sanction Scanner. URL: https://www.sanctionscanner.com/knowledge-base/know-your-transaction-kyt-603.
34. The 2022 Global Crypto Adoption Index: Emerging Markets Lead in Grassroots Adoption, China Remains Active Despite Ban, and Crypto Fundamentals Appear Healthy / Chainanalysis. 2022. URL: https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/.
35. 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs / FATF. 2020. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html
36. Дмитренко Т. Л., Любіч О. О., Пархоменко Ю В. Регулювання ринку віртуальних активів: глобальний та національний рівні імплементації міжнародних стандартів ПВК/ФТ. *Фінанси України.* 2021. № 7. С. 31–52. DOI: https://doi.org/10.33763/finukr2021.07.031.
37. FATF Report to G20 on So-Called Stablecoins / FATF. 2020. June. URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.
38. Virtual Assets - Red Flag Indiciators of Money Laundering and Terrorist Financing / FATF. 2020. URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.
39. Єфименко Т. І., Дмитренко Т. Л. Сучасні пріоритети у сфері протидії відмиванню коштів та фінансуванню тероризму. *Наукові праці НДФІ.* 2022. № 2. С. 5–20. DOI: https://doi.org/10.33763/npndfi2022.02.005.

40. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text.
41. Russia-related Designations and Designation Removal; Cyber-related Designation; CAATSA - Russia-related Designations; Issuance of Russia-related Determination pursuant to Executive Order 14024 / U. S. Department of the Treasury's Office of Foreign Assets Control (OFAC). 2022. March 31. URL: https://ofac.treasury.gov/recent-actions/20220331.
42. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers / FATF. 2021. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf.
43. FATF Report to G20 Finance Ministers and Central Bank Governors / FATF. 2019. URL: http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-g20-april-2019.html.
44. Prosper (PROS) is non-custodial prediction market / Prosper Exchange. URL: https://prosper.exchange/.
45. Kosse A., Mattei I. Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies. *BIS.* 2022. May 6. URL: https://www.bis.org/publ/bppdf/bispap125.htm.
46. Central bank digital currency. Opportunities challenges and design / The Bank of England. 2020. URL: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf.
47. China uses digital yuan stimulate virus hitconsumption. *Reuters.* 2022. May 30. URL: https://www.reuters.com/markets/currencies/china-uses-digital-yuan-stimulate-virus-hit-consumption-2022-05-30/.
48. Partz H. Draft bill to ban chinas digital yuan fromus app stores. *CoinTelegraph.* 2022. May 27. URL: https://cointelegraph.com/news/draft-bill-to-ban-china-s-digital-yuan-from-us-app-stores.

49. Global CBDC Challenge 2021 Report. *Monetary Authority of Singapore*. 2022. January 7. URL: https://www.mas.gov.sg/publications/monographs-or-information-paper/2022/global-cbdc-challenge-2021.
50. Iefymenko T., Dmytrenko T., Development and integration of digital currencies in the activity of the virtual asset market. *Science and Innovation.* (2024). DOI: https://scinn-eng.org.ua/ojs/index.php/ni/article/view/837/252
51. Bank of Japan enters second phase of CBDC experiments. *Ledger Insights*. 2022. March 25. URL: https://www.ledgerinsights.com/bank-of-japan-enters-second-phase-of-cbdc-experiments/.
52. Inthanon-Lion Rock to mBridge Building a multi CBDC platform for international payments / Hong Kong Monetary Authority (HKMA). 2021. September. URL:https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Inthanon-LionRock_to_mBridge_Building_a_multi_CBDC_platform_for_international_payments.pdf
53. Central bank digital currency opportunities challenges and design. The Bank of England. URL: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunitieschallenges-and-design.pdf
54. Project Dunbar: international settlements using multi-CBDCs. (November, 2021) / BIS. URL: https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm.
55. New experiments pave way international payments using CBDCs. *SWIFT*. 2022. URL: https://www.swift.com/ru/node/308520.
56. Visa partners with consensys to help bridge CBDC networks with existing payment rails. *Payments journal*. 2022. January 13. URL: https://www.paymentsjournal.com/visa-partners-with-consensys-to-help-bridge-cbdc-networks-with-existing-payment-rails/.
57. Central Bank Digital Currency Tracker / Atlantic Council. URL: https://www.atlanticcouncil.org/cbdctracker//

58. Keister T., Sanches D. Should Central Banks Issue Digital Currency? *The Review of Economic Studies.* 2023. Vol. 90, Iss. 1. P. 404–431. URL: https://doi.org/10.1093/restud/rdac017.
59. Brunnermeier M. K., James H., Landau J.-P. The Digitalization of Money. *NBER.* NBER Working Paper Series. 2019 No. 26300. URL: https://doi.org/10.3386/w26300.
60. Franklin A., Gu X, Julapa J. Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China. *Journal of International Money and Finance*. 2022. Vol. 124(C). DOI: https://doi.org/10.1016/j.jimonfin.2022.102625.
61. Niepelt D. Reserves for All? Central Bank Digital Currency, Deposits, and their (Non)-Equivalence. CESifo Working Paper Series. 2018. No. 7176. URL: h https://dx.doi.org/10.2139/ssrn.3254206.
62. Schilling L., Fernández-Villaverde J., Uhlig H. Central Bank Digital Currency: When Price and Bank Stability Collide. *CESifo Working Paper Series.* 2020. No. 8773. URL: https://ideas.repec.org/p/ces/ceswps/_8773.html.
63. Veneris A., Park A., Long F., Puri P. Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. *SSRN Electronic Journal*. 2021. DOI: https://doi.org/10.2139/ssrn.3891121.
64. Pocher N., Veneris A. Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. *IEEE Transactions on Network and Service Management.* 2021. Vol. 19, Iss. 2. P. 1766–1788. URL: https://doi.org/10.1109/TNSM.2021.3136984.
65. On the Future of Currency: Interview with Charles Hoskinson, Part 2. *Harvard International Review.* 2021. URL: https://hir.harvard.edu/charles-hoskinson-2/.
66. Wright R. E. Imperial Monetary Policy and the Independence Movement. *American Institute for Economic Research.* 2023. URL: https://www.aier.org/article/imperial-monetary-policy-and-the-independence-movement/.

67. Report on a digital euro / European Central Bank. 2020. URL: https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html.
68. Progress on the investigation phase of a digital euro – second report / European Central Bank. URL: https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.degov221221_Progress.en.pdf.
69. Ensuring Responsible Development of Digital Assets. *Federal Register*. 2022. URL: https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets
70. Electronic Currency and Secure Hardware (ECASH) Act. H.R. 7231. *United States Congressman Stephen F. Lynch.* URL: https://lynch.house.gov/2022/3/rep-lynch-introduces-legislation-to-develop-electronic-version-of-u-s-dollar.
71. Ross R. Data Privacy and Security Implications of a U.S. Central Bank Digital Currency (CBDC). Seton Hall University, 2024. URL: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=2369&context=student_scholarship.
72. Аналітичний звіт пілотного проекту НБУ щодо е-гривні / Національний банк України. URL:https://bank.gov.ua/admin_uploads/article/Analytical%20Report%20on%20E-hryvnia.pdf?v=4.
73. Syrstad H. Introduction of central bank digital currency – necessary legislative amendments. *Staff Memo.* 2023. No. 4/2023. URL: https://hdl.handle.net/11250/3058248.
74. Mu Ch. Balancing Privacy and Security: Theory and Practice of the E-CNY's Managed Anonymity. *Digital Currency Institute at the People's Bank of China.* URL: http://www.pbc.gov.cn/en/3935690/3935759/4696666/2022110110364344083.pdf.

75. E-krona pilot Phase 2 : E-krona report of Riksbank. 2022. URL: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf.
76. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.
77. Ross V. Keeping on track in an evolving digital world. Afore Consulting 5-th Annual FinTech and Regulation Conference. *ESMA.* 2022. URL: https://www.esma.europa.eu/sites/default/files/library/esma50-164-5533_keynote_speech_-_verena_ross_-_keeping_on_track_in_an_evolving_digital_world.pdf.
78. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114&pk_campaign=todays_OJ&pk_source=EURLEX&pk_medium=TW&pk_keyword=Crypto%20assets&pk_content=Regulation&pk_cid=EURLEX_todaysOJ.
79. Missing Key – The Challenge of Cybersecurity and CBDCs : Atlantic Council GeoEconomics Center Report. 2022 URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/.
80. Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (COM/2020/594 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594.
81. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014,

(EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

82. Directive 2011/16/EU on administrative cooperation in the field of taxation. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0707.
83. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591.
84. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng.
85. ESMA Strategy 2023 – 2028. *ESMA.* URL: https://www.esma.europa.eu/sites/default/files/library/esma_strategy_2023-2028.pdf
86. Directive 2014/65/EU of the European Parliament and of the Council Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MIFID II). URL: www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mifid-ii.
87. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. URL: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0110.
88. Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. 2019. July. P. 20. URL:

https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en.

89. Report with advice for the European Commission on crypto-assets / EBA. 2019. January. URL: https://eba.europa.eu/eba-reports-on-crypto-assets.
90. Advice on Initial Coins Offerings and Crypto-Assets / ESMA. 2019. January. P. 42. URL: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
91. Snyers A. and Pauwels K. De ITO: a new kid on the block in het kapitaalmarktenrecht. *HDL*. 2019. URL: https://hdl.handle.net/10067/1621030151162165141.
92. Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms / IOSCO. 2019. May. URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf.
93. Global Money Laundering Terrorist Financing Threat Assessment / FATF-GAFI. 2010. URL: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Globalmoneylaunderingterroristfinancingthreatassessment.html.
94. Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms / IOSCO. 2020. February. URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf.
95. Maas T. Initial coin offerings: when are tokens securities in the EU and US? *SSRN*. 2019. February. URL: https://www.researchgate.net/publication/331706212_Initial_Coin_Offerings_When_Are_Tokens_Securities_in_the_EU_and_US.
96. Directive (EU) 2019/1937 of European Parliament and of Council of 23 October 2019 on protection persons who report breachs of Union law. URL: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.305.01.0017.01.FRA.

97. Markets in Crypto-Assets Regulation (MiCA) / ESMA. URL: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.
98. Digital assets-existing law— SF0125 / State of Wyoming Legislature. URL: https://www.wyoleg.gov/Legislation/2019/SF0125.
99. Revised Uniform Fiduciary Access to Digital Assets Act (2015) with prefatory note and comments. *The Uniform Law Commission (ULC).* URL: https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=112ab648-b257-97f2-48c2-61fe109a0b33&forceDialog=0.
100. An Act to amend the estates, powers and trusts law, in relation to the administration of digital assets / The New York State Senate. 2016. URL: https://legislation.nysenate.gov/pdf/bills/2015/A9910A.
101. Uniform access to digital assets by fiduciaries act / The Uniform Law Conference of Canada. 2016. URL: https://www.ulcc-chlc.ca/ULCC/media/EN-Uniform-Acts/Uniform-Access-to-Digital-Assets-by-Fiduciaries-Act-(2016).pdf
102. Digital Asset Business Act 2018. *Bermuda Laws Online.* URL: https://www.bma.bm/viewPDF/documents/2023-11-14-11-11-48-Digital-Asset-Business-Act-2018.pdf.
103. Emergency Decree on Digital Asset Businesses. 2018. URL: https://www.sec.or.th/EN/Documents/EnforcementIntroduction/digitalasset_decree_2561_EN.pdf.
104. CEO Tether: біткоїн — єдина децентралізована валюта. *Forklog*. 2024. URL: https://forklog.com.ua/news/ceo-tether-bitkoyin-yedyna-detsentralizovana-valyuta
105. Buntinx J. P. Digital assets vs cryptocurrencies. *The Merkle*. 2017. URL: https://themerkle.com/digital-assets-vs-cryptocurrencies/.
106. Gray G. H. New York's Fiduciary Access to Digital Assets Act. *Gfrllp: web portal.* Last updated: 20.10.2016. URL:

https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22

107. Harbinja E. Legal aspects of transmission of digital assets on death: Doctoral dissertation. *University of Strathclyde. Glasgow*. 2017. URL: https://stax.strath.ac.uk/concern/theses/k3569438f.

108. Kud A., Pypenko I. Social and economic foundation of the implementation of blockchain-based systems of digital assets in developing countries. *International Journal of Education and Science.* 2018. Vol. 1. No. 3-4. P. 30. DOI: https://doi.org/10.26697/ijes.2018.3-4.30.

109. Walker M. D. The new uniform digital assets law: estate planning and administration in the information age. *Real Property, Trust and Estate Law Journal*. 2017. Vol. 52 (1). P. 52–78. URL: https://estateplanning.osbar.org/files/2016/12/Est_2016Dec.pdf.

110. Peterson R E. A cross section study of the demand for money: The United States, 1960-62. *The Journal of Finance.* 1974. Vol. 29 (1). P. 73–88. URL: https://doi.org/10.1111/j.1540-6261.1974.tb00025.x.

111. Li Yaxiong, Ni Shan. Research on accounting recognition and measurement of data assets [J]. *Journal of Hunan University of Finance and Economics*. 2017, 33(04):82-90.

112. Shi Ai-xin, Gao Ding, Xie Jing. Construction of data asset value evaluation system of Internet enterprises [J]. *Times Finance*. 2017(14):109-112.

113. Qin Rongsheng. Research on the Confirmation, Measurement and Reporting of Enterprise Data Assets [J]. *Accounting and Economic Research*. 2020,34(06):3-10.

114. Ripple CEO Brad Garlinghouse Discusses Banking Challenges and Crypto Policy. Binance Square. URL:

115. Великая Е. Обложат ли виртуальные активы реальными налогами? *Дело UA.* 2018. URL: https://delo.ua/econonomyandpoliticsinukraine/oblozhat-li-virtualnyeaktivy-realnymi-nalogami-348461.

116. Lenz D. M. Afterlife on the cloud: creating a heavenly plan for electronic assets. *Bar Journal.* 2012. URL: https://www.sssblaw.com/media/1104/afterlife_on_the_cloud.pdf.
117. Owens J. Blockchain 101 for Governments. *Vienna: Wilton Park.* URL: https://www.wiltonpark.org.uk/wpcontent/uploads/WP1566-Blockchain-101-for-Governments.pdf
118. Wink S. P. and others. Latham & Watkins discusses SEC official's analysis of digital assets as securities. *The CLS Blue Sky Blog: web portal.* Last updated: 2018. July 2. URL: https://clsbluesky.law.columbia.edu/2018/07/02/latham-watkins-discusses-sec-officials-analysis-of-digital-assets-as-securities/.
119. Пестовська З. С. Токенізація економіки України: мрія чи реальність. *Академічний огляд.* 2022. № 1 (56) URL: https://acadrev.duan.edu.ua/images/PDF/2022/1/4.pdf.
120. Hines B. Digital Finance: Security Tokens and Unlocking the Real Potential of Blockchain. Wiley, 2021. 208 p. URL: https://books.google.com.ua/books?id=5W0DEAAAQBAJ&printsec=copyright&redir_esc=y#v=onepage&q&f=false
121. Москвін Б. Ю. Перспективи розвитку правового регулювання цифрових активів в Україні. *Київський часопис права.* 2024. № 2. DOI: https://doi.org/10.32782/klj/2024.2.27.
122. Hudima T., Kamyshanskyi V., Dmytrenko T., Shmyhov M. Optimal CBDC design for Ukraine through the lens of privacy and security. *Amazonia Investiga.* 2023. No. 12 (69). P. 73–83. DOI: https://doi.org/10.34069/AI/2023.69.09.6.
123. Chernykh O. Problems of legal regulation of the use of artificial intelligence technologies in court procedures within the framework of the Ukraine-EU action plan. *Artificial Intelligence.* 2023. № 28 (2). С. 27–31. DOI: https://doi.org/10.15407/jai2023.02.027
124. Meyer H. Tips for safeguarding your digital assets. *Computers & Security*, 1996. Vol. 15 (7). DOI: https://doi.org/10.1016/S0167-4048(97)88123-0.

125. Niekerk A V. A Methodological Approach to Modern Digital Asset Management: An Empirical Study. *Allied academies international conference, international academy for case studies*. 2006. URL: https://www.academia.edu/91321118/A_METHODOLOGICAL_APPROACH_TO_MODERN_DIGITAL_ASSET_MANAGEMENT_AN_EMPIRICAL_STUDY.
126. Toygar A. A New Asset Type- Digital Assets. *Journal of International Technology and Information Management*. 2013. Vol. 22 (4). DOI: https://doi.org/10.58729/1941-6679.1024.
127. Lu. H., Xiaoguang W. Digital Asset Management. 2013. DOI: https://doi.org/10.1109/ICCDA.2010.5541487.
128. Houben R., Snyers A. Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion. 2018. April. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf.
129. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.
130. Houben R., Snyers A. Crypto-assets: Key developments, regulatory concerns and responses. 2020. April. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf.

131. Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. *ECB Occasional Paper*. 2019. No.223. URL: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf.

132. Crypto-assets: work underway, regulatory approaches and potential gaps / FSB. 2019. May. URL: https://www.fsb.org/wp-content/uploads/P310519.pdf.

133. G7 working group on stablecoins. Investigating the impact of global stablecoins / BIS. 2019. October. URL: https://www.bis.org/cpmi/publ/d187.pdf.

134. Haffke L., Fromberge M., Zimmermann P. Virtual Currencies and Anti-Money Laundering. The Shortcomings of the 5th AML Directive (EU) and How to Address Them. *Journal of Banking Regulation*. 2020. Vol. 21, Iss. 2. P. 125–138. URL: https://doi.org/10.2139/ssrn.3328064.

135. Treatment of crypto assets in macroeconomic statistics / Prepared by M. Dinenzon, V. Josyula, J. C. Moreno-Ramirez, R. Dippelsman, T. Razin. 2019. URL: https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf.

136. Liao G. Y., Caramichael J. Stablecoins: Growth Potential and Impact on Banking Gordon. ternational Finance Discussion Papers. 2022. Iss. 1334. URL: https://www.federalreserve.gov/econres/ifdp/files/ifdp1334.pdf.

137. Eyers J. ANZ the first bank to mint an Australian dollar stablecoin, the A$DC . *The Australian Financial Review*. 2022. March 24. URL: https://www.afr.com/companies/financial-services/anz-the-first-bank-to-mint-an-australiandollar-stablecoin-the-a-dc-20220323-p5a743.

138. Japan's Largest Financial Institution To Issue Yen-Pegged Stable Coin, Progmacoin. *Coindesk.* URL: https://www.coindesk.com/business/2022/02/07/japans-biggest-bank-to-issue-yen-pegged-stablecoin-for-settlement-report

139. 5 critical challenges NFTs still need to overcome. *World Economic Forum.* 2021. URL: https://www.weforum.org/agenda/2021/08/nft-boom-cryptocurrency-digital-collectible-artwork/?DAG=3&gad_source=1&gclid=Cj0KCQjw7Py4BhCbARIsAMMx-

_LE7AIeuSK1bcUb48125SD2wWNgRuENrEj4WV2XblrbyIXgERlcmosaAo8JEALw_wcB.

140. Що таке DeFi і як вони працюють? *WhiteBITBlog.* 2023. URL: https://blog.whitebit.com/uk/what-is-defi-and-how-does-it-work/.

141. What is the metaverse? And why should we care? *World Economic Forum.* 2021. URL: https://www.weforum.org/agenda/2021/10/what-is-the-metaverse-why-care/?DAG=3&gad_source=1&gclid=Cj0KCQjw7Py4BhCbARIsAMMx-_KThbMF3YBsMtiatV0bSm67XUNABP_8WXZDJy-QNrz_n32SwkByT9caAu26EALw_wcB

142. Trading in NFTs spiked 21,000% to more than $17 billion in 2021. Report of Ryan Browne. *CNBC.* 2022. URL: https://www.cnbc.com/2022/03/10/trading-in-nfts-spiked-21000percent-to-top-17-billion-in-2021-report.html.

143. Metaverse Hype to Transition into New Business Models that Extend Digital Business : Press Release of Gartner, Inc. 2022. URL: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026.

144. How to Buy Land on Decentraland? *Binance.* URL: https://www.binance.com/en/square/post/765635070649.

145. Nike Sold an NFT Sneaker for $134,000. *The New York Times.* 2022. URL: https://www.nytimes.com/2022/05/26/style/nike-nft-sneaker.html.

146. Mastercard Files 15 Trademark Applications for a Wide Range of Metaverse, NFT Services. *Bitcoin.com.* 2022. URL: https://news.bitcoin.com/mastercard-files-15-trademark-applications-for-a-wide-range-of-metaverse-nft-services/.

147. Fidelity Investments Launches Crypto, Metaverse ETFs — Says 'We Continue to See Demand'. *Bitcoin.com.* 2022. URL: https://news.bitcoin.com/fidelity-investments-launches-crypto-metaverse-etfs-says-we-continue-to-see-demand/.

148. Morris C. Citi says metaverse economy could be worth $13trillion. *Fortune.* 2022. URL: https://fortune.com/2022/04/01/citi-metaverse-economy-13-trillion-2030.
149. Pai S. Banking on the Metaverse. *Forbes.* 2022. URL: https://www.forbes.com/councils/forbestechcouncil/2022/03/15/banking-on-the-metaverse/.
150. HSBC Enters the Metaverse Through Partnership with The Sandbox. *Coindesk.* 2022. URL: https://www.coindesk.com/business/2022/03/16/hsbc-enters-the-metaverse-through-partnership-with-the-sandbox.
151. Standard Chartered Bank Enters the Metaverse. *Bitcoin.com.* 2022. URL: https://news.bitcoin.com/standard-chartered-bank-enters-the-metaverse/.
152. Worldline steps into the metaverse. *MetaNews.* 2022. URL: https://www.metanews.com/worldline-steps-into-the-metaverse/.
153. Coinbase and Mastercard partner to revolutionize NFT purchase experience. *Cointelegraph.* 2022. URL: https://www.coinbase.com/blog/coinbase-and-mastercard-partner-to-revolutionize-nft-purchase-experience.
154. Vera partners with ONTO wallet to bring essential financial services for NFT's to its user's. *Vera Labs.* 2022. URL: https://blog.vera.financial/vera-partnerswith-ontowallet-to-bring-essential-financialservices-for-nfts-to-its-user-s-8e82cdad693.
155. Goldman Sachs Says It Is Exploring the Tokenization of Real Assets. *Coindesk.* 2022. URL: https://www.coindesk.com/business/2022/04/27/goldman-sachs-says-it-is-exploring-the-tokenization-of-real-assets/.
156. AXA France joins the metaverse. *Atlas Magazine.* 2022. URL: https://www.atlas-mag.net/en/article/axa-france-joins-the-metaverse.
157. Chinese Banking Associations Target NFTs. *Coindesk.* 2022. URL: https://www.coindesk.com/policy/2022/04/13/chinese-banking-associations-target-nfts.

158. UN approves NFT standards initiative led by Tencent. *Cointelegraph.* 2022. URL: https://cointelegraph.com/news/un-approves-nft-standards-initiative-led-by-tencent.

159. Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability. *Metaverse Standards Forum*. 2022. URL: https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/.

160. Today's Cryptocurrency Prices by Market Cap. *CoinMarketCap.* URL: https://coinmarketcap.com/.

161. Boar C., Wehrli A. Ready, steady, go? – Results of the third BIS survey on central bank digital currency. *BIS Papers.* 2021. No 114. URL: https://www.bis.org/publ/bppdf/bispap114.htm.

162. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: zakon.rada.gov.ua/laws/show/2074-20#Text.

163. Стаття 179-1 «Поняття цифрової речі». *Цивільний кодекс України від 16.01.2003 № 435-IV*. URL: https://zakon.rada.gov.ua/laws/show/435-15#n6917.

164. Прогнозування впливу цифрових активів на соціально-економічний розвиток підприємства: метод. посіб. / Кудь А. А. та ін. Харків: ХОГОКЗ, 2020. 76 с. DOI: https://doi.org/10.26697/9786177089093.2020.

165. Овчаренко А.С. Правове регулювання віртуальних активів та криптовалют в Україні: сучасний стан та перспективи. *Юридичний науковий електронний журнал.* 2020. № 4. С. 200–202. URL: http://www.lsej.org.ua/4_2020/49.pdf.

166. Дмитрик О.О. Віртуальні активи і цифрові активи: до питання про співвідношення понять. *Право та інноваційне суспільство*. 2021. № 2 (17). URL: https://www.apir.org.ua/index.php/lais/article/view/403/353.

167. Pestovska Z. S. Tokenization of Ukraine’s economy: dream or reality. *Академічний огляд.* 2022. № 1. DOI: https://doi.org/10.32342/2074-5354-2022-1-56-3.

168. Havva V., Haponiuk M. Digital financial assets: definition and classification. *Economic analysis.* 2023. Vol. 33 (3). P. 238–246. DOI: https://doi.org/10.35774/econa2023.03.238
169. Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard. OECD. 10 October 2022. Paris. 104 p. URL:
170. Demystifying cryptocurrency and digital assets. *PwC.* URL: https://www.pwc.com/us/en/tech-effect/emerging-tech/understanding-cryptocurrency-digital-assets.html.
171. The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption. *Chainanalysis.* URL: https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/.
172. Countries Say No to Energy Guzzling Bitcoin Mines. *Greenpeace.* 2024. URL: https://www.greenpeace.org/usa/countries-say-no-to-bitcoin-mines/.
173. Дмитренко Т. Л., Волкова В. М. Особливості регулювання операцій із віртуальними активами щодо діяльності у сфері майнінгу. *Наукові праці НДФІ.* 2021. № 2. С. 85–95. DOI: https://doi.org/10.33763/npndfi2021.02.085.
174. The Collapse Of FTX. *Forbes.* 2024. URL: https://www.forbes.com/sites/forbesstaff/article/the-fall-of-ftx/.
175. Final Report of Shoba Pillay, examiner / United States Bankruptcy Court, Southern District Of New York. 2022. URL: https://www.jenner.com/a/web/aag4HeVaPPyEsfWyTp9N5G/4SaB6v/celsius-final-report-shoba-pillay.pdf.
176. Волкова В., Дмитренко Т. Децентралізовані фінанси: їх розвиток у сучасній фінансовій системі та ризики, які вони спричиняють. *Grail of Science*. 2022. № 12-13. С. 71–80. DOI: https://doi.org/10.36074/grail-of-science.
177. Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (updated June 2023). FATF-GAFI. URL:

http://www.fatf-gafi.org/publications/mutualevaluations/docu-ments/fatf-methodology.html

178. International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations / FATF. 2012–2025. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.

179. Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems. 2022. FATF-GAFI. URL: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html.

180. Risk Assessment Support for Money Laundering/Terrorist Financing / The World Bank Group. 2016. URL: https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support.

181. Про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, про внесення змін до Регламенту Європейського Парламенту і Ради (ЄС) № 648/2012 та про скасування Директиви Європейського Парламенту і Ради 2005/60/ЄС та Директиви Комісії 2006/70/ЄС : Директива Європейського Парламенту і Ради (ЄС) 2015/849 від 20.05.2015. URL: https://zakon.rada.gov.ua/laws/show/984_037-15#Text.

182. Глущенко О. О., Райхерт Х. Я. Наслідки відмивання нелегальних доходів для фінансово-економічної безпеки україни. *Financial and Credit Activity Problems of Theory and Practice*. 2015. Т. 2 (17). С. 115–124. DOI: https://doi.org/10.18371/fcaptp.v2i17.37328.

183. Core Principles for Effective Banking Supervision / Bank for International Settlements: Basel Committee on Banking Supervision 1997. URL: https://www.bis.org/publ/bcbs129.pdf.

184. Bonneau J., Miller A., Clark J., Narayanan A., Kroll J. A., Felten E. W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy, San Jose, CA, USA*. 2015. P. 104–121. DOI: https://doi.org/10.1109/SP.2015.14.

185. Stewart I., Ilie D., Zamyatin A., Werner S., Torshizi M. F., Knottenbelt W. J. Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. *R. Soc. Open Sci.* 2018. 5180410. DOI: http://doi.org/10.1098/rsos.180410

186. Ma S., Hao W., Dai H. -N., Cheng S., Yi R., Wang T. A Blockchain-Based Risk and Information System Control Framework. *IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Athens, Greece*. 2018. P. 106–113, DOI: https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00031.

187. Goffard P.-O. Fraud risk assessment within blockchain transactions. *Advances in Applied Probability*. 2019. Vol. 51, Iss. 2. P. 443–467. DOI: https://doi.org/10.1017/apr.2019.18.

188. Chen C., Chen X., Yu J., Wu W., Wu D. Impact of Temporary Fork on the Evolution of Mining Pools in Blockchain Networks: An Evolutionary Game Analysis. *IEEE Transactions on Network Science and Engineering*. 2021. Vol. 8, No. 1. P. 400–418, DOI: https://doi.org/10.1109/TNSE.2020.3038943

189. Drljevic N., Aranda D.A., Stantchev V. Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Computer Standards & Interfaces.* 2020. Vol. 69, DOI: https://doi.org/10.1016/j.csi.2019.103409.

190. Patel D. Blockchain Technology towards the Mitigation of Distributed Denial of Service Attacks. *International Journal of Recent Technology and Engineering*

(IJRTE). 2020. Vol. 8 (6). P. 961–967. DOI: https://doi.org/10.35940/ijrte.F7420.038620.

191. Saad M., Spaulding J., Njilla L., Kamhoua C., Shetty S., Nyang D., Mohaisen A., Exploring the Attack Surface of Blockchain: A Systematic Overview. *arXiv. Operational Status.* 2019. DOI: https://doi.org/10.48550/arXiv.1904.03487

192. Canh N. P., Wongchoti U., Thanh S. D., Thong N. T. Systematic risk in cryptocurrency market: Evidence from DCC-MGARCH model. *Finance Research Letters*. 2019. Vol. 29. P. 90–100. DOI: https://doi.org/10.1016/j.frl.2019.03.011.

193. Lemieux V. L. Trusting records: is Blockchain technology the answer? Records Management Journal. 2016. Vol. 26 No. 2. P. 110–139. DOI: https://doi.org/10.1108/RMJ-12-2015-0042.

194. Muchlis Gazali H., Hafiz Bin Che Ismail C. M., Amboala T. Exploring the Intention to Invest in Cryptocurrency: The Case of Bitcoin. *International Conference on Information and Communication Technology for the Muslim World (ICT4M), Kuala Lumpur, Malaysia*. 2018. P. 64–68. DOI: https://doi.org/10.1109/ICT4M.2018.00021.

195. Yang L. The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*. 2019. Vol. 15. P. 80–90. DOI: https://doi.org/10.1016/j.jii.2019.04.002.

196. Dyhrberg A. H. Hedging capabilities of bitcoin. Is it the virtual gold? *Finance Research Letters*. 2016. Vol. 16. P. 139–144. DOI: https://doi.org/10.1016/j.frl.2015.10.025.

197. Bouri E., Molnár P., Azzi G., Roubaud D., Hagfors L. I. On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? *Finance Research Letters*. 2017. Vol. 20. P. 192–198. DOI: https://doi.org/10.1016/j.frl.2016.09.025.

198. Das D., Kannadhasan M. Do Global Factors Impact Bitcoin Prices? Evidence from Wavelet Approach. *Journal of Economic Research*. 2018. No. 23. P. 227–264. URL:

https://www.researchgate.net/publication/329308550_Do_global_factors_impact_bitcoin_prices_evidence_from_wavelet_approach.

199. Wang G., Zhang S., Yu T., Ning Y. A Systematic Overview of Blockchain Research. *Journal of Systems Science and Information*. 2021. Vol. 9 (3). P. 205–238. URL: https://doi.org/10.21078/JSSI-2021-205-34.

200. Koutmos D. Liquidity uncertainty and Bitcoin's market microstructure. *Economics Letters*. 2018. Vol. 172, P. 97–101. DOI: https://doi.org/10.1016/j.econlet.2018.08.041.

201. Biais B., Bisière C., Bouvard M., Casamatta C. The Blockchain Folk Theorem. *The Review of Financial Studies*. 2019. Vol. 32, Iss. 5. P. 1662–1715. DOI: https://doi.org/10.1093/rfs/hhy095.

202. Biais B., Bisière C., Bouvard M., Casamatta C., Menkveld A. J., Equilibrium Bitcoin Pricing. *Journal of Finance*/ *Forthcoming.* 2022. DOI: http://dx.doi.org/10.2139/ssrn.3261063.

203. Sockin M., Xiong W. A Model of Cryptocurrencies. *NBER Working Paper Series*. 2020. No. 26816. DOI: https://doi.org/10.3386/w26816.

204. L. Yang. The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration.* September 2019. Volume 15., pp. 80-90. DOI: https://doi.org/10.1016/j.jii.2019.04.002

205. Cong L. W., Li Ye., Wang N, Tokenomics: Dynamic Adoption and Valuation. *The Review of Financial Studies.* 2021. Vol. 34, Iss. 3. P. 1105–1155. DOI: https://doi.org/10.1093/rfs/hhaa089.

206. Momtaz P. P. The Pricing and Performance of Cryptocurrency. *The European Journal of Finance*. 2019. Vol. 27 (4–5). P. 367–380. DOI: https://doi.org/10.1080/1351847X.2019.1647259.

207. Routledge B., Zetlin-Jones A. Currency stability using blockchain technology. *Journal of Economic Dynamics and Control*. Vol. 142. DOI: https://doi.org/10.1016/j.jedc.2021.104155.

208. Pagnotta E. S. Decentralizing Money: Bitcoin Prices and Blockchain Security, *The Review of Financial Studies*. 2022. Vol. 35, Iss. 2. P. 866–907. DOI: https://doi.org/10.1093/rfs/hhaa149.

209. Liu Yu., Tsyvinski A., Wu Xi. Common Risk Factors in Cryptocurrency. *Journal of Finance, American Finance Association,* 2022. Vol. 77 (2). P. 1133–1177. DOI: https://doi.org/10.1111/jofi.13119

210. Андрійченко Ж. О. Фінансовий моніторинг у системі управління ризиками ринків фінансових послуг *Розвиток системи управління ризиками ринків фінансових послуг: монографія.* Наук. ред. та кер. кол. авт. д-р екон. наук, проф. Н. М. Внукова. Харків: Ексклюзив, 2014. С. 140–150.

211. Дмитров С. О., Меренкова О. В., Дмитров С. О., Медвідь Т. А., Ващенко О. М. Оцінка та управління ризиком використання послуг для легалізації кримінальних доходів або фінансування тероризму в комерційному банку: монографія / за заг. ред. О. М. Бережного. Суми: ДВНЗ «УАБС НБУ», 2010. 114 с.

212. Розвиток національної системи фінансового моніторингу / Т. І. Єфименко, С. С. Гасанов, О. Є. Користін та ін. Київ: ДННУ «Академія фінансового управління», 2013. 380 с. URL: https://afu.kiev.ua/getfile.php?page_id=450&num=13.

213. Zhang Yan-Hua Y.-W. Research on money laundering risk assessment of customers – based on the empirical research of China. *Journal of Money Laundering Control*. 2016. Vol. 19, Iss, 3. P. 249–263. DOI: https://doi.org/10.1108/JMLC-01-2015-0004.

214. Каднічанська В. М., Ромась Т. О. Оцінка ризику легалізації доходів, одержаних злочинним шляхом, і фінансування тероризму. *Вісник Університету банківської справи Національного банку України*. 2013. № 1 (16). С. 251–254.

215. Лазебник Л. Л. Управління ризиками відмивання незаконних доходів у комерційному банку. *Економіка та держава*. 2012. № 11. С. 4–7.

216. Худокормова М. І. Методика оцінювання ризику клієнта при використанні ним послуг банку для легалізації кримінальних доходів. *Актуальні проблеми економіки*. 2012. № 6. С. 283–289.

217. Черевко О. В. Вдосконалення методології моніторингу ризиків легалізації доходів у банківській системі. *Стратегічні пріоритети детінізації економіки України у системі економічної безпеки: макро та мікро вимір :* монографія / за ред. Черевка О. В. Черкаси: ПП Чабаненко Ю. А., 2014. 442 с.

218. Міщенко В. І., Науменкова С. В., Міщенко С. В. Теоретичні засади та практичні аспекти впровадження і використання цифрових грошей. *Економічна теорія.* 2022. № 2. С. 44–66. DOI: https://doi.org/10.15407/etet2022.02.044

219. Hulei A. I., Hulei S. A. Digital transformation of the domestic banking environment in the conditions of development of the fintech ecosystem. *Ukrainian Journal of Applied Economics*. 2019. Т. 4. №. 1. С. 6–15.

220. Коваленко Ю., Гулей А., Унинець-Ходаківська В., Рябокінь М. Сек'юритизація фінансових активів: сутність та причини поширення в економічних процесах. *Проблеми і перспективи економіки та управління*. 2022. Т. 4 (28), С. 177–185. URL: http://ppeu.stu.cn.ua/article/view/262941.

221. Цифрова трансформація промислового менеджменту: теорія і практика : кол. моногр. / [М. А. Ажажа, В. І. Аскольдов, Р. П. Афонов, Л. Б. Долінський та ін.]; за наук. ред. В. Г. Воронкової, Н. Г. Метеленко; Міністерство освіти і науки України, Запорізький національний університет. Львів; Торунь: Liha-Pres. 2023. 814 с.

222. Долінський Л. Б. Фінансовий ризик-менеджмент : навчально-методичний посібник. Київ: Національний університет "Києво-Могилянська академія", 2022. 130 с.

223. Recommandation 15: New technologies. GAFI-FATF. URL: https://cfatf-gafic.org/index.php/documents/fatf-40r/381-fatf-recommendation-15-new-technologies
224. Bridging the compliance gap: building AML controls for crypto / BNVK. URL: https://www.bvnk.com/blog/bridging-the-compliance-gap-crypto.
225. Crypto losses due to hacks and scams rise to $573 million in Q2: Immunefi. *Dailycoin.* 2022. URL: https://dailycoin.com/573m-lost-to-crypto-scams-and-hacks-in-q2-immunefi/
226. Cryptocurrencies: Opportunities, risks and challanges for anticorruption compliance systems. 2019. URL: https://digitalmoneyforum.biz/wp-content/uploads/2020/05/09_Cryptocurrencies_AntiCorruption_K.Ciupa_.pdf.
227. Choo R. Bitcoin's impacts on climate and the environment. *Columbia Climate School.* 2021. URL: https://news.climate.columbia.edu/2021/09/20/bitcoins-impacts-on-climate-and-the-environment/.
228. The Basics about Cryptocurrency. *Oswego State Univeristy of New York*. URL: https://www.oswego.edu/cts/basics-about-cryptocurrency.
229. Chinn M. D., Ito H. A New Measure of Financial Openness. *Journal of Comparative Policy Analysis Research and Practice.* 2008. Vol. 10 (3). DOI: https://doi.org/10.1080/13876980802231123.
230. Cryptocurrencies: Tracing the evolution of criminal finances / Europol. 2022. URL: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.
231. Oettler, Mario. Anonymity vs pseudonymity. *Blockchain Academy Mittweida.* 2021. URL: https://blockchain-academy.hsmittweida.de/courses/blockchain-introductiontechnical-beginner-cointermediate/lessons/lesson-4-privacy-inblockchain-2/topic/anonymity-vs-pseudonymity/.
232. Hsu S. US issues charges in first criminal cryptocurrency sanctions case. *The Washington Post.* 2022. URL: https://www.washingtonpost.com/dc-mdva/2022/05/16/first-us-criminal-cryptocurrencysanctions/.

233. Kereibayev O. All You Need to Know About UK Crypto Regulations. Guide. *The SumSub*. 2024. URL: https://sumsub.com/blog/all-you-need-to-know-about-uk-crypto-regulations-guide/.
234. Coin ATM Radar data. *Cryptolinks.* URL: https://cryptolinks.com/1074/coinatmradar.
235. Phadtare M. Bitcoin: How to use bitcoin mining to launder money. *Regtech. Times.* 2022. URL: https://regtechtimes.com/bitcoin-mining-to-launder-cryptocurrency/.
236. Coin Desk Annual Crypto Review. 2021. URL: https://downloads.coindesk.com/research/2021-annual-crypto-review-coindesk-research.pdf.
237. Holtmeier M., Sandner P. The impact of cryptocurrencies on developing countries. 2020. URL: https://philippsandner.medium.com/the-impact-of-crypto-currencies-on-developing-countries-dce44c529d6b.
238. Albrecht C., Duffin K. M., Hawkins S., Morales Rocha V. M. The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control.* 2019. Vol. 22 (2). URL: https://doi.org/10.1108/JMLC-12-2017-0074.
239. Financial Crime Typologie in Cryptoassets: The Concise Guide for Compliance Leaders . Elliptic. 2020. URL: https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf
240. Bains P., Arif I., Melo F., Sugimoto N. Regulating the crypto ecosystem: The case of unbacked crypto assets. *FinTech Notes.* 2022. Iss. 007. URL: https://doi.org/10.5089/9798400221361.063.
241. Difference Between DEX And CEX & Which One Should You Choose? *Binance Square.* 2023. URL: https://www.binance.com/uk-UA/square/post/637214.

242. Holtmeier M., Sandner P. The impact of cryptocurrencies on developing countries. 2017. URL: https://dx.doi.org/10.2139/ssrn.2965436.

243. De Pace P., Jayant R. Comovement and instability in cryptocurrency markets. *International Review of Economics and Finance*. 2023. Vol. 83. P. 173–200. URL: https://doi.org/10.1016/j.iref.2022.08.010.

244. Bitcoin shows that the getrich-quick dream never dies. *Alarabiya News*. 2022. URL: https://english.alarabiya.net/views/2022/06/20/Bitcoin-shows-that-the-get-rich-quick-dream-never-dies.

245. Kutera M. Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management, and Innovation.* 2022. Vol. 18 (4). URL: https://doi.org/10.7341/20221842.

246. Leuprecht, C., Jenkins, C. and Hamilton, R. Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*. 2023. Vol. 30 No. 4, pp. 1036-1054. URL: https://doi.org/10.1108/JFC-07-2022-0161

247. Larkin, Aiden. CEO of asset reality. Crypto asset recovery Q&A. Part 1. Scope, laws and cooperation. *Basel Institute on Governance. Basel.* 2022. URL: https://baselgovernance.org/blog/crypto-asset-recovery-qa-part-1-scope-laws-and-cooperation

248. Larkin, Aiden. CEO of asset reality. Crypto asset recovery part 2 – DeFi, auctions, cryptocurrency bans and capacity. *Basel Institute on Governance. Basel.* 2022. URL: https://baselgovernance.org/blog/crypto-asset-recovery-part-2-defi-auctions-cryptocurrency-bans-and-capacity?utm_source=chatgpt.com

249. On the periphery: Financial crime risks in cryptocurrency mining. *KYC360*. 2020. URL: https://kyc360.riskscreen.com/article/on-theperiphery-financial-crime-risks-in-cryptocurrencymining/.

250. The 2022 Crypto Crime Report. *Chainalysis*. 2022. URL: https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

251. Campanelli A. Cryptocurrencies: Instruments for payments or corruption? *FCPA.* 2017. URL: https://www.corporatecomplianceinsights.com/cryptocurrencies-instruments-for-payments-or-corruption/.
252. The 2024 Crypto Crime Report. *Chainalysis.* 2024. URL: https://go.chainalysis.com/crypto-crime-2024.html.
253. The 2023 Crypto Crime Report. *Chainalysis.* 2023. URL: https://go.chainalysis.com/crypto-crime-2023.html.
254. *Дмитренко Т. Л.* Особливості регулювання операцій із віртуальними активами щодо протидії легалізації доходів, отриманих злочинним шляхом. *Фінанси України.* 2020. № 3. С. 112–126. DOI: https://doi.org/10.33763/finukr2020.03.112
255. Bitcoin & Darknet 2022: Is OMG!OMG! The New Hydra? *The Crystal analytics team.* 2022. URL: https://crystalblockchain.com/articles/darknet-interactions-2022-is-omgomg-the-new-hydra/?utm_source=Digest&utm_medium=email&utm_cam-paign=June+2022.
256. Mansfield-Devine S. Darknets. *Computer Fraud & Security.* 2009. Vol. 2009, Iss. 12. DOI : https://doi.org/10.1016/S1361-3723(09)70150-2.
257. Морі Є. Що таке даркнет і чи справді він такий небезпечний. *Суспільне. Новини.* 2021. 8 жовт. URL: https://suspilne.media/170190-so-take-darknet-i-ci-spravdi-vin-takij-nebezpecnij/.
258. Дмитренко Т. Л., Любіч О. О. Упровадження міжнародних стандартів регулювання ринку віртуальних активів в Україні. *Фінанси України.* 2020. №9. С. 65–79. URL: https://doi.org/10.33763/finukr2020.09.065.
259. 10 Best Privacy Coins in 2022 – Most Private Cryptos. *Coinjournal.* 2022. URL: https://coinjournal.net/news/10-best-privacy-coins-in-2022/
260. Navazan H. FATF update on cross-chain, DeFi & unhosted wallets. *Crystal Blockchain.* 2022. URL: https://crystalintelligence.com/crypto-regulations/fatf-update-on-cross-chain-defi-unhosted-wallets/.

261. Ринкова капіталізація USDT зросла на 2 мільярди доларів після фіаско Tornado Cash. Кріптіх.ком.уа. 2022. 16 серп. URL: https://cryptih.com.ua/rynkova-kapitalizaciya-usdt-zrosla-na-2-milyardy-dolariv-pislya-fiasko-tornado-cash

262. Cryptocurrency Prices by Market Cap. *CoinGecko.* URL: https://www.coingecko.com/

263. Woods AK. Mutual Legal Assistance in the Digital Age. In: Gray D, Henderson SE, eds. The Cambridge Handbook of Surveillance Law. Cambridge Law Handbooks. Cambridge University Press; 2017:659-676.

264. Дмитренко Т.Л., Волкова В.М. Децентралізовані фінанси: їх розвиток у сучасній фінансовій системі та ризики, які вони спричиняють. *Наукові праці НДФІ.* 2022. № 1. С. 55-68. DOI: https://doi.org/10.33763/npndfi2022.01.055

265. 24% of New Tokens Launched in 2022 Bear On-Chain Characteristics of Pump and Dump Schemes. *Chainanalysis.* 2022. URL: https://www.chainalysis.com/blog/2022-crypto-pump-and-dump-schemes/?u-tm_campaign=newsletter&utm_source=linkedin&utm_medium=organicsocial.

266. «Pump & Dump» на ринку криптовалют: як кити маніпулюють курсом. *Trustee.* 2024. URL: https://trusteeglobal.com/academy/pump-dump-na-rynku-kryptovalyut-yak-kyty-manipulyuyut-kursom/.

267. Guidance on Digital ID / FATF. 2020. URL: https://www.fatf-gafi.org/en/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

268. Anti-Money Laundering and Countering the Financing of Terrorism Programs. *Federal Register.* 2024. URL: https://www.federalregister.gov/documents/2024/07/03/2024-14414/anti-money-laundering-and-countering-the-financing-of-terrorism-programs

269. Дмитренко Т. Л. Регулювання ринку віртуальних активів як інструмент протидії уникненню міжнародних санкцій проти рф. *Фінанси України.* 2022. № 4. С. 107128. DOI: https://doi.org/10.33763/fi nukr2022.04.107.

270. Для України зібрали вже понад $100 мільйонів у криптовалюті. *Укрінформ.* 2022. URL: https://www.ukrinform.ua/rubric-uarazom/3497586-dla-ukraini-zibrali-vzeponad-100-miljoniv-u-kriptovaluti.html.

271. Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact / UNODC of Southeast Asia and the Pacific. 2024. October. URL: https://www.unodc.org/roseap/uploads/documents/2024/TOCTA_Pacific_2024.pdf.

272. Using CBDCs across borders: lessons from practical experiments / BIS Innovation Hub. 2022. June. URL: https://www.bis.org/publ/othp51.pdf

273. Carstens A., Frost J., Song Shin H. A Foundation of Trust. *F&D Magazin.* 2022. URL: https://www.imf.org/en/Publications/fandd/issues/2022/09/A-foundation-of-trust-Carsten-Frost-Shin.

274. Самітова В. О. Класифікація та кластеризація даних, що задані в нечислових шкалах : автореф. дис. ... канд. техн. наук : 05.13.23 / М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків. 2017. С. 20. URL: https://open-archive.nure.ua/bitstreams/2b2f21a0-1ef9-48f2-b72f-be3e965379a4/download.

275. Aziz R. M., Baluch M. F., Patel S., Ganie A. H. LGBM: a machine learning approach for Ethereum fraud detection. *International Journal of Information Technology (Singapore)*. 2022. Vol. 14, No. 7. P. 3321–3331, DOI: https://doi.org/10.1007/s41870-022-00864-6.

276. Dutta A., Voumik L. C., Ramamoorthy A., Ray S., Raihan A. Predicting cryptocurrency fraud using ChaosNet: The Ethereum manifestation. *Journal of Risk and Financial Management.* 2023. Vol. 16, No. 4. P. 216. DOI: https://doi.org/10.3390/jrfm16040216.

277. Tripathy N., Balabantaray S. K., Parida S., Nayak S. K. Cryptocurrency fraud detection through classification techniques. *International Journal of Electrical and Computer Engineering (IJECE)*. 2024. Vol. 14, No. 3. P. 2918–2926. DOI: https://doi.org/10.11591/ijece.v14i3.pp2918-2926.

278. Anti-Money Laundering and Countering the Financing of Terrorism National Priorities. *Financial Crimes Enforcement Network U.S. Department of the Treasury*. June 30, 2021. URL: https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

279. Дмитренко Т. Як криптовалюти використовують у схемах Понці та як з цим борються: кейс Казахстану. *Incrypted*. URL: https://incrypted.com/ua/jak-kryptovaljuty-vykorystovujut-u-shemah-pontsi/

280. Jeremy Hill. Bankman-fried resigns from FTX, puts empire in bankruptcy. URL https://www.bloomberg.com/news/articles/2022-11-11/ftx-com-goes-bankrupt-in-stunning-reversal-for-crypto-exchange.

281. Guarino, M. FTX Crypto Collapse: Ex-CEO Sam Bankman-Fried Denies 'Improper Use' of Customer Funds. *Good morning, America*. URL: https://www.goodmorningamerica.com/news/story/ftx-crypto-collapse-ceo-sam-bankman-fried-denies-94215046

282. Feder, A., Gandal, N., Moore, T., and Vasek, M. The rise and fall of cryptocurrencies. In 17th Workshop on the Economics of Information Security (WEIS), 2018. URL https://tylermoore.utulsa.edu/weis18.pdf

283. Gandal, N., Hamrick, J.T., Moore, T. et al. The rise and fall of cryptocurrency coins and tokens. *Decisions Econ. Finan.* 2021. 44, 981–1014. https://doi.org/10.1007/s10203-021-00329-8

284. *Грабовецький Б. Є.* Методи експертних оцінок: теорія, методологія, напрями використання : монографія. Вінниця: ВНТУ, 2010. 171 с.

285. Мінцифра разом з представниками ринку розробляє стратегією розвитку сфери віртуальних активів в Україні / Міністерство цифрової трансформації України. 2021. URL: https://thedigital.gov.ua/news/mintsifra-razom-z-predstavnikami-rinku-rozroblyae-strategieyu-rozvitku-sferi-virtualnikh-aktiviv-v-ukraini.

286. Бідюк П.І. Байєсівський аналіз даних : монографія / П. І. Бідюк, І. О. Калініна, О П. Гожий. – Херсон: Книжкове видавництво ФОП Вишемирський В.С., 2021. – 208 с.

287. AML program to check crypto wallets for illicit funds. *AMLbot.* URL: https://amlbot.com/

288. Crystal Blockchain B.V. *Crystal Expert.* URL: https://crystalintelligence.com/get-crystal/

289. Global Ledger Protocol. *Global Ledger*. URL: https://glprotocol.com/

290. Bridging Compliance and Security in Web3 Ecosystems. *Purefi.* URL: https://purefi.io/

291. Конвенція про захист прав людини і основоположних свобод. Конвенція Ради Європи від 04.11.1950. *ВРУ.* - URL: http://zakon3.rada.gov.ua/laws/show/995_004

292. Бережний О. М. Оцінка та управління ризиком використання послуг для легалізації кримінальних доходів або фінансування тероризму в комерційному банку : монографія /за заг. ред. О.М. Бережного; [С. О. Дмитров, О. В. Меренкова, Т. А. Медвідь, О. М. Ващенко]. Суми: ДВНЗ “УАБС НБУ”. 2010. С. 114.

293. Карташов М. В. Імовірність, процеси, статистика : посібник. Київ : Видавничо-поліграфічний центр «Київський університет», 2008.

294. Долінський Л. Б. Фінансовий ризик-менеджмент : навч.-метод. посіб. / Нац. ун-т “Києво-Могилянська академія”. Київ : НаУКМА, 2022. С. 130 URL: https://ekmair.ukma.edu.ua/bitstreams/12d1e5eb-37a5-4a9f-bf03-ce3f2f92b78b/download

295. Дмитренко Т.Л. Методологічні підходи до розробки моделей оцінки ризиків використання цифрових активів у легалізації та злочинних операціях. *Фінанси України.* 2024. С. 75–92. DOI: https://doi.org/10.33763/finukr2024.12.075.

296. Anderson J. E. The Gravity Model. *Annual Review of Economics*. 2011. Vol. 3 (1). P. 133–160. DOI: https://doi.org/10.1146/annurev-economics-111809-125114.

297. Asgharzadeh M. F., Hashemi H., Frese R. B. Comprehensive gravitational modelling of the vertical cylindrical prism by Gauss. *Legendre quadrature integration. Geophysical Journal International*. 2018. Vol. 212, P. 591–611. DOI: https://doi.org/10.1093/gji/ggx413.

298. Dmytrenko T., Hudima T. Risk assessment models for cryptocurrency use in fraud and criminal proceeds legalization. *Фінанси України*. 2025. № 1. С. 75–92. DOI: https://doi.org/10.33763/finukr2025.01.110.

299. Ferwerda J., Kattenberg M., Chang H.-H., Unger B., Groot L., Bikker A. J. Gravity Models of Trade-based Money Laundering. *DNB Working Paper*. 2011. No. 318. P. 1–28. DOI: https://doi.org/10.2139/ssrn.1943473.

300. Brisard J.-C., Martinez D. ISIS Financing in 2015. Center for the Analysis of Terrorism, 2016. URL: https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf.

301. Перелік найкращих бірж криптовалют. *MixFin.* URL: https://mixfin.com/ua/crypto-exchanges.

302. Dell™ Statistica™ 13.0. *Dell Technologies.* 2015. URL: https://www.dell.com/uk-ua/lp.

303. Berzin P., Shyshkina O., Kuzmenko O., Yarovenko H. Innovations in the risk management of the business activity of economic agents. *Marketing and Management of Innovations.* 2018. No. 4, P. 221–233. DOI: https://doi.org/10.21272/mmi.2018.4-20.

304. Isard W. Location Theory and Trade Theory: Short-Run Analysis. *The Quarterly Journal of Economics, President and Fellows of Harvard College*. 1954. Vol. 68 (2). P. 305–320. DOI: https://doi.org/10.2307/1884452.

305. VACG roadmap: jurisdictions with materially important virtual asset activity / FATF-GAFI. 2024. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf.
306. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні : проект Закону України від 07.11.2023 № 10225. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43123.
307. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні : проект Закону України від 17.11.2023 № 10225-1. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/43232.
308. Про надання рекомендацій щодо фінмоніторингу. Лист НБУ від 30.12.2023 р. № 25-0005/97009. *НБУ.* URL: https://document.vobu.ua/doc/23250
309. Cambridge Alternative Finance Benchmarks / The Cambridge Centre for Alternative Finance. URL: https://ccaf.io/.
310. The 2024 Geography of Crypto Report. *Cyainanalysis*. 2024. URL: https://go.chainalysis.com/2024-geography-of-cryptocurrency-report.html.
311. 550 Top Attack Vectors: February 2022: *EXPEL.* URL: https://expel.com/blog/top-attack-vectors-february-2022/.
312. Dickler J. Russia-Ukraine crisis: How to avoid fundraising scams. *CNBC.* 2022. URL: https://cnb.cx/3MBPfjz
313. Flowers G. Want to help Ukraine? Avoid these war scammers asking you for bitcoin and money. *Yahoo.News!.* 2022. URL: https://www.yahoo.com/news/want-to-help-ukraine-avoid-these-war-scammers-asking-you-for-bitcoin-and-money-175126458.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIg6ssDwslDDHZ37DMgysldggXRsWWUJcu0CHBqNAlGpA2RnneAwmUtuXEWTgl_7H5k5Kg2IahsVezJlRw08bzgBifd7HE7Qo8aqnMwTUXdef2ZSOZTrYPMZYO87QZYjlZ9LbJO2NbmyHwcDTfAfB8VQQHNbdEh5p8tmMZvoGsjU

314. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. *FATF-GAFI.* URL: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html
315. Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму(сепаратизму). Типологічні дослідження Держфінмоніторингу України / Держфімоніторинг України. 2021. С. 82. URL : https://fiu.gov.ua/assets/userfiles/200/Typologies%20of%20the%20SFMS/UKR_Typology_2021_26_05.pdf.
316. Crystal updates report on crypto donations for Ukraine. *The Paypers.* URL: https://thepaypers.com/cryptocurrencies/crystal-updates-report-on-crypto-donations-for-ukraine--1256318Основні засади грошово-кредитної політики на 2022 рік та середньострокову перспективу. *НБУ.* URL: https://bank.gov.ua/admin_uploads/article/MPG_2022-mt.pdf?v=4
317. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/.
318. Протокол засідання Ради з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення від 22.12.2022 № 14. *Держфінмоніторинг України.* URL: https://fiu.gov.ua/assets/userfiles/330/RADA/Protokol_14.pdf.
319. Ключові напрями євроінтеграційного руху Національного банку в 2022 році. *НБУ.* URL: https://bank.gov.ua/ua/news/all/klyuchovi-napryami-yevrointegratsiynogo-ruhu-natsionalnogo-banku-v-2022-rotsi
320. Ключові напрями євроінтеграційного руху Національного банку в 2022 році / НБУ. 2023. URL: https://bank.gov.ua/ua/news/all/klyuchovi-napryami-yevrointegratsiynogo-ruhu-natsionalnogo-banku-v-2022-rotsi
321. Про внесення змін до деяких нормативно-правових актів Національного банку України щодо порядку здійснення авторизації діяльності надавачів

фінансових платіжних послуг : постанова Правління Національного банку України від 01.03.2023 № 14. URL: https://bank.gov.ua/ua/legislation/Resolution_01032023_14.

322. Why Decentralized Finance (DeFi) Matters and the Policy Implications / Boston Consulting Group. URL: https://web-assets.bcg.com/d4/47/64895c544486a7411b06ba4099f2/bcg-global-wealth-2021-jun-2021.pdf.

323. Олійник Я., Кучерява М., Коритник Л., Дмитренко Т., Кузьмінська О., Лагунов К. Формування інформаційного забезпечення управління фіскальними ризиками в умовах криз. Financial and Credit Activity Problems of Theory and Practice. 2023. Т. 6 (53). С. 432–450. URL: https://doi.org/10.55643/fcaptp.6.53.2023.4219.

324. Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers / FATF-GAFI. 2021. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html

325. Carstens A., Frost J., and Shin H. S. A Foundation of Trust: Central banks should harness crypto's technical wizardry to enable a rich monetary ecosystem. Finance&Devepopment. *IMF*. September, 2022. URL: https://www.imf.org/en/Publications/fandd/issues/2022/09/A-foundation-of-trust-Carsten-Frost-Shin.

326. Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text.

327. Imperial Monetary Policy and the Independence Movement. *American Institute for Economic Research.* URL: https://www.aier.org/article/imperial-monetary-policy-and-the-independence-movement/

328. Eurosystem report on the public consultation on a digital euro / European Central Bank. 2021. URL:

https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf.

329. Progress on the preparation phase of digital euro / European Central Bank. URL: https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202412.en.html.

330. Progress on the investigation phase of a digital euro – second report / European Central Bank. URL: https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.degov221221_Progress.en.pdf.

331. CBDCs: The Time Has Come. *ACAMS.Today*. 2021. URL: https://www.acamstoday.org/cbdcs-the-time-has-come/#:~:text=Traditional%20rule,CBDCs%20and%20private%20virtual%20assets.

332. Ensuring Responsible Development of Digital Assets. *Federal Register*. 2022. April 20. URL: https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

333. The Electronic Currency and Secure Hardware (ECASH) Act, H.R. 7231. *Congressman Stephen Lynch.* URL: https://lynch.house.gov/_cache/files/5/0/500162f9-7fce-4981-b9b9-16bf22e10ede/83EE032381B9431A65DE22B213D3A10E.rep.-lynch-ecash-act-fact-sheet.pdf.

334. Using Modern Portfolio Theory for Crypto - How to create an Optimal risky portfolio. *Reddit.* URL: https://www.reddit.com/r/CryptoCurrency/comments/wrhfix/using_modern_portfolio_theory_for_crypto_how_to/.

335. CBDC Tracker. *Peak Shift & HRF*. URL: https://cbdctracker.hrf.org/home.

336. Про захист персональних даних : Закон України від 01.06.2010 №2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17.

337. Про банки та банківську діяльність : Закон України від 07.12.2000 № 2121-III. URL: https://zakon.rada.gov.ua/go/2121-14.

338. Digital Currency Governance Consortium White Paper Series. Compendium Report / WEF. 2021. November. URL: https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf.

339. Central Bankers' New Cybersecurity Challenge. *Finance and Development Magazin*. 2022 No. 9. URL: https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr.

340. The Hamilton Project. URL: https://www.hamiltonproject.org/.

341. Нігерія першою в Африці запустила цифрову валюту — eNaira. там вважають, що це підвищить ВВП. *Дзеркало тижня.* 2021. 25 жовт. URL: https://zn.ua/ukr/ECONOMICS/niherija-pershoju-v-afritsi-zapustila-tsifrovu-valjutu-enaira-tam-vvazhajut-shcho-tse-pidvishchit-vvp.html.

342. What is Libra? All you need to know about Facebook's new cryptocurrency. *The Guardian.* 2019. URL: https://www.theguardian.com/technology/2019/jun/18/what-is-libra-facebook-new-cryptocurrency.

343. Prasad E. S. The future of money: how the digital revolution is transforming currencies and finance. Belknap Press, 2021. URL: https://www.hup.harvard.edu/file/feeds/PDF/9780674258440_sample.pdf.

344. Communiqué. Finance ministers and central bank governors. 2018. March 20. Buenos Aires. URL: http://www.g20.utoronto.ca/2018/2018-03-30-g20_finance_communique-en.html.

345. Rogoff K. S. The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy. Princeton University Press, 2016. URL: https://doi.org/10.2307/j.ctvc77m90.

346. Дмитренко Т. Л., Пархоменко Ю. В., Волкова В. М., Гавриленко С. В. Географічні кореляції щодо контролю над капіталом, криптоактивами та

корупцією. *Фінанси України*. 2023. № 12. С. 114–128. DOI: https://doi.org/10.33763/finukr2023.12.114.

347. Graf von Luckner C.,. Reinhart C. M., Rogoff K. S. Decrypting New Age International Capital Flows. *Policy Research Working Paper*. 2021. No. 9794. URL: https://doi.org/10.1596/1813-9450-9794,

348. Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons. IMF. FinTech Notes. 2022. URL: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174

349. The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption. Chainanalysis. URL: https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

350. Cryptocurrency adoption rates : Finder Crypto Report. URL: https://www.3bit-lab.com/documents/finder-cryptocurrency-adoption-rates_202106.pdf.

351. Global crypto acceptance. *Triple A.* URL: https://triple-a.io/crypto-ownership-data/.

352. Market Cap by Cryptocurrency Current & Historical Market Capitalizations by Cryptocurrency. *Coin Dance*. URL: https://coin.dance/stats#demographics.

353. Worldwide Governance Indicators. *World Bank Group.* URL: http://info.worldbank.org/governance/wgi/.

354. Inflation rate, average consumer prices. *IMF*. URL: https://www.imf.org/external/datamapper/pcpipch@weo/oemdc/advec/weoworld.

355. Chinn M. D., Ito H. A New Measure of Financial Openness. *Journal of Comparative Policy Analysis Research and Practice*. 2008. Vol. 10 (3). URL: https://doi.org/10.1080/13876980802231123.

356. The Annual Report on Exchange Arrangements and Exchange Restrictions (AREAER) / *IMF*. URL: https://www.elibrary-areaer.imf.org/Pages/Home.aspx.

357. Hendry D., Krolzig H.-M. Improving on Data Mining Reconsidered by K. D. Hoover and S. J. Perez. *Econometrics Journal*. 1999. Vol. 2. P. 41–58. DOI: https://doi.org/10.1111/1368-423X.00027.

358. Hoover K., Perez S. Data mining reconsidered: encompassing and the general-to specific approach to specification search. *The Econometrics Journal*. 1999. Vol. 2 (2). P. 167–191. DOI: https://doi.org/10.1111/1368-423X.00025.

359. Fernández A., Klein M. W., Rebucci A., Schindler M., Uribe M. Capital Control Measures: A New Dataset. *NBER Working Paper Series*. 2015. No. 20970. URL: https://doi.org/10.3386/w20970.

360. Aldaz-Carroll E. Can cryptocurrencies and blockchain help corruption? Washington, DC: Brookings Institute, 2018. URL: https://www.brookings.edu/blog/future–development/2018/02/01/can-cryptocurrencies-and-blockchain-help-fight-corruption/.

361. Dudley S., Pond T., Carden S. Evasive Maneuvers How Malign Actors Leverage Cryptocurrency. Washington, DC: National Defence University, 2019. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

362. Adrianit I., Arif B. Corruption and cryptocurrency: Blockchains as corruption tools. *Academicus International Scientific Journal*. 2022. Vol. 13 (26). P. 93–103. DOI: https://doi.org/10.7336/academicus.2022.26.06.

363. European Council Conclusions on Ukraine, the Membership Applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and External Relations / Council of the EU and the European Council. 2022. June 23. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022/pdf

364. Сорок Рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF). 2003. URL: https://zakon.rada.gov.ua/laws/show/835_001#Text.
365. Рекомендації FATF/ Міжнародні стандарти боротьби з відмиванням коштів, фінансуванням тероризму і розповсюдженням зброї масового знищення; Методологія з оцінки технічної відповідності рекомендаціям FATF та ефективності систем протидії відмиванню коштів та боротьби з фінансуванням тероризму; Правила та процедури 5-го раунду взаємних оцінок комітетом MONEYVAL. 2018. URL: https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf.
366. Про засади державної антикорупційної політики на 2021–2025 роки : Закон України № 2322-IX від 20.06.2022. URL: https://zakon.rada.gov.ua/laws/show/2322-20#Text.
367. Індекс Сприйняття Корупції. *Transparency.org*. URL: https://cpi.ti-ukraine.org/2022/.
368. Антикорупційна структура України не має аналогів у Європі – Зеленський. *Факти ICTV.* 2021. 20 серп. URL: https://fakty.com.ua/ua/ukraine/polituka/20210820-antykoruptsijna-struktura-ukrayiny-ne-maye-analogiv-u-yevropi-zelenskyj/.
369. Вхід до системи «Єдиний державний реєстр декларацій». *НАЗК України.* URL: https://portal.nazk.gov.ua/login/
370. Про затвердження бланку декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, та Порядку заповнення і подання декларації особи, уповноваженої на здійснення функції держави або місцевого самоврядування : наказ Національного агентства з питань запобігання корупції № 449/21 від 23.07.2021. URL: https://zakon.rada.gov.ua/laws/show/z1965-23#Text.

371. Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення / НАЗК України. URL: https://corruptinfo.nazk.gov.ua/.

372. До перемоги над рашистськими загарбниками декларанти не повинні втрачати час на заповнення та подання декларації. *НАЗК України*. 2022. URL: https://nazk.gov.ua/uk/do-peremogy-nad-rashystskymy-zagarbnykamy-deklaranty-ne-povynni-vtrachaty-chas-na-zapovnennya-ta-podannya-deklaratsiyi-nazk/.

373. Про внесення змін до деяких законів України про визначення порядку подання декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, в умовах воєнного стану : Закон України від 20.09.2023 № 3384-IX. URL: https://zakon.rada.gov.ua/laws/show/3384-20#Text.

374. Відкрито публічний доступ до Реєстру декларацій / НАЗК України. 2023. URL: https://nazk.gov.ua/uk/novyny/vidkryto-publichnyy-dostup-do-reestru-deklaratsiy/.

375. Біткоїни на ₴2 млрд і понад 10 000 токенів: які криптовалюти декларували українські посадовці у 2023 році. *Incrypted.* 2024. URL: https://incrypted.com/ua/kriptovalyuti-ukrayinskih-chinovnikiv-u-2023-roci/.

376. Декларація співробітника ГУ Держпродспоживслужби в Одеській області Олексія Клімова. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/b3f11566-aea7-4e04-9f9b-0b4c6604729f.

377. Декларація депутата Одеської облради Микити Кузькевича. ЕДРД. *НАЗК України.* URL: https://public.nazk.gov.ua/documents/39766355-2e6a-4d31-94c1-44fbbd36069b.

378. Декларація депутата ВРУ Олега Бондаренка. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/f47b6f54-431f-405e-9fcc-4933c14d9e8d.

379. Декларація голови Державної регуляторної служби Олексія Кучера. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/a27a1df7-31b9-49ef-8add-5923be1c3b53.

380. Декларація заступника начальника ГУНП у Миколаївській області Едуарда Соловйова ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/10894852-9da6-493f-8d45-9f11e3356baa.

381. Декларація депутат Хмельницької районної ради Олександра Кізляра. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/ced0da3d-d2d2-4502-936e-6929653a5d21/

382. Декларація депутата Верховної Ради України. Дмитра Гуріна. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/5d792492-42ab-4c46-a186-2cd8c7c86122

383. Декларація директор департаменту Державної виконавчої служби Мін'юсту Максима Кисельова. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/a83ee416-9a41-4bce-9a46-b0c0c4c3f44a.

384. Декларація начальника департаменту Офісу Генпрокурора Віталія Бровко. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/dec44e01-30e8-4bd7-974a-b6238498d34d.

385. Декларація депутата Подільської райради Одеської області Ігора Осіпова. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/410ea39a-6077-4242-9d24-152985192731.

386. Декларація спеціалістки Дніпровської міськради Крістіни Павлової. ЕДРД. *НАЗК України*. URL: https://public.nazk.gov.ua/documents/327461a4-60f8-4e00-992f-8be53b40a577.

387. 2023 Cryptocurrency Gains by Country. *Chainanalysis.* 2024. URL: https://www.chainalysis.com/blog/cryptocurrency-gains-by-country-2023/.

388. Про внесення змін до деяких законодавчих актів України щодо забезпечення ефективності інституційного механізму запобігання корупції : Закон України від 02.10.2019 № 140-IX. URL: https://zakon.rada.gov.ua/laws/show/140-20#Text.

389. Роз'яснення щодо застосування окремих положень Закону України «Про запобігання корупції» щодо заходів фінансового контролю (подання

декларації, повідомлення про суттєві зміни в майновому стані, повідомлення про відкриття валютного рахунку)» / НАЗК України. 2021. 29 груд. URL: https://wiki.nazk.gov.ua/wp-content/uploads/2021/12/1111_compressed.pdf .

390. Щодо міжвідомчої координації системи фінансового моніторингу / Державна служба фінансового моніторингу України. 2022. 31 берез. URL: fiu.gov.ua/pages/dijalnist/funkcional/news/shhodo-mizhvidomchoji-koordinacziji-sistemi-finansovogo-monitoringu.html.

391. OSCE training courses for Ukrainian officials on cryptocurrency risks, investigations and supervision conclude. *OSCE*. 2023. March 31. URL: https://www.osce.org/oceea/540440.

392. НАБУ вмітиме виявляти і розслідувати корупційні криптоактиви. *НАБУ.* 2023. 18 трав. URL: https://nabu.gov.ua/news/nabu-vm-time-viiavliati-rozsl-duvati-koruptc-in-kriptoaktivi/.

393. Experts from Ukraine discuss virtual assets regulation at OSCE-UNODC joint workshop. *OSCE*. 2022. December 7. URL: https://www.osce.org/oceea/533732.

394. АРМА налагоджує співробітництво з провідними криптобіржами світу. *АРМА.* URL: https://arma.gov.ua/news/typical/arma-nalagodjue-spivrobitnitstvo-z-providnimi-kriptobirjami-svitu.

395. АРМА розробило рекомендації з пошуку та арешту крипто-валютних активів. *АРМА*. 2020. URL: https://arma.gov.ua/news/typical/arma-rozrobilo-rekomendatsii-z-rozshuku-ta-areshtu-kriptovalyutnih-aktiviv.

396. Рішення Конституційного Суду України у справі за конституційним поданням від 27.10.2020 № 13-р/2020. URL: https://zakon.rada.gov.ua/go/v013p710-20.

397. Russia Values Local Crypto at $200 Billion as Rules Near. *Bloomberg*. 2022. February 1. URL: https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near.

398. Дмитренко Т.Л. «Особливості імплементації Європейських Директив щодо обігу віртуальних активів в національне законодавство України» Т. Л.

Дмитренко // Фінанси України. - 2022. - № 10. DOI: https://doi.org/10.33763/finukr2022.12.056

399. Aggression against Ukraine: resolution A/RES/ES-11/1 / The UN General Assembly. 2022. URL: https://digitallibrary.un.org/record/3965290?ln=ru&v=pdf.

400. Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation : Executive Order 14024 of April 15, 2021 / *OFAC*. URL: https://ofac.treasury.gov/media/57936/download?inline.

401. Sanctions adopted following Russia's military aggression against Ukraine. *European Commission.* 2025. URL: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en.

402. Kirkpatrick K., Savage C., Johnston R., Hanson M. Virtual currency in sanctioned jurisdictions: stepping outside of SWIFT. *Journal of Investment Compliance.* 2019. Vol. 20, No. 2. P. 39–44. DOI: https://doi.org/10.1108/JOIC-04-2019-0019.

403. Targeting Elites of the Russian Federation / U. S. Department of State. 2022. March 24. URL: https://pl.usembassy.gov/factsheet_targeting_elites/.

404. Notice of Virtual Forum for Risks in the Information Communication Technology Supply Chain (Billing code 3510-33-p.) / Department of commerce, Bureau of Industry and Security. 2022. URL: https://www.bis.doc.gov/index.php/documents/pdfs/2859-final-version/file.

405. Stein J., Whalen J. Biden aides explore rarely used sanctions weapon against Russia. *The Washington Post.* 2022. March 24. URL: https://www.washingtonpost.com/us-policy/2022/03/24/russia-economy-sanctions/.

406. Ukraine war: US sanctions on China for supporting Russia are not needed yet, says Treasury Secretary Janet Yellen. *US-China Relations.* 2022. March 26. URL: https://www.scmp.com/news/china/article/3171939/ukraine-war-us-sanctions-china-supporting-russia-are-not-needed-yet-says.

407. Gromek M. Sanctioning Russia On The Blockchain: Following The Money To A Network of OTC Providers. *Forbes* 2022. URL: https://www.forbes.com/sites/michalgromek/2022/05/04/sanctioning-russia-on-the-blockchain-following-the-money-to-a-network-of-otc-providers/?sh=60c109-802fc2.
408. Шейко Ю. Санкції ЄС за війну РФ проти України: чого вже вдалося досягнути. *DeutscheWelle*. 24 квіт. 2022. URL: https://www.dw.com/uk/sanktsii-yes-za-viinu-rf-proty-ukrainy-choho-vzhe-vdalosia-dosiahnuty/a-61534456.
409. EU agrees 10th package of sanctions against Russia. *The Europian Commission*. 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1185.
410. Parliament slams repression and show trials in Belarus. *The Europian Commission*. 2023. URL: https://www.europarl.europa.eu/news/en/press-room/20230310IPR77231/parliament-slams-repression-and-show-trials-in-belarus.
411. Gromek M. Wrestling Russia On The Blockchain - Six Most Likely Sanctions To Be Imposed. *Forbes*. 2022. April 27. URL: www.forbes.com/sites/michalgromek/2022/04/27/wrestling-russia-on-the-blockchainsix-most-likely-sanctions-to-be-imposed/.
412. Про внесення змін до деяких нормативно-правових актів Національного банку України щодо порядку здійснення авторизації діяльності надавачів фінансових платіжних послуг : постанова Правління Національного банку України від 01.03.2023 № 14. URL: https://bank.gov.ua/ua/legislation/Resolution_01032023_14.
413. Про роботу банківської системи в період запровадження воєнного стану : постанова Правління Національного банку України від 24.02.2022 № 18. URL: https://bank.gov.ua/ua/legislation/Resolution_24022022_18.
414. 12 Month Review of Revised FATF Standards - Virtual Assets and VASPs / GAFI-FATF. 2021. URL: https://www.fatf-

gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html.

415. Shetret L. Practical implementation of FATF Recommendation 15 for VASPs: Leveraging on-chain analytics for crypto compliance. *Elliptic.* 2024. URL: https://www.elliptic.co/blog/practical-implementation-of-fatf-recommendation-15-for-vasps-leveraging-on-chain-analytics-for-crypto-compliance.

416. Cambridge Bitcoin Electricity Consumption Index. *Cambridge Centre for Alternative Finance.* URL: https://ccaf.io/cbnsi/cbeci

417. Bitcoin Mining Map. *Cambridge Centre for Alternative Finance*. URL: https://ccaf.io/cbeci/mining_map.

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

419. Деякі питання єдиної державної інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : постанова Кабінету Міністрів України від 22.07.2020 № 627. URL: https://zakon.rada.gov.ua/laws/show/627-2020-%D0%BF#Text.

420. Про затвердження Порядку формування переліку осіб, пов’язаних з провадженням терористичної діяльності або стосовно яких застосовано міжнародні санкції : постанова Кабінету Міністрів України від 22.07.2020 № 622. URL: https://zakon.rada.gov.ua/go/622-2020-%D0%BF .

421. *DDoS-Guard.* URL: https://ddos-guard.net/.

422. War&Sanction : головний портал про спонсорів та співучасників агресії. URL: https://war-sanctions.gur.gov.ua/.

423. The 2020 state of crypto crime. Chainalysis. 2020. January. URL: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf.
424. Elliptic Typologies Report Exposes Real Impact of Illicit Behavior in Crypto. Elliptic. URL: https://www.elliptic.co/blog/elliptic-typologies-report-exposes-real-impact-of-illicit-behavior-in-crypto?utm_campaign=Typologies%20Report%202022&utm_content=202181793&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267
425. Ciphertrace cryptocurrency intelligence, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 34. Ciphertrace. URL: https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/
426. CertiK - Securing The Web3 World. CertiK. URL: https://www.certik.com/
427. Lukka Data Solutions. Lukka, Inc. URL: https://lukka.tech/
428. SlowMist - Focusing on Blockchain Ecosystem Security. SlowMist. URL: https://www.slowmist.com/index.html
429. Про віртуальні активи : Закон України від 11.06.2020 № 3637. *ВРУ.* URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.
430. Про санкції : Закон України від 14.08.2014 № 1644-VII. URL: https://zakon.rada.gov.ua/laws/show/1644-18.
431. Про національну безпеку України : Закон України від 21.06.2018 № 2469. URL: https://zakon.rada.gov.ua/go/2469-19.
432. Дмитренко, Т. Л. Визначення сутності віртуальних активів як чинник формування методологічних підходів до оподаткування їх обороту. Вісник Чернівецького торговельно-економічного інституту. 2024. Вип. IV (96). С. 125-150. DOI: http://doi.org/10.34025/2310-8185-2024-4.96.08 (1,13 друк. арк.)
433. Дмитренко Т.Л., Волкова В.М., Гавриленко С.В., Пархоменко Ю.В. «Огляд нових пропозицій щодо регулювання ринку криптоактивів в Європі та шляхи імплементації їх в Україні». Наукові праці НДФІ №2 (23) 2023. DOI: https://doi.org/10.33763/npndfi2023.01.030

434. Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC. URL: https://eur-lex.europa.eu/eli/dir/2011/16/oj

435. EU adopts Directive introducing tax transparency rules for crypto assets (DAC8). *Ernst & Young LLP*. 2023. URL: https://taxnews.ey.com/news/2023-1765-eu-adopts-directive-introducing-tax-transparency-rules-for-crypto-assets-dac8?uAlertID=Sd%2FG8rua1oj6%2Fl58EZ2AiA%3D%3D.

436. Crypto-Asset Reporting Framework and amended Common Reporting Standard: OECD releases IT format for transmitting information and issues interpretative guidance. *OECD*. 2024. URL: https://www.oecd.org/en/about/news/announcements/2024/10/crypto-asset-reporting-framework-and-amended-common-reporting-standard-oecd-releases-it-format-for-transmitting-information-and-issues-interpretative-guidance.html.

437. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770.

438. Про внесення змін до Цивільного кодексу України щодо розширення кола об’єктів цивільних прав : Закон України від 10.08.2023 № 3320-IX. URL: https://zakon.rada.gov.ua/laws/show/3320-20.

439. Майданик Р. А., Майданик Н. І., Попова Н. Р. Цифрові речі. Право України на шляху до широкого розуміння речі. *Scientia*. 2022. Т. 1. С. 84–88. URL: https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/17852.

440. Сліпченко А. С., Сліпченко С. О. Цифрова річ як «новий» об’єкт «нових» цивільних правовідносин. *Право і безпека.* 2023. № 4 (91). С. 68–81. DOI: https://doi.org/10.32631/pb.2023.4.06.

441. Про затвердження Національного положення (стандарту) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності» : наказ Міністерства

фінансів України від 07.02.2013 № 73. URL: https://zakon.rada.gov.ua/laws/show/z0336-13#Text.

442. Міжнародний стандарт бухгалтерського обліку 7 (МСБО 7). Звіт про рух грошових коштів. URL: https://zakon.rada.gov.ua/laws/show/929_019#Text.

443. Міжнародний стандарт бухгалтерського обліку 38 (МСБО 38). Нематеріальні активи. URL: https://zakon.rada.gov.ua/laws/show/929_050#Text

444. Податковий кодекс України. Наказ від 28.03.2021 № 2755-VI. *ВРУ.* URL: https://zakon.rada.gov.ua/laws/show/z0336-13#Text

445. Назва видів економічної діяльності та пояснення до них. *Держстат України.* URL: http://kved.ukrstat.gov.ua/KVED2010/63/KVED10_63_11.html

446. Баранов О.А. Інтернет речей (IoT) і блокчейн. *Інформація і право.* 2018. № 1 (24). 2018. С. 59–61. URL: https://doi.org/10.37750/2616-6798.2018.1(24).270747.

447. Про електронну комерцію : Закон України від 03.04.2015 № 957. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text.

448. Про захист прав споживачів : Закон України від 12.05.1991 № 1023-XII. URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text.

449. Регулювання ринку криптовалют. Зелена книга Офісу ефективного регулювання BRDO / BRDO. 2018. URL: https://brdo.com.ua/wp-content/uploads/2024/06/ZK-Regulyuvannya-rynku-kryptovalyut.pdf

450. Дмитренко Т. Л., Волкова В. М. Сучасні проблеми/прогалини у регуляторній політиці щодо майнінгу криптовалют в системі віртуальних активів, наслідки та шляхи подолання їх. *Наукові праці НДФІ.* 2024. № 3. С. 65–82. DOI: https://doi.org/10.33763/npndfi2024.03.065.

451. Про внесення змін до деяких актів Кабінету Міністрів України. постанова Кабінету Міністрів України від 28.07.2021 № 821. URL: https://zakon.rada.gov.ua/laws/show/821-2021-%D0%BF#Text.

452. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

453. Про регулювання товарообмінних (бартерних) операцій у галузі зовнішньоекономічної діяльності : Закон України від 23.12.1998 № 351-XIV. URL: https://zakon.rada.gov.ua/go/351-14.

454. Про деякі питання регулювання товарообмінних (бартерних) операцій у галузі зовнішньоекономічної діяльності : постанова Кабінету Міністрів України від 29.04.1999 № 756. URL: https://zakon.rada.gov.ua/laws/show/756-99-%D0%BF#Text.

455. Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами від 15.11.2019 № 2461. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423.

456. Міжнародний стандарт бухгалтерського обліку 2 (МСБО 2). Запаси. URL: https://zakon.rada.gov.ua/laws/show/929_021#Text.

457. Міжнародний стандарт бухгалтерського обліку 1 (МСБО 1). Подання фінансової звітності. URL: https://zakon.rada.gov.ua/laws/show/929_013#Text

458. Події після звітного періоду Міжнародний стандарт бухгалтерського обліку 10. Міжнародний документ № z0725-99 від 01.01.2012. Національне положення (стандарт) бухгалтерського обліку 10 "Дебіторська заборгованість" : затв. наказом Міністерства фінансів України від 08.10.1999 № 237. URL: https://zakon.rada.gov.ua/laws/show/z0725-99

459. План рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій та інструкція про його застосування : затв. наказом Міністерства фінансів України від 30.11.1999 № 291. URL: http://minfin.gov.ua/control/uk/publish/archive/main?cat_id=293534.

460. Яцик Т. В. Нормативно-правове забезпечення оподаткування операцій з крипто-активами в Україні та світі. *«Молодий вчений»*. 2019. № 8 (72). DOI: https://doi.org/10.32839/2304-5809/2019-8-72-31.

461. IFRS Standards apply to holdings of cryptocurrencies / IFRS. URL: https://www.ifrs.org/news-and-events/updates/ifric/2019/ifric-update-march-2019/.

462. Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами : проєкт Закону від 13.03.2022 № 7150. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/39211.

463. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні : проєкт Закону від 17.11.2023 № 10225. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/43232.

464. FATCA (Про податкові вимоги до іноземних рахунків : закон США) / міністерство фінансів України. URL: https://mof.gov.ua/uk/fatca-442.

465. MF Executive Board Completes the Fifth Review of the Extended Fund Facility Arrangement for Ukraine. *IMF*. 2024. October 18. URL: https://www.imf.org/en/News/Articles/2024/10/18/pr24381-ukraine-imf-executive-board-completes-fifth-rev-eff-arrangement.

466. Мінфін обговорив з операторами цифрових платформ концепцію запровадження звітності про доходи своїх користувачів. *Міністерство фінансів України.* 2024. URL: https://mof.gov.ua/uk/news/minfin_obgovoriv_z_operatorami_tsifrovikh_platform_kontseptsiiu_zaprovadzhennia_zvitnosti_pro_dokhodi_svoikh_koristuvachiv-4746.

467. Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32016L1164.

468. Освітній курс УНП ООН по криптовалютам. UNODC Global e-learning. 19. Cybercrime. *UNODC*. URL: https://www.unodc.org/elearning/en/courses/course-catalogue.html#cyber

469. Деякі питання єдиної державної інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : постанова Кабінету Міністрів України від 22.07.2020 № 627. URL: https://zakon.rada.gov.ua/laws/show/627-2020-%D0%BF#Text.

470. Деякі питання електронної взаємодії електронних інформаційних ресурсів : постанова Кабінету Міністрів України від 08.09.2016 № 606. URL: https://za--kon.rada.gov.ua/laws/show/606-2016-%D0%BF#Text.

471. Про поточну операційну діяльність Держфінмоніторингу. *ДСФМУ.* 2022. 18 берез. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/news/pro-potochnu-operaczijnu-diyalnist-derzhfinmonitoringu.html.

472. 3 questions for Alina Nedea, Head of Sanction Unit, DG FISMA European Commission. *August Debouzy.* 2023. URL: https://www.august-debouzy.com/en/blog/1951-3-questions-for-alina-nedea-head-of-sanction-unit-dg-fisma-european-commission.

473. Preventing abuse of the financial system for money laundering and terrorism purposes (until 2027). The European Commission. URL: https://eur-lex.europa.eu/EN/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes-until-2027.html.

474. Щодо міжвідомчої координації системи фінансового моніторингу. Держфінмоніторинг. *ДСФМУ.* 2022. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/news/shhodo-mizhvidomchoji-koordinaczizi-sistemi-finansovogo-monitoringu.html.

475. Із початку повномасштабного військового вторгнення рф кіберполіція попередила понад 300 кібератак на українські ресурси. *Національна поліція України.* 2022. URL: https://mvs.gov.ua/news/iz-pocatku-povnomasstabnogo-viiskovogo-vtorgnennya-rf-kiberpoliciya-poperedila-ponad-300-kiberatak-na-ukrayinski-resursi.

476. Про ринки капіталу та організовані товарні ринки : Закон України від 23.02.2006 № 3480-IV. URL: https://zakon.rada.gov.ua/laws/show/3480-15/print1491296480899025#Text.
477. Decentralised financial technologies: Report on financial stability, regulatory and governance implications. Financial Stability Board. *FSB*. 2019. April. URL: https://www.fsb.org/2019/06/decentralised-financial-technologies-report.
478. Virtual assets and virtual asset service providers. Supervisory money laundering/terrorist financing risk assessment methodology (draft). *IMF* A draft framework for money laundering/terrorist financing risk assessmentof a remittance corridor. 2021. September. URL: https://www.elibrary.imf.org/view/journals/063/2021/002/article-A001-en.xml
479. 2023 Review of The Fund's Anti-Money Laundering and Combating the Financing of Terrorism Strategy—Background Papers / IMF. 2023. November. URL: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Fund-s-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542020.
480. Knobel A. The IMF’s anti-money laundering strategy review is promising, but it all comes down to implementation. The Tax Justice Network. *The Tax Justice Network*. 2024. URL: https://taxjustice.net/2024/02/26/the-imfs-anti-money-laundering-strategy-review-is-promising-but-it-all-comes-down-to-implementation/.
481. Anti-money laundering and combating the financing of terrorism (AML/CFT) policies and measures / IMF. URL: https://www.imf.org/en/Topics/Financial-Integrity/amlcft.
482. Рада виконавчих директорів МВФ завершила третій перегляд програми в рамках механізму розширеного фінансування (EFF) для України. *IMF*. 2024. URL: https://www.imf.org/uk/News/Articles/2024/03/21/pr2496-ukraine-imf-executive-board-completes-third-review-eff.

483. Національна стратегія доходів до 2030 року : схв. розпорядження Кабінету Міністрів України від 27.12.2023 № 1218-р. URL: https://zakon.rada.gov.ua/laws/show/1218-2023-%D1%80#Text.

484. Про державно-приватне партнерство : Закон України від 01.07.2010 № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#n44.

485. Публічно-приватне партнерство у відносинах держави з міжнародними організаціями та транснаціональними компаніями : кол. наук. моногр./ за ред. Т. І.Єфименко; НАН України, ДУ «Ін-т екон. Та прогнозув. НАН України». Київ, 2015. 444с.

486. Мех Ю. В., Горобець Д., Головко В. Державно-приватне партнерство в секторі безпеки України: основні принципи та форми. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2022. Вип. 74 (2). С. 224–231. DOI: https://doi.org/10.24144/2307-3322.2022.74.72.

487. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. Київ : НІСД, 2018. 84 с.

488. Feedback Statement. Call for Input on Supporting the Development and Adopters of RegTech. Financial Conduct Authority / Financial Conduct Authority. 2016. URL: https://www.fca.org.uk/publication/feedback/fs-16-04.pdf.

489. Regulatory Intelligence. Thomson Reuters. *Thomson Reuters.* URL: https://regintel-content.thomsonreuters.com/

490. EBA analysis of RegTech in the EU financial sector. European Banking Authority / EBA. 2021. URL: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf.

491. Regulatory Technology. Rethinking Regulation / BearingPoint. URL: https://www.bearingpoint.com/files/RegTech_Brochure_BearingPoint.pdf.

492. Стратегія розвитку фінансового сектору України до 2025 року / НБУ. URL: https://bank.gov.ua/ua/file/download?file=Strategy_FS_2025_2020.pdf.
493. Стратегія розвитку фінтеху в Україні до 2025 року / НБУ. 2020. URL: https://bank.gov.ua/ua/files/DDWIAwXTdqjdClp.
494. Стратегія Національного банку України до 2025 року / НБУ. URL: https://bank.gov.ua/admin_uploads/article/Strategy_NBU_2021-2022.pdf.
495. Стратегія розвитку фінансового сектору України / НБУ. 2023. URL: https://bank.gov.ua/ua/news/all/strategiya-rozvitku-finansovogo-sektoru-ukrayini.
496. OECD Business and Finance Outlook 2021: AI in Business and Finance / OECD. 2021. URL: hhttps://doi.org/10.1787/ba682899-en.
497. Anti-Money-Laundering System AMLgo / UNODC. URL: http://goaml.unodc.org.
498. Tarawneh A., Abdul-Rahman A., Mohd Amin S. I., Ghazali M. F. A Systematic Review of Fintech and Banking Profitability. *International Journal of Financial Studies.* 2024. Vol. 12 (1). DOI: https://doi.org/10.3390/ijfs12010003.
499. The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities / World Bank Group. 2018. URL: https://www.worldbank.org/en/news/press-release/2018/10/11/bali-fintech-agenda-a-blueprint-for-successfully-harnessing-fintechs-opportunities.
500. Ready for the digital decade? Improving skills to meet the technological challenge in Ukraine. *EU4Digital*. 2021. URL: https://eufordigital.eu/ uk/ready-for-the-digital-decade-improving-skills-to-meet-the-technological-challenge-in-ukraine/.
501. Фінансова грамотність, фінансова інклюзія та фінансовий добробут в Україні у 2021 / DAI Global LLC. 2021. URL: https://bank.gov.ua/admin_uploads/article/Research_Financial_Literacy_Inclusion_Welfare_2021.pdf?v=4.

502. Дмитренко Т. Л., Терещенко Г. М. Підвищення інвестиційної грамотності на крипторинку. Освітня аналітика України. 2024. № 5. С. 55–65. DOI: https://doi.org/10.32987/2617-8532-2024-5-55-65.

503. Narula S. Achieving sustainability through financial literacy training. International Journal of Innovation and Sustainable Development. 2022. Vol. 16. Iss. 2. P. 197–213. DOI: https://doi.org/10.1504/IJISD.2022.121784.

504. Jayaraman J. D., Jambunathan S. Financial literacy among high school students: Evidence from India. Citizenship, Social and Economics Education. 2018. Vol. 17, Iss. 3. P. 168–187. DOI: https://doi.org/10.1177/2047173418809712.

505. Cristofaro M., Giardino P. L., Misra S., Pham Q. T., Hiep Phan H. Behavior or culture? Investigating the use of cryptocurrencies for electronic commerce across the USA and China. Management Research Review. 2023. Vol. 46, Iss. 3. P. 340–368. DOI: https://doi.org/10.1108/MRR-06-2021-0493.

506. Krylova L. V., Lukashenko I. V. Cryptocurrencies vs Central Banks' Digital Currencies: The Role of Financial Literacy. Finance: Theory and Practice. 2022. Vol. 26, Iss. 5. P. 220–232. DOI: https://doi.org/10.26794/2587-5671-2022-26-5-220-232.

507. Modjo M. I., Santoso F. Overconfidence Educated Young Males: A Study on Cryptocurrency Investors in Indonesia. 2022 International Conference on Information Management and Technology. ICIMTech. 2022. P. 630–633. DOI: https://doi.org/10.1109/ICIMTech55957.2022.9915258.

508. Zhao H., Zhang L. Financial literacy or investment experience: which is more influential in cryptocurrency investment? International Journal of Bank Marketing. 2021. Vol. 39, No. 7. P. 1208–1226. DOI: https://doi.org/10.1108/IJBM-11-2020-0552.

509. Fletcher E. Data Spotlight: Reports show scammers cashing in on crypto craze. Federal Trade Commission. 2022. URL: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze.

510. Стадник М. Популярні шахрайські схеми з криптовалютою. Як уберегти свою інвестицію. Вісник МСФЗ. 2021. № 8. URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ002526.
511. Навчальні матеріали «Фінансова грамотність. Фінанси. Що? Чому? Як?» для учнів 10, 11 класів / М-во освіти і науки України. URL: https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/navchalni-materiali-programi-pidruchniki-ta-navchalno-metodichni-posibniki/navchalni-materiali-finansova-gramotnist-finansi-shcho-chomu-yak-dlya-uchniv-10-11-klasiv.
512. План-конспект уроку з фінансової грамотності «Правила платіжної безпеки. Види шахрайства» для учнів середньої школи / Нац. банк України. 2022. URL: https://talan.bank.gov.ua/uploads/navchalni_materialy/plan-konspekt-do-uroku-pravila-platizhnoyi-bezpeki-vidi-shakhraistva-serednia-shkola.pdf?v=6.
513. Опис рамки цифрової компетентності для громадян України. Міністерство цифрової трансформації України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf.
514. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
515. Дмитренко Т. Л., Терещенко Г. М. Підвищення рівня освіти у сфері кібербезпеки, фінансової та цифрової грамотності як чинник зниження ризиків на ринку віртуальних активів. *Освітня аналітика України*. № 1 (22) 2023. DOI: https://doi.org/10.32987/2617-8532-2023-1-38-50.

ДОДАТОК А

Типологічні дослідження

Типологічне дослідження А.1. Silk Road (з англ. - " Шовковий шлях ") - анонімний торговий інтернет-майданчик, що знаходився в зоні .onion анонімної мережі Tor[2] і працював з 2011 по 2013 рік. Більшість товарів, що продавалися, було нелегально, проте власниками сайту були заборонені до купівлі-продажу крадені реквізити банківських карток, фальшиві гроші, дитяча порнографія, персональні дані, послуги кілера та зброя. Сайт був найбільш відомий як майданчик з торгівлі забороненими психоактивними речовинами, які становили 70% товарів, крім них, продавалися інші легальні та напівлегальні товари, наприклад, порнографія або електронні копії незаборонених книг, що охороняються авторськими правами.

Власник майданчика Росс Вільям Ульбріхт неодноразово заявляв про свої лібертаріанські погляди та критикував державні економічні регулювання[3].

Покупці та продавці проводять усі грошові операції через криптовалюту біткойн, яка у поєднанні з Tor може забезпечувати анонімність учасників угоди та неможливість блокування платежу. Для цього ж Silk Road у механізм платежів інтегрувала біткойн-міксер, що робить практично неможливим відстеження транзакцій. Покупці реєструються безкоштовно, а продавці зобов'язані купувати аккаунт через аукціон, щоб зменшити ризик шахрайства.

Станом на березень 2013 року в магазині продавалося понад 10 тисяч товарів, 70% з них — заборонені у всіх або більшості країн психоактивні речовини (340 видів)[4], найпопулярнішими з яких були MDMA, ЛСД та марихуана. Опіоїди, наприклад, героїн також були у продажу, проте попит на них був вкрай низький[5]. Правила магазину забороняли продаж дитячої порнографії, даних банківських карток, замовлення вбивств, зброї масового враження. На сайті також продавалася невелика кількість товарів, оборот яких не заборонено, наприклад, книги, ювелірні вироби, порнографія. Власник Silk Road відкривав для продажу зброї подібний магазин The Armory, але в 2012 закрив його через низький попит. На 2012-2013 роки щорічні продажі через Silk Road оцінювалися в 14-15 мільйонів доларів[6]. В якості валюти продавці та покупці використовують криптовалюту біткойн (BTC), яка могла надати анонімність та безвідкликаність транзакцій. Silk Road використовував хеджування по відношенню до долара США[7].

Silk Road іноді називають аналогом eBay або Amazon.com для нелегальних товарів. За даними, опублікованими ФБР після арешту Ульбріхта, за допомогою сайту за два з половиною роки було проведено 1,2 млн угод на 9,5 мільйонів біткойнів (за оцінкою Christopher Tarbell,

---

[2] A Trip Down The Revamped Silk Road Website . Дата звернення: 31 липня 2013 року.Архівовано 4 серпня 2013 року.

[3] *Andy Greenberg*. Сполучені Quotations of The Dread Pirate Roberts, Founder of Underground Drug Site Silk Road And Radical Libertarian (англ.) . Forbes (29 квітня 2013 року). Дата звернення: 2 жовтня 2013 року. Архівовано 12 червня 2018 року.

[4] James Ball (2013-03-22)."Silk Road: online market online place officials seem powerless to stop". The Guardian. Дата звернення: 28 квітня 2013 року. Архівовано 29 квітня 2013 року.

[5] The popular drugs bought with bitcoin on Silk Road - Quartz . Дата звернення: 22 січня 2014 року Архівовано 22 січня 2014 року.

[6] Bitcoin vs. Big Government - Reason.com . — «Silk Road, an encrypted website that has been operating with impunity for the past two years faciliting annual sales estimated at all $15 million." Дата звернення: 30 квітня 2013 року. Архівовано з оригіналу 16 травня 2013 року.

[7] Founder Of Drug Site Silk Road Says Bitcoin Booms And Busts Won't Kill His Black Market - Forbes . Дата звернення: 30 квітня 2013 року. Архівовано з оригіналу 16 травня 2013 року.

ФБР[8]). Комісії сайту (8-10% з угоди) склали понад 600 тис. біткойнів (близько 80 мільйонів доларів за цінами того періоду).

За документами судової справи над Ульбріхтом, Silk Road використовувався кількома тисячами продавців наркотиків та більш ніж 100 тисяч покупців. За словами ФБР, таке співвідношення між обсягом угод на сайті та кількістю біткойнів може свідчити про те, що основним використанням криптовалюти, за винятком спекулятивних інвестицій, була купівля нелегальних товарів.

2 жовтня 2013 року Вільям Росс Ульбріхт (Dread Pirate Roberts) був заарештований у Сан-Франциско . Його звинувачують у наркоторгівлі, хакерських атаках і змові з метою відмивання грошей. Агенти змогли заарештувати його завдяки виявленій канадським урядом посилці з дев'ятьма підробленими документами, відправленою до Сан-Франциско, які Ульбріхт планував використовувати з метою оренди серверів для Silk Road[9].

Ціна біткойна відреагувала на дану новину наступним чином: у перші кілька годин було різке падіння зі 124 до 82 доларів (66%), а потім відновлення до рівня 108 доларів (87%).

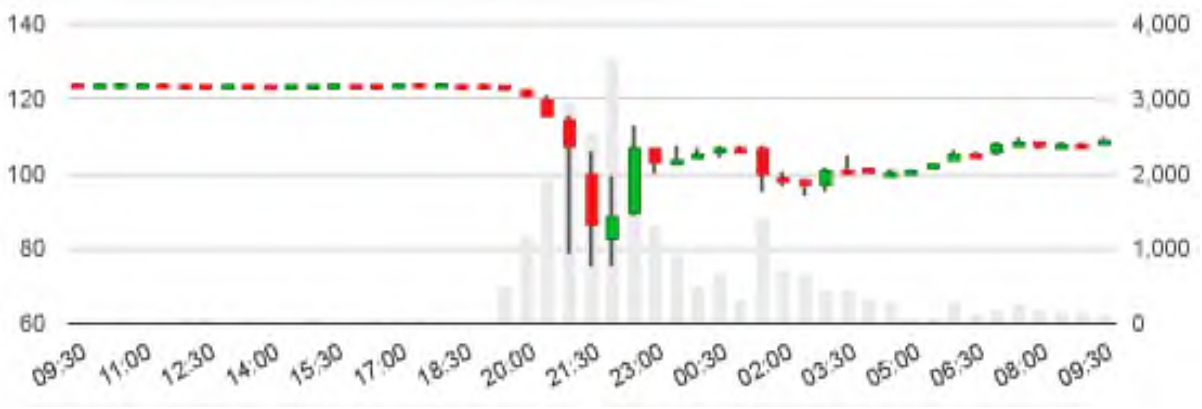


Рис.1. Реакція котирування біткойну на майданчику обміну BTC-E на новину про арешт Вільяма Росса Ульбріхта

Джерело: Troosh. Власна робота, CC BY-SA 3.0, URL: https://commons.wikimedia.org/w/index.php?curid=28831225

29 травня 2015 року суддя засудив Ульбріхта до довічного ув'язнення. Найбільші інвестори в біткойни брати Вінкельвосс, які планують запуск Winklevoss Bitcoin Trust в США після отримання дозволу, пов'язують зростання курсу біткойнів (станом на 22 січня 2014 року в 8 разів) після закриття Silk Road з тим, що біткойн перестав асоціюватись з Silk Road. Кемерон Вінкельвосс у своєму онлайн-інтерв'ю користувачам Reddit дав оцінку обороту Silk Road у біткойн-економіці. На його думку, вона становила 4%[10].

[8] Michelle Starr (2013-10-03). "FBI seizes online black market Silk Road, arrests owner" (англ.) . CNet, Australia. Архівовано 6 жовтня 2013 року . Дата звернення: 10 жовтня 2013 року . Silk Road has generated over 9.5 million Bitcoins in revenue from 1,229,465 transactions, collecting 614,305 Bitcoins in commissions.

[9] *Dan Goodin.* FBI: Silk Road mastermind couldn't even keep himself anonymous online. Memo to online crooks: Forget Tor exploits, sloppy opsec will get you every time. ArsTechnica (2 жовтня 2013 року). Дата звернення: 2 жовтня 2013 року . Архівовано 2 жовтня 2013 року.

[10] I am Cameron Winklevoss and I love me some Bitcoin AMA! : IAmA . Дата звернення: 29 вересня 2017 року. Архівовано 23 червня 2017 року.

Типологічне дослідження А 2. OneCoin (ванкойн, від One — одиниця, Coin — монета) — фінансова піраміда, яку рекламували як криптовалюту офшорні компанії OneCoin Ltd (розташована в Болгарії, зареєстрована в Дубаї) та OneLife Network Ltd (зареєстрована в Белізі), засновані Ружі Ігнатовою за участю Себастьяна Грінвуда. The Times охарактеризував це як «одне з найбільших шахрайств в історії»[11]

«Ванкойн» позиціонували як «цифрову валюту, яка базується на криптографії», як аналог біткойна. При цьому є істотні відмінності ванкойна від того, що зазвичай прийнято вважати криптовалютою:

• відсутня однорангова мережа, майнінгом займається виключно сама компанія «One Coin Limited»;

• будь-які операції доступні тільки через сайти, підконтрольні компанії (особистий кабінет, МЛМ мережа OneLife, платформа DealShaker);

• контроль над базою транзакцій знаходиться виключно у компанії-емітента «One Coin Limited», для інших користувачів вона недоступна у будь-якому вигляді.

Електронне видання CoinTelegraph, спеціалізацією якого є напрямок криптовалют, одним з перших став вважати, що OneCoin має ознаки фінансової піраміди[12]. Аналогічну оцінку давали й інші видання як з посиланнями на особливості створення, так і за значну роль в OneCoin багатьох людей, що раніше брали участь в інших подібних схемах. CoinTelegraph звертає увагу на те, що інформація про освіту і діяльність Ружі Ігнатової до створення OneCoin підтверджується лише посиланнями на пов’язані особисто з нею джерела.

За різними оцінками, по всьому світу у піраміду було вкладено від 4 до 15 млрд євро[13].

У 2017 році Ружа Ігнатова не з'явилася на запланований захід і виїхала з Болгарії. З тих пір про неї не було відомостей. Замість неї піраміду очолив її брат Костянтин Ігнатов. Згодом більшість лідерів зникли або були заарештовані, хоча Ружа Ігнатова так і не була затримана. Грінвуд був заарештований у 2018, а Костянтин Ігнатов у березні 2019. У листопаді 2019 року Костянтин Ігнатов визнав свою провину за звинуваченнями у відмиванні грошей та шахрайстві. Загальне максимальне покарання за звинуваченнями — 90 років ув'язнення.

Для продажу ванкойнів компанія «One Coin Ltd» використовувала мережевий маркетинг. За інформацією компанії, її основним бізнесом є продаж навчальних матеріалів з біржової торгівлі у вигляді відео-уроків, які навчають людей користуванню криптовалютами, тому юридично у компанії не виникало ніяких фінансових зобов'язань перед учасниками. Менеджмент та керівництво компанії спеціально наголошували на цьому у прес-релізах, у яких вказувалось, що ванкойни в особистому кабінеті користувача — лише інструмент для навчання людей працювати з криптовалютами, що вони не мають за собою ніякого реального забезпечення та не являють собою фінансові зобов'язання будь-якої юридичної чи фізичної

11 Bartlett, Jamie (15 грудня 2019). The £4bn OneCoin scam: how crypto-queen Dr Ruja Ignatova duped ordinary people out of billions — then went missing. *The Times*. Архів оригіналу за 15 грудня 2019. Процитовано 23 березня 2021.

12 One Coin, Much Scam: OneCoin Exposed as Global MLM Ponzi Scheme (англ.). Архів оригіналу за 27 грудня 2015.

13 Cryptoqueen: How this woman scammed the world, then vanished. *BBC*. 24 листопада 2019. Архів оригіналу за 21 грудня 2020. Процитовано 26 листопада 2019.

особи перед будь-ким. Безкоштовний ознайомчий пакет надає загальну інформацію про OneCoin та електронну книжку «Думай та багатій».

Навчальні пакети мали 7 рівнів з ціною від 110 до 118 000 євро[14]. Пакети надавали деяку кількість «токенів», які можна було «використати» для «видобутку» ванкойнів. Прямий продаж ванкойнів за фіатні гроші компанія «One Coin Ltd» не проводила, але їх можна було придбати у інших учасників на внутрішньому майданчику обміну. Обсяг дозволених операцій залежав від рівня купленого учасником навчального пакету.

Угорський національний банк видав попередження про те, що OneCoin є пірамідальною схемою[15].

28 квітня 2017 року Банк Таїланду випустив попередження проти OneCoin, заявивши, що це незаконна цифрова валюта, яка не повинна використовуватися в торгівлі[16].

12 липня 2017 р. Управління з фінансових ринків Австрії оприлюднило заяву, за якою компанія OneCoin не має права здійснювати банківські операції в Австрії, які вимагають ліцензії[17].

В 2018 році у Китаї правоохоронці стягнули 1,7 млрд юанів (267,5 млн дол. США), притягнувши до відповідальності 98 осіб, пов'язаних з OneCoin[18]

У 2021 Міністерство цифрової трансформації та Кабінет Міністрів України «зацікавилися співпрацею з фінансовою пірамідою OneCoin, яку позиціюють як криптовалюту»[19].

Заява болгарської Комісії з фінансового нагляду:

Болгарська Комісія з фінансового нагляду 30 вересня 2015 року опублікувала спеціальне повідомлення, присвячене OneCoin[20]. Потенційні інвестори інформуються про те, що придбання, торгівля і оплата через OneCoin та інші криптовалюти не регулюється існуючим в ЄС або болгарським національним законодавством про ринки капіталу. OneCoin, як й інші віртуальні валюти, не визнається і не розглядається як фінансовий інструмент. Потенційні інвестори попереджуються про те, що інвестиції в криптовалюти мають високий рівень ризику. У разі банкрутства організатора, подібні інвестиції не підлягають компенсації з «Фонду компенсацій інвесторам». Після попередження, OneCoin припинив всю діяльність в Болгарії і почав використовувати неболгарські банки для обробки платежів від болгарських учасників.

Управління з фінансового регулювання і нагляду Великої Британії:

---

[14] Finns investing millions in new virtual currency; police keeping tabs on case. Архів оригіналу за 14 березня 2016. Процитовано 3 березня 2019.
[15] Fokozott kockázatot hordoznak a világhálón elérhető virtuális fizetőeszközök (in Hungarian). *mnb.hu*. Архів оригіналу за 22 грудня 2016. Процитовано 22 грудня 2016.
[16] Bangkok Post (28 квітня 2017). BoT warns public about OneCoin currency.
[17] Austria's Financial Regulator Warns Onecoin Operating Without License. Архів оригіналу за 6 березня 2019. Процитовано 3 березня 2019.
[18] China prosecutes 98 people, recovers US$268 million in OneCoin cryptocurrency investigation, report says. South China Morning Post. Архів оригіналу за 29 травня 2018. Процитовано 29 травня 2018.
[19] Мінцифри та Кабмін зацікавилися співпрацею з фінансовою пірамідою OneCoin: деталі. *Новини України - #Букви* (укр.). 25 травня 2021. Процитовано 18 листопада 2022.
[20] СЪОБЩЕНИЕ — OneCoin [Архівовано 30 грудня 2015 у Wayback Machine.] // Комісія за фінансів нагляд 30/09/2015(болг.)

У вересні 2016 року Управління з фінансового регулювання і нагляду Великої Британії[en] (FSA) заявило, що OneCoin Ltd не робіть ніяких дій, які вимагають ліцензування, однак є стурбованість потенційними ризиками, які ця фірма створює для споживачів у Великій Британії. В заяві споживачів, які вважають, що вони були ошукані, закликали зв'язатися з лондонським поліцейським відділом шахрайства, яке веде відповідне розслідування[21].

Рішення Італійського антимонопольного управління:

Італійське антимонопольне управління в грудні 2016 року прийняло тимчасову заборону на діяльність компанії One Network Services Ltd. за просування і розповсюдження криптовалюти OneCoin, описуючи їх діяльність як «незаконну пірамідальну систему продажу» («sistema di vendita piramidale vietato dalla legge»). 27 лютого 2017 року після завершення розслідування регулятор заборонив всі дії з OneCoin до подальшого повідомлення[22].

Рішення Федерального управління фінансового нагляду Німеччини:

У лютому 2017 року Федеральне управління фінансового нагляду Німеччини заморозило 29 мільйонів євро на банківських рахунках, які використовувались для відмивання грошей в мережі OneCoin. Крім того, компанія IMS International Marketing Services GmbH отримала припис припинити всі несанкціоновані транзакції, пов'язані з OneCoin, і повернути останні грошові транзакції своїм інвесторам. У квітні 2017 року регулятор наказав «OneCoin Ltd» припинити весь бізнес в Німеччині і заборонив торгівлю ванкойнами[23].

Комітет державних доходів Міністерства фінансів Казахстану:

В квітні 2017 року Комітет державних доходів Міністерства фінансів Казахстану прокоментував «схему роботи псевдокріптовалютной піраміди OneCoin в Астані»[24]. На їх думку, «продукт OneCoin фактично не є криптовалютою, а являє собою аналог електронних платіжних одиниць, широко використовуваних в онлайн-іграх, відповідно, вся інформація, навіювана вкладникам компанії, про можливість отримання надприбутку, є злочинною вигадкою, спрямованою на незаконне заволодіння грошовими коштами вкладників».

Заява Комісії з фінансових послуг Белізу:

29 травня 2017 року Міжнародна комісія з фінансових послуг Белізу (IFSC) випустила попередження про те, що «OneLife Network Ltd» веде торговельну діяльність без ліцензії або дозволу від IFSC або будь-якого іншого органу. На адресу компанії було направлено пропозицію припинити незаконний торговий бізнес[25].

«В'єтнамська ліцензія»:

---

[21] London Police Investigate OneCoin Cryptocurrency Scheme. Архів оригіналу за 26 червня 2017. Процитовано 21 червня 2017.
[22] PS10550 - Vendite piramidali: Antitrust sospende la promozione della criptomoneta OneCoin da parte di One Life. *agcm.it*. Архів оригіналу за 8 травня 2017. Процитовано 12 березня 2017.
[23] BaFin (27 квітня 2017). OneCoin Ltd (Dubai), OneLife Network Ltd (Belize) und One Network Services Ltd (Sofia/Bulgaria): BaFin issues cease and desist orders holding the companies to stop own funds trading in "OneCoins" in Germany. Архів оригіналу за 4 жовтня 2018. Процитовано 3 березня 2019.
[24] Схему работы псевдокриптовалютной пирамиды разъяснили в КГД. Архів оригіналу за 5 серпня 2017. Процитовано 20 липня 2017.
[25] IFSC (29 травня 2017). One Life Network Limited. Архів оригіналу за 8 вересня 2017.

16 червня 2017 року від керівництва OneCoin Ltd. було поширено заяву про те, що OneCoin ліцензується урядом В'єтнаму і отримує законну можливість використання у В'єтнамі як цифрову валюту[26]. 20 червня 2017 року Міністерство планування та інвестицій В'єтнаму опублікувало заяву про підробку документу, який OneCoin використовував як доказ легалізації Міністерство почало перевірку щодо підробки державних документів та попередило людей і підприємства про пильність, якщо вони зіткнулися з цим документом.

Типологічне дослідження А 3. Quadriga Fintech Solutions була власником і оператором **QuadrigaCX**, яка вважалася найбільшою криптовалютною біржею Канади на момент її краху в 2019 році, коли біржа припинила роботу, а компанія оголосила про банкрутство з 215,7 мільйонами канадських доларів у зобов'язаннях і близько С Активи на 28 мільйонів доларів[27].

Генеральний директор і засновник компанії Джеральд Вільям Коттен помер у 2018 році після подорожі до Індії. До 250 мільйонів канадських доларів (190 мільйонів доларів США) у криптовалюті , які були заборговані 115 000 клієнтам, зникли[28] або до них не вдалося отримати доступ, оскільки лише Коттен мав пароль до автономних холодних гаманців[29].

За словами Chainalysis, фірми, що займається відстеженням криптовалют, Quadriga, ймовірно, ніколи не інвестувала довірені їй кошти. Кошти або не були отримані, або швидко пропали. «Що Quadriga насправді зробила з грошима, які клієнти дали їй для купівлі біткойнів, залишається загадкою», - повідомляє Chainalysis[30].

«Ернст енд Янг» було призначено незалежним спостерігачем, а «Квадризі» надано тимчасовий правовий захист від кредиторів відповідно до Закону про домовленості з кредиторами компаній. 8 квітня 2019 року компанія оголосила про банкрутство відповідно до Закону про банкрутство та неспроможність, оскільки можливість успішної реорганізації здавалася віддаленою[31].

Повідомляється, що Королівська канадська кінна поліція (RCMP) і Федеральне бюро розслідувань США (ФБР) розслідували компанію. Адвокати клієнтів біржі попросили ексгумувати тіло Коттена[32].

Джеральд Коттен (народився 11 травня 1988) жив у Бельвілі, Онтаріо, перш ніж відвідати школу бізнесу Шуліха при Йоркському університеті в Торонто. У 2010 році він закінчив Йорк,

---

[26] Behind MLM (20 червня 2017). OneCoin Vietnamese regulatory document forged, govt says. Архів оригіналу за 24 червня 2017. Процитовано 3 березня 2019.

[27] «Розслідування краху криптовалюти Quadriga виявило лише 28 мільйонів доларів активів» . Громадянин Оттави . Канадська преса . 13 травня 2019. Архів оригіналу за 14 травня 2019. Процитовано 14 травня 2019.

[28] *Вінья, Пол; Шиффлетт, Шейн (19 лютого 2019 р.).*" «Наші гроші пішли на щось»: клієнти шукають зниклі мільйони збанкрутілої криптобіржі» . *Wall Street Journal.* Архів *оригіналу за 19 лютого 2019 року*. Процитовано 20 лютого 2019 року.

[29] *Ligaya, Armina (4 лютого 2019).* «Найбільша канадська криптовалютна біржа Quadriga шукає захисту від кредиторів» . CTV News . *BellMedia.* Архівовано *з оригіналу 5 лютого 2019 року* . Процитовано 5 лютого 2019 .

[30] *Wieczner, Jen (24 квітня 2019).* «На біткойн припадає 95% криптовалютних злочинів, каже аналітик» . *Фортуна.* Архівовано *з оригіналу 27 квітня 2019 року* . Процитовано 27 квітня 2019 . *«Ми дуже швидко виявили, що Quadriga як біржа насправді не мала тих коштів клієнтів, які, як повідомлялося в ЗМІ, зараз були втрачені — цих коштів насправді ніколи не існувало», — пояснює Левін. Що насправді Quadriga зробила з грошима, які клієнти дали їй для покупки біткойнів, залишається загадкою.*

[31] *McDonald, Michael (8 квітня 2019).* «Суперечливу криптовалютну біржу QuadrigaCX оголосили про банкрутство» . CBC News . *Канадська преса.* Архівовано *з оригіналу 8.04.2019 року*. Процитовано 9.04.2019

[32] *«Квадрига: Юристи користувачів збанкрутілої криптофірми вимагають ексгумації засновника» . BBC. 14 грудня 2019 р. Процитовано 14 грудня 2019.*

отримавши ступінь бакалавра ділового адміністрування. У підлітковому віці Коттен уже брав участь у схемах Понці, використовуючи онлайн-розділ Scepter на онлайн-форумі TalkGold. Там Коттен рекламував HYIP (високоприбуткові інвестиційні програми), які «обіцяли дуже високі прибутки, але були нерегульованими та анонімними, розкриваючи мало або взагалі не розкриваючи подробиць про інвестиції або хто за ними стоїть», тоді як транзакції були анонімними та прихованими за допомогою цифрової валюти. Коттен таємно співпрацював із Майклом Патріном у цих схемах Понці. Коттен також продав «проксі-сервіс, який перенаправляв би інтернет-з'єднання користувача таким чином, щоб його IP-адреса була прихована»[33].

Коттен дізнався про біткойн у Торонто та поїхав до Ванкувера, Британська Колумбія, де в листопаді 2013 року разом із Майклом Патріном заснував Quadriga. Коттен і Патрін раніше були залучені в онлайн-схеми Понці, але хоча Патрін привернув увагу влади, причетність Коттена ще не була виявлена, тому чудова репутація Коттена дозволила йому бути публічним обличчям Квадриги[34].

Квадрига починала з того, що займалася виключно місцевими промислами. Їхній онлайн-обмін запустився після першого місяця. У січні 2014 року вони встановили другий біткоін-банкомат у Ванкувері. У 2014 році на Quadriga було обміняно біткоїни на суму 7,4 мільйона канадських доларів[35]. В інтерв'ю 2014 року засновник Джеральд Коттен пояснив, що компанія зберігає кошти клієнтів на паперових гаманцях у сейфах: «Тож ми просто надсилаємо їм гроші, нам не потрібно повертатися до банку кожного разу, коли ми хочемо. щоб вкладати в нього гроші. Ми просто надсилаємо гроші з нашого додатка для біткойнів безпосередньо на ці паперові гаманці та зберігаємо їх у безпеці»[36].

Компанія намагалася зібрати гроші та розмістити акцію на Канадській біржі цінних паперів (CSE), працюючи з Патріном. Компанія зібрала 850 000 канадських доларів, але скасувала плани вийти на біржу на початку 2016 року. У 2015 році у Quadriga було чотири співробітники з офісами у Ванкувері та Торонто, але до червня 2015 року гроші закінчилися.

У 2016 році Коттен став єдиним директором Quadriga, коли всі інші директори пішли у відставку. Крім кількох підрядників, після цього у нього не було працівників, офісів чи банківських рахунків. У 2017 році біткойн пережив спекулятивний ажіотаж, коли ціна зросла приблизно з 1000 доларів США до майже 20 000 доларів США. На Quadriga було обміняно біткоїни на суму близько 1,2 мільярда канадських доларів. Хоча велике збільшення обсягу збільшило комісійні, це також спричинило проблеми з грошовими потоками через залежність біржі від зовнішніх платіжних процесорів і відсутність у неї належної системи обліку. У червні

[33] *Hui, Stephen (14 лютого 2014).* «Geek Speak: Джеральд Коттен, генеральний директор Quadriga CX» . *Пряма Джорджія* . Архівовано *з оригіналу 2 лютого 2019 року.*
[34] *Річ, Натаніель (22 листопада 2019 р.).*«Схеми Понці, приватні яхти та зниклі 250 мільйонів доларів у криптовалюті: дивна історія Квадриги».*Ярмарок марнославства*. Процитовано 30 липня 2022.
[35] Кастальдо, Джо; Посадський, Олександра; Джессіка, Лідер; Jones, Lindsay (8 лютого 2019 р.).«Криптохаос: від Ванкувера до Галіфакса, розгадуючи таємницю зниклих мільйонів Квадриги». Глобус і пошта .Архівованоз оригіналу 9 лютого 2019 року. Процитовано 12 лютого 2019.
[36] *Alexander, Doug (15 лютого 2019).* «Покійний засновник Квадриги зберігав паролі біткойн клієнтів на папері, щоб вони не загубилися» . *Фінансовий пост* . Процитовано 19 червня 2019.

2017 року Quadriga оголосила, що втратила ефіріум на суму 14 мільйонів доларів США через помилку смарт-контракту[37].

Протягом 2018 року, коли ціни на біткойни падали, клієнти біржі повідомляли про затримки при спробі зняти долари. 28 мільйонів канадських доларів, збережених Costodian, платіжним процесором Quadriga, були заморожені Канадським імперським торговим банком (CIBC) у січні 2018 року. CIBC заявив, що вони не можуть визначити право власності на гроші та не можуть зв'язатися з ним. Коттен або Квадрига. У листопаді 2018 року справу було вирішено, рахунки передано до суду для індивідуального вирішення питання власності. Ні Костодіан, ні Квадрига не мали доступу до коштів[38].

Відповідно до судових документів, Quadriga також використовувала WB21 як платіжний процесор. Майкл Гастауер, виконавчий директор WB21, був названий у цивільному позові Комісії з цінних паперів і бірж США як частина шахрайства на 165 мільйонів доларів США. Інший платіжний процесор, який використовує Quadriga, Crypto Capital, був названий у цивільному позові, поданому генеральним прокурором Нью-Йорка в квітні 2019 року. У цій справі 851 мільйон доларів, довірений Crypto Capital, було «втрачено, викрадено або зникло», за позовом[39].

Квадрига використовувала незвичайну систему каси, щоб клієнти знімали свої гроші. Замість того, щоб платити клієнтам через банківські перекази, їм сказали прийти до непоказної будівлі в Лавалі, Квебек, щоб забрати готівку. Клієнти повідомили, що як тільки вони прийшли, в офісі нікого не було або не було готівки для видачі.

У січні 2019 року компанія Ernst & Young повідомила, що Quadriga не мала банківського рахунку, а використовувала сторонні платіжні процесори. Очевидно, у нього не було офіційної системи бухгалтерського обліку. Бізнесом керував зашифрований ноутбук Коттена з дому Коттена у Фолл-Рівері, Нова Шотландія.

Співзасновник Quadriga Майкл Патрін був ідентифікований The Globe and Mail як Омар Дханані, який був засуджений за звинуваченням у крадіжці особистих даних у США та відсидів 18 місяців у федеральній в'язниці. Дханані також визнав себе винним у крадіжці зі зломом і великому розмірі та був депортований до Канади. Bloomberg також ідентифікував Патріна як Дханані, показавши, що він офіційно змінив своє ім'я з Омара Данані на Омар Патрін у Британській Колумбії в березні 2003 року та змінив його знову на Майкл Патрін у жовтні 2008 року[40].

За словами Дженніфер Робертсон, вдови Коттена, він помер 9 грудня 2018 року під час подорожі Індією. Напередодні вона супроводжувала його до лікарні в Джайпурі, і йому поставили діагноз: септичний шок, перфорація, перитоніт і кишкова непрохідність. 9 числа він нібито помер після епізодів зупинки серця. 10 грудня свідоцтво про смерть було видано

---

[37] *Butcher, Jared (12 червня 2017).* «Мій смарт-контракт щойно з'їв 14 мільйонів доларів — що тепер? Переосмислення компенсації за ризики смарт-контракту». *Лексологія.* Архівовано *з оригіналу 2 лютого 2019р.*

[38] *Posadzki, Alexandra (13 листопада 2018).* «Суддя вирішує питання CIBC, передає право власності на спірні кошти Quadriga Верховному суду Онтаріо» . Глобус і пошта . Архівовано *з оригіналу 24 січня 2019.*

[39] Олександр, Даг; Leising, Matthew (26 квітня 2019). «Криптофірма, згадана у справі Bitfinex, також працювала з Quadriga». Bloomberg. Архівовано з оригіналу 28 квітня 2019 року . Процитовано 28 квітня 2019.

[40] *Олександр, Даг; Робінсон, Метт (19 березня 2019 р.).* «Злочинне минуле переслідує вижилого засновника проблемної криптобіржі» . *Bloomberg.* Архівовано *з оригіналу 27 березня 2019 року* . Процитовано 20.03.2019.

місцевим муніципалітетом, а також «свідоцтво про відсутність заперечень» від поліції для повернення тіла до Нової Шотландії.

У червні 2020 року Комісія з цінних паперів Онтаріо офіційно дійшла висновку[41], що Quadriga справді була шахрайством і схемою Понці. У ньому стверджувалося, що Джеральд Коттен вчинив шахрайство, відкривши рахунки під псевдонімами та приписавши собі фіктивні баланси валюти та криптовалюти, якими він торгував з нічого не підозрюючими клієнтами, і що «те, що сталося в Quadriga, було старомодним шахрайством, загорнутим у сучасні технології». Вдова Джеральда Коттена стверджувала, що нічого не знала про діяльність свого чоловіка, і погодилася конфіскувати активи на 12 мільйонів доларів.

5 лютого 2019 року суддя Верховного суду Нової Шотландії Майкл Дж. Вуд видав розпорядження про «30-денну зупинку, що виключає подачу позовів проти Quadriga», що є тимчасовим правовим захистом від її кредиторів відповідно до Закону про домовленості з кредиторами компаній, правового статус, який дозволяє неплатоспроможним корпораціям реструктуризувати свій бізнес і фінансові справи. Тим часом, щоб керувати фінансами компанії під час процесу, було призначено стороннього спостерігача, Ernst & Young. Аарон Метьюз працював директором з операцій. 6 лютого 2019 року компанія Ernst & Young повідомила, що біткойни на суму 468 675 канадських доларів були «ненавмисно» відправлені на недоступний холодний гаманець[42].

5 березня 2019 року суддя Вуд продовжив судовий захист Квадриги до 23 квітня. Він призначив Пітера Ведлейка з Grant Thornton головним директором з реструктуризації. Клієнти Quadriga заборгували 260 мільйонів канадських доларів у криптовалюті та готівкою. Було заплановано виплату 24,7 мільйонів канадських доларів із 300 000 канадських доларів для вдови Коттена, Дженніфер Робертсон , яка передала цю суму для початку судового розгляду; 200 000 канадських доларів отримають Ernst & Young, а ще 250 000 канадських доларів – її юристам; 229 842 канадські долари отримають юристи Quadriga; і 17 000 канадських доларів незалежним підрядникам[43]. Адвокат Quadriga, фірма Stewart McKelvey, відмовилася від участі у справі через потенційний конфлікт інтересів.

10 березня 2023 року арбітражний керуючий у справі про банкрутство Ernst & Young оголосив про перші проміжні дивіденди за ставкою 0,13 канадського долара за канадські долари підтвердженої вартості вимоги. Загальна сума першого проміжного дивіденду становить приблизно 40 000 000 доларів США. Виплата першого проміжного дивіденду підлягає сплаті Управлінням банкрутства приблизно 0,39% від дивіденду. Проміжні дивіденди передбачають розподіл приблизно 87,0% коштів, якими зараз володіє Довірена особа.

Топологічне дослідження A 4. Bitcoin Fog

Будівельна компанія встановлює анонімні біткойн-гаманці за допомогою вживаного ноутбука, підключеного до публічної мережі Wi-Fi у кав'ярні, а менеджер компанії щотижня вносить депозити в гаманець через анонімні біткойн-банкомати. Потім хабар передається міській владі за допомогою Bitcoin Fog, інструменту Deep Web, який додатково приховує передачу коштів. Під час розкішної відпустки міський чиновник переводить гроші на хабар за

[41] QuadrigaCX: Огляд персоналу Комісії з цінних паперів Онтаріо
[42] Олександр, Даг; Хариф, Ольга (13 лютого 2019). «Квадрига випадково перемістила більше біткойнів у недоступний гаманець» . Bloomberg. Архівовано з оригіналу 27 березня 2019 року. Процитовано 8.03.2019.
[43] Alexander, Doug (5 березня 2019). «Вдова засновника Квадриги вимагає відшкодування своїх витрат» . Bloomberg. Архівовано з оригіналу 5 березня 2019 року. Процитовано 16 березня 2019.

допомогою місцевих торговців біткойнами та банкоматів, майже не залишаючи слідів транзакції. Завдяки перевагам анонімності та відсутності методів виявлення хабарництво з використанням біткойнів створює серйозну проблему для правоохоронних органів. Навіть якщо викривач розкриє загальні подробиці скандалу, слідчі, ймовірно, зіткнуться з глухого кута [30].

Схоже, тенденція зростання використання криптоактиви для хабарництва та відкатів. Згідно з висновками Асоціації сертифікованих дослідників шахрайства (ACFE 2022), у 2021 році 8 відсотків випадків шахрайства в усьому світі стосувалися використання криптовалют. З цих випадків 48% стосувалися виплати хабарів і відкатів, тоді як 43% стосувалися конвертації розкрадених активів у криптовалюту.

Типологічне дослідження А 5. e-BTC. У 2017 році прокуратура США Північного округу Каліфорнії висунула звинувачення росіянину та його біткойн-обміннику e-BTC за 21 звинуваченням, зокрема у відмиванні грошей і веденні неліцензованого бізнесу з переказу грошей, за нібито причетність до міжнародної грошової операції. операція з відмивання, яка сприяла транзакціям криптоактиви на суму понад 4 млрд дол. США.

Підсудних звинувачують у тому, що вони використовували свою біржу, щоб допомогти злочинцям відмивати гроші та ухилятися від правоохоронних органів, надаючи їм анонімний доступ до криптоактиви.

Типологічне дослідження А 6. Liberty Reserve. У травні 2013 року Міністерство юстиції США висунуло звинувачення Liberty Reserve, компанії з переказу грошей у Коста-Ріці, і семи її співробітникам з відмиванням грошей і веденням незареєстрованого бізнесу з переказу грошей [46]. Відповідно до заяви Міністерства юстиції, компанія дозволила злочинцям поширювати, зберігати та відмивати доходи від незаконної діяльності, як-от шахрайство з кредитними картками, викрадення особистих даних і торгівля наркотиками, здійснивши анонімно понад 55 мільйонів незаконних транзакцій на суму понад 6 мільярдів доларів США. і безслідно. Міністерство фінансів визнало Liberty Reserve основним центром відмивання грошей і відключило його від фінансової системи США відповідно до розділу 311 Патріотичного акту США. Liberty Reserve мав понад мільйон користувачів у всьому світі, у тому числі 200 000 у США, і використовував власну віртуальну валюту Liberty Dollars, яка була деномінована та зберігалася в доларах США.

Користувачі можуть сплачувати додаткову комісію, щоб приховати номери своїх рахунків і зробити перекази неможливими для відстеження. Після того, як правоохоронні органи США дізналися про розслідування, Liberty Reserve зробив вигляд, що закрився в Коста-Ріці, але продовжив працювати через підставні компанії, переміщуючи мільйони доларів у кілька країн.

Типологічне дослідження А 7. Монети RG. У вересні 2020 року американське журі засудило засновника болгарський крипто обмінника RG монет за сприяння Інтернет-шахрайству та відмивання грошей.

За даними Міністерства юстиції США, Россен Іоссіфов, власник RG Coins, дозволив румунській злочинній організації відмивати крипто валюту через свій обмінник. Злочинці обдурили громадян США, пропонуючи підроблені товари на сайтах аукціонів, таких як eBay. Отримавши кошти жертв у фіатних валютах, шахраї перетворювали їх на крипто активи численними методами. Потім вони перетворили крипто активи назад у місцеву валюту через RG Coins і перерахували кошти через банківську систему.

Судові документи свідчать про те, що RG Coins здійснювали ці незаконні обміни крипто валют з вересня 2015 року по грудень 2018 року. За один дворічний період RG Coins сприяли обміну біткойнами на суму понад 4,9 мільйона доларів для організованої злочинної групи.

Типологічне дослідження А 8. P2P трейдери з Сінгапуру

У червні 2020 року влада Сінгапуру звинуватила 23-річну жінку, яка виступала в ролі неліцензійного торговця P2P. Жінка нібито отримувала кошти на свій Сінгапурський доларовий банківський рахунок від шахраїв. Шахраї заплатили їй комісію за конвертацію коштів у біткойни для подальшого відмивання. Їй було пред'явлено звинувачення в тому, що вона не отримала ліцензію на надання біржових послуг відповідно до закону про платіжні послуги Сінгапуру (PSA).

Типологічне дослідження А 9. Кібератака KuCoin

25 вересня 2020 року криптобіржа KuCoin, що базується в Сінгапурі, стала об’єктом великого злому. Кіберзлочинці викрали з біржі крипто активів на 281 мільйон доларів США, включаючи Bitcoin, Litecoin, XRP, Tether та ефір. Приблизно 152 мільйони доларів від загальної викраденої суми включали цілий ряд токенів на основі блокчейн-платформи Ефіріум.



Отримавши ці кошти, злочинці застосували складну серію методів відмивання. Вони переміщували кошти через послуги змішування, а також намагалися обміняти їх через DEX. Злочинці продали майже 20 мільйонів доларів викрадених токенів на DEX протягом одного тижня після злому. Більшість цих коштів були депоновані в DEX Uniswap та Kyber Network.

Типологічне дослідження А 10. Криптомонета «Platincoin» (PLC)

У провадженні ДЕР у місті Алмати знаходилась кримінальне впровадження №237500121000152, за фактом незаконної підприємницької діяльності за ознаками кримінального правопорушення, передбаченого ст. 214 ч. 1 КК РК. За даними Міжнародного фінансового центру Астана – у «Platincoin» відсутня ліцензія надання фінансових послуг з цифровими активами. За даними Міністерства цифрового розвитку, інновацій та

аерокосмічної промисловості РК – «Platincoin» за дозволом випуск і оборот незабезпечених цифрових активів не зверталися, повідомлення початку діяльності не направляли.

«Platincoin» - платформа, яка пропонує навчальний проект, інноваційну технологію гібридного ланцюжка блоків, сучасну бізнес – платформу та соціальну мережу. Люди, які стоять за цією програмою, позиціонували себе як глобальний проект, метою якого є об'єднання людей по всьому світу і надання їм унікальної можливості, яка змінить їхнє життя.

Реєстрація облікового запису на платформі «Platincoin» доступна лише за кодом запрошення (посилання). За наявністю посилання користувач отримує можливість завантажити програмне забезпечення на телефон і приступити до здійснення торгових операцій. При реєстрації клієнту обіцяють стабільно отримувати 30% на рік протягом наступних 10 років із щоденними виплатами відсотки нараховуються у вигляді монети PLC.

Вкладникам було запропоновано придбати ліцензії (ферми). Так, вартість першої категорії ліцензії складає 110 ЄВРО, другий вид категорії становила 275 ЄВРО, третій вид становив 550 ЄВРО і четвертий вид становив 1100 ЄВРО.

Ферма - це ліцензія, яка дає право на мінтинг (видобуток) монет. Видобуток монет залежить від місткості ферми відповідно від вартості ферми. Ферму купують за крипто долари USDT. Для покупки USDT необхідно зареєструватися на платформі криптобіржі Binance, Coinsbit, де після реєстрації організаторами платформи «Platincoin» відкривався особистий кабінет із гаманцем. Далі в даному додатку необхідно було перейти у розділі торгівля, де є була надана можливість купити USDT та інші валюти. При купівлі USDT при виборі способу оплати надана можливість купити USDT у великої кількості продавців. На куплені та перераховані до Ultimafarm.com USDT, здійснювалась оплата ферми.

Більше того, кожному учаснику пропонується залучити нових вкладників та отримати бонус у вигляді 20% від вкладеної суми останнього, проте бонуси нараховуються у вигляді монети PLC, для зняття яких вкладники за переказом на біржу «Coincbit» мали можливість обміняти монети PLC на USDT за курсом монети. Після продажу монет за USDT криптоактиви з біржі Coincbit переводилися на біржу Binance. У свою чергу USDT продавалася за поточним курсом долара США і виводилися на банківські рахунки вкладників.

В даному кримінальному впровадженні співорганізатор платформи «Platincoin» за поданими до нього звинуваченнями потерпілих вкладників визнав вину і повністю відшкодував завдані ним збитки. За законодавством Республіки Казахстан і в порядку медіації досудового слідства суд прийняв рішення провадження у кримінальній справі припинити за примиренням сторін.

На глобальному ринку за інформацією Bloomberg із посиланням на дані Crypto Fund Research зафіксували різке зростання кількості криптофондів у 2024 році. Із січня до березня на ринку з’явилося 25 орієнтованих на криптовалюту венчурних і хедж-фондів, що є максимальним показником із II кварталу 2021 року.

ДОДАТОК Б

Анонімні криптовалюти

У XXI столітті люди прагнуть бути обережними у всіх справах. Багато інвесторів обирають анонімні криптовалюти, оскільки це дозволяє захистити їхні персональні дані від доступу третіх осіб.

Анонімні криптовалюти можна порівняти з готівкою. Коли люди знімають гроші в банкоматі, операція фіксується, але все, що станеться з цією сумою далі, залишається таємницею. Концепція анонімності криптовалюти працює аналогічно.

Звичайні криптовалютні біржі вимагають перевірки особистості, через що альткоїни можуть бути відстежені, а витрати проаналізовані. Відмінність анонімних активів полягає в тому, що після зарахування на електронний гаманець їх рух стає неможливо відстежити. Користувачі також можуть конвертувати ці активи у фіатні гроші.

Псевдоанонімні криптовалюти розкривають особу власника, але фінансові операції залишаються прозорими та легко відстежуваними. Щоб уникнути прив'язки до конкретного користувача, фахівці радять вводити нову адресу для кожної транзакції. Однак важливо розуміти, що всі операції в блокчейні Bitcoin можна відстежити. Далі в огляді ми розглянемо 10 анонімних криптовалют, транзакції з якими неможливо відстежити.

1.	**Monero**	Анонімність у Monero включена за замовчуванням, але операції займають більше часу. Легко приховати особу відправника і отримувача коштів, а також суму монет, які передаються.
2.	**Dash**	Dash — це безпечна та анонімна криптовалюта, створена як альтернатива Bitcoin з підвищеним рівнем безпеки. Вона повністю децентралізована і не залежить від зовнішніх регуляторів.
3.	**Komodo**	Платформа використовує інноваційну технологію, де всі проєкти є незалежними блокчейнами, які приєднуються до спільної екосистеми. Можна створювати власні анонімні блокчейни.
4.	**Zcash**	Це цифрова валюта, яка працює на базі вихідного коду Bitcoin. Транзакції надійно захищені, забезпечуючи повну конфіденційність. Для операцій потрібно вводити спеціальну адресу, від якої залежить анонімність.
5.	**Bytecoin**	Ця криптовалюта була створена в 2012 році. Анонімність забезпечується за допомогою кільцевих підписів і прихованих адрес. Переклади здійснюються швидко і їх неможливо відстежити.
6.	**Bitcoin Private**	Ця криптовалюта працює на основі комбінації Bitcoin і ZClassic. Це фактично форк першого у світі блокчейну. Операції проводяться без посередників, монета безпечна і анонімна.

7.	**Verge** 	Криптовалюта Verge спрямована на захист конфіденційних даних. Вона була запущена у 2014 році і використовує технології TOR та I2P для захисту особистих даних користувачів.
8.	**NavCoin** 	Популярна анонімна криптовалюта, яка з'явилася в 2014 році. Валюту вдосконалили, і тепер операції здійснюються через засекречені транзакції.
9.	**PIVX** 	Ця валюта забезпечує миттєве підтвердження транзакцій. Спочатку вона носила назву Darknet, але пізніше була перейменована.
10.	**Zcoin** 	Транзакції фіксуються в публічному реєстрі, але для забезпечення анонімності використовується механізм «чеканки». Цифрові активи знищуються, створюючи закриту криптовалюту без історії операцій.

Джерело: Топ-10 популярних у 2023 році анонімних криптовалют. Binance Square. URL: https://www.binance.com/ru-UA/square/post/250453

Головною перевагою є конфіденційність. Можна приховати будь-яку суму операцій. Транзакції є анонімними. Однак, є і недоліки, такі як вища вартість операцій та відсутність можливості вбудовувати скрипти в транзакції.

У будь-якому випадку потрібно бути обережним. Останнім часом активізувалися шахраї, які можуть переглядати старі записи операцій, оскільки оновлення стосується лише нових транзакцій.

ДОДАТОК В

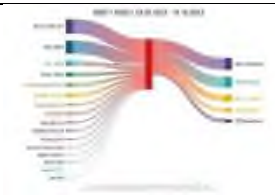
Блокчейн-аналітичні програми

Впровадження політик і процедур ПВК/ФТ для постачальників послуг, пов'язаних з обігом віртуальних активів (ППВА), та фінансових установ, які обслуговують ППВА і співпрацюють з ними, вимагає постійної оцінки ризиків діяльності крипторинку—учасників, інструментів і транзакцій. У відповідності з розвитком цифрового світу ці завдання виконуються спеціалізованими програмами від компаній, що займаються блокчейн-аналітикою. Наразі таких компаній багато, оскільки кожна країна намагається мати власний програмний продукт. Проте, з історичної точки зору і на основі глибини розробки цих програм і їхніх баз даних, можна виділити лідерів галузі. Незважаючи на схожі підходи до оцінки ризиків, програмні продукти конкурують через свої інтерфейси, напрямки досліджень, на які вони зосереджують увагу, регіональне охоплення послуг та типи клієнтів—державні правоохоронні і регуляторні органи, приватний сектор, фінансові компанії та банки, і ППВА.

Огляд блокчейн-аналітичних продуктів дозволяє обрати програмне забезпечення, яке найкраще підходить для їхньої діяльності. Однак використання кількох програм завжди дає перевагу, хоча це може бути дорогим задоволенням. Необхідно розробляти бізнес-рішення, які забезпечують доступ до кількох постачальників. Давайте порівняємо деяких лідерів цієї індустрії.

Вибір програмного продукту є особистим рішенням клієнтів і професійних операторів на крипто- і фінансових ринках. Однак, щоб оцінити ризик діяльності крипторинку в кожній юрисдикції, важливо проаналізувати, які програмні продукти використовуються в їхньому регіоні та скільки користувачів використовують аналітичні програми блокчейну. Ця інформація може бути частиною галузевої оцінки ризиків діяльності на крипторинку та впровадження 15 Рекомендації FATF.

Chainalysis	Crystal Blockchain	Global Ledger	Elliptic	TRM Labs
Підтримувані платформи				
Windows Mac Linux **SaaS / Web** **On-Premises** iPhone iPad Android Chromebook	Windows Mac Linux **SaaS / Web** On-Premises iPhone iPad Android Chromebook	Windows Mac Linux **SaaS / Web** On-Premises iPhone iPad Android Chromebook	Windows Mac Linux **SaaS / Web** On-Premises iPhone iPad Android Chromebook	Windows Mac Linux **SaaS / Web** On-Premises iPhone iPad Android Chromebook

Користувачі				
Організації, які мають запобігати, виявляти та розслідувати відмивання грошей у криптовалюті, шахрайство та порушення комплаєнсу	Агентства та організації, зацікавлені в інструменті розслідування блокчейну для відображення підозрілих транзакцій і пов'язаних осіб	Компанії, які шукають рішення для відстеження цифрових активів і відповідності AML	Криптобізнес і фінансові установи шукають рішення для аналітики, навчання та сертифікації блокчейну	Державний сектор, фінансові установи та крипто-бізнес, які потребують відповідності цифрових активів і рішення для управління ризиками для моніторингу, виявлення та розслідування криптовалютного шахрайства та фінансових злочинів
Зображення та відеопрезентація				
				
API				
Пропозиція API	Пропозиція API	Пропозиція API	**Пропозиція API**	**Пропозиція API**
Цінові пропозиції				
Інформація відсутня. Безкоштовна версія Безкоштовне випробування	Інформація відсутня. Безкоштовна версія Безкоштовне випробування	Інформація відсутня. Безкоштовна версія **Безкоштовне випробування**	Інформація відсутня. Безкоштовна версія **Безкоштовне випробування**	Інформація відсутня. Безкоштовна версія Безкоштовне випробування
Підтримка				
Підтримка по телефону **Цілодобова підтримка в реальному часі** **Онлайн**	**Підтримка по телефону** Цілодобова підтримка в реальному часі **Онлайн**	Підтримка по телефону Цілодобова підтримка в реальному часі **Онлайн**	**Підтримка по телефону** **Цілодобова підтримка в реальному часі** **Онлайн**	**Підтримка по телефону** **Цілодобова підтримка в реальному часі** **Онлайн**

Навчання				
Документація **Вебінари** **Наживо онлайн** **Особисто**	**Документація** Вебінари Наживо онлайн **Особисто**	**Документація** **Вебінари** Наживо онлайн **Особисто**	**Документація** **Вебінари** **Наживо онлайн** **Особисто**	**Документація** **Вебінари** **Наживо онлайн** **Особисто**
Інформація про компанію-розробника				
Chainalysis Founded: 2014 United States www.chainalysis.com	**Crystal Blockchain** Founded: 2018 Netherlands crystalblockchain.com/	**Global Ledger** Founded: 2018 Switzerland globalledger.io	**Elliptic** Founded: 2013 United States www.elliptic.co	**TRM Labs** Founded: 2017 United States www.trmlabs.com
Сфери моніторингу				
Аналіз блокчейну Безпека блокчейну Відповідність Крипто Crypto Compliance Виявлення шахрайства	ПВК/ФТ Аналіз блокчейну Дослідники блокчейну Crypto Compliance	ПВК/ФТ Crypto Compliance Виявлення шахрайства	ПВК/ФТ Аналіз блокчейну Безпека блокчейну Crypto Compliance Децентралізована ідентифікація Управління фінансовими ризиками Виявлення шахрайства	Аналіз блокчейну Моніторинг блокчейну Crypto Compliance
Альтернативні блокчейн-аналітичні програми				
CipherTrace **Scorechain** **BitRank Verified** Blockchain Intelligence Group	**AMLbot** **Purefi** **Validus** Eventus	**Signal21** **QLUE** Blockchain Intelligence Group	**AnChain.AI** **Breadcrumbs**	**Acuant** **Coinbase Analytics** Coinbase

Джерело: The Complete Software Platform. SourceForge. URL: https://sourceforge.net/

Додаток Г

Анкета для опитування:

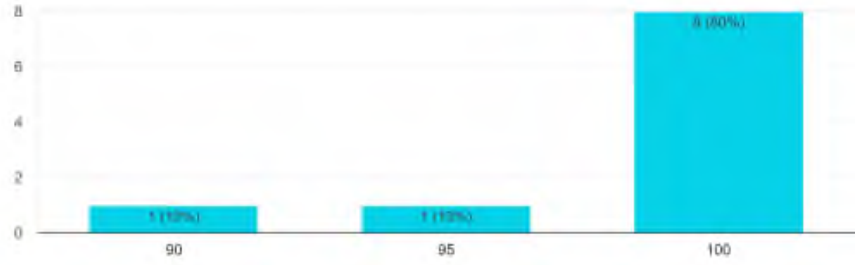
Значущість критеріїв ризику використання ВА в злочині ВК/ФТ.

https://forms.gle/Ha8TFRJsbxAJy5EA6

Позначте (оцініть) від 100 до 0 ризик критеріїв, що перелічені нижче:

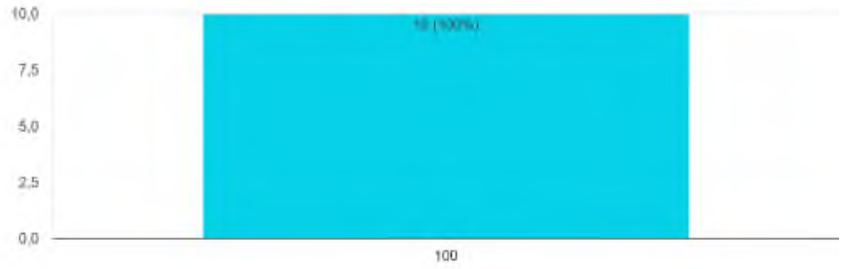
1. Постійне користування анонімізаторами (міксери, монети з підвищеною анонімністю та інші способи приховування інформації про адреси криптогаманців та криптотрансакції).

10 відповідей



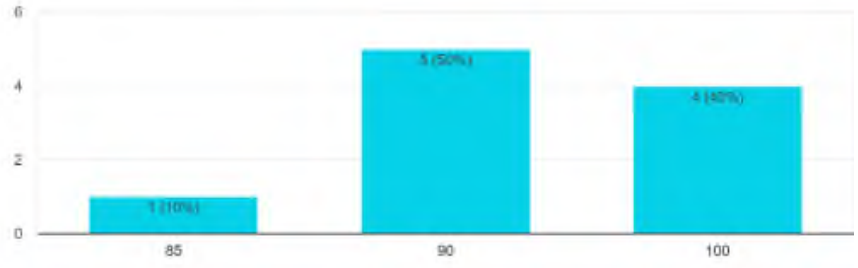
2. Трансакції у високоризикових індустріях (онлайн-азартні ігри, недозволені товари в Даркнеті, торгівля зброєю, наркотиками, людьм...ми мистецтва та індустрії для дорослих тощо).

10 відповідей



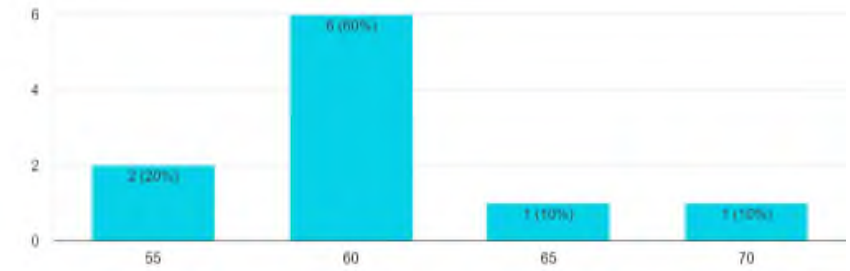
3. Присутність у списках санкцій окремих країн та міжнародних організацій.

10 відповідей



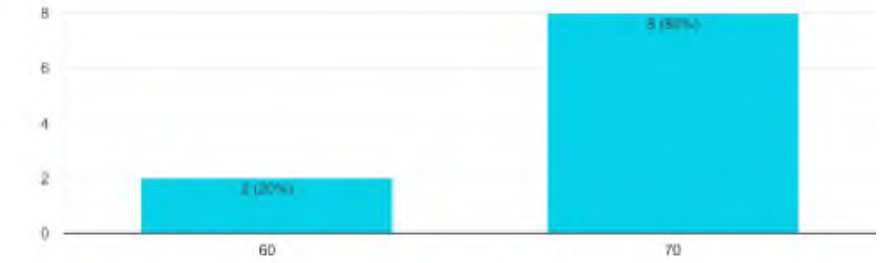
4. Швидке зняття готівки після депозитів.

10 відповідей



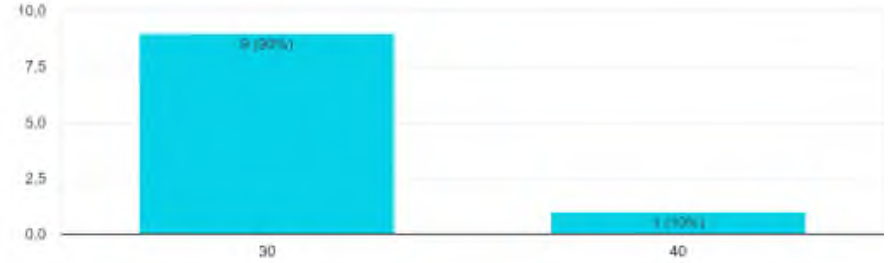
5. Часті придбання віртуальних активів на великі суми.

10 відповідей



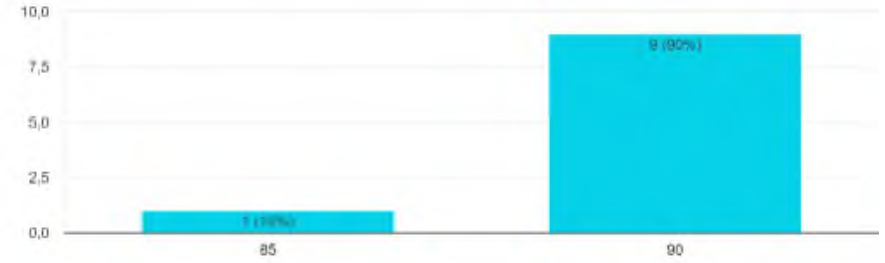
6. Різкі зміни ціни на віртуальні активи, які не відповідають загальному ринковому тренду (котируванням на криптобіржах).

10 відповідей



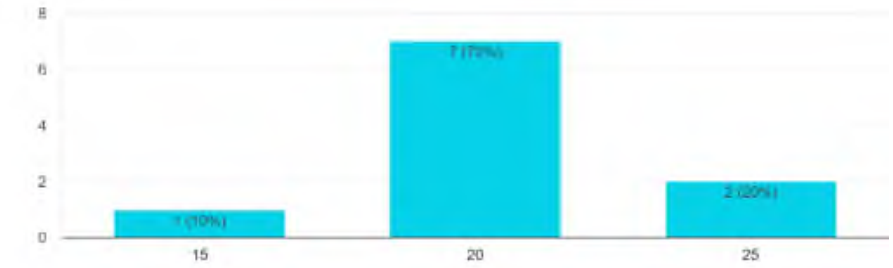
7. Трансакції з особами чи певними локаціями з показником високого ризику.

10 відповідей



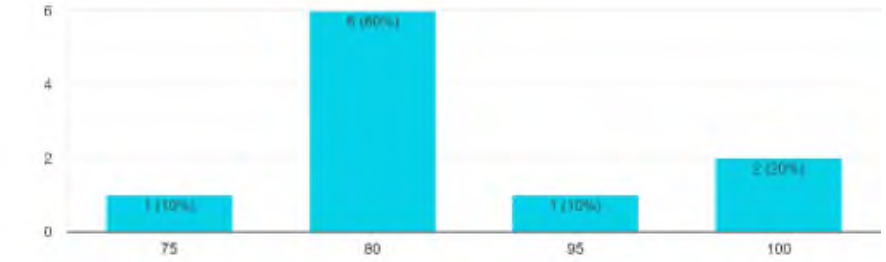
8. Негативне висвітлення клієнтів у медіа.

10 відповідей



9. Незвичні трансакції та типології використання ВА у ВК.

10 відповідей



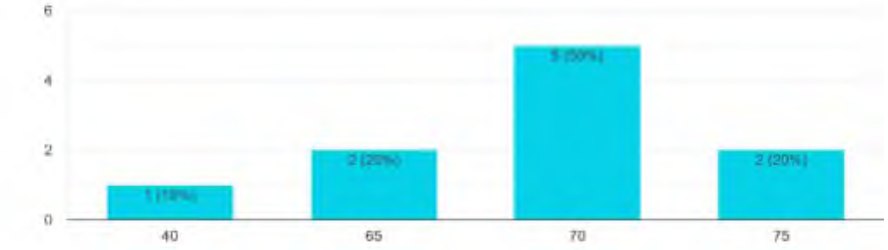
10. Короткострокова активність на криптогаманцях із нульовим залишковим балансом та взаємодія між криптогаманцями з такою ознакою.

10 відповідей



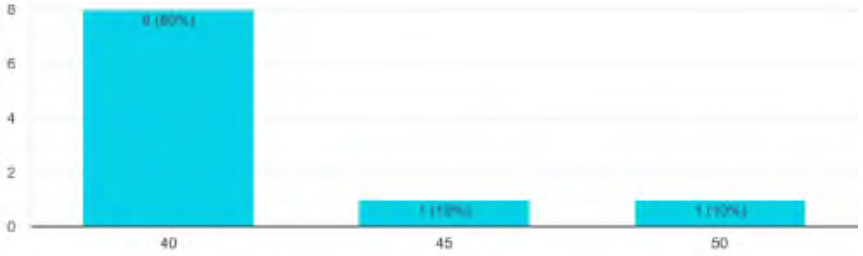
11. Підозрілі або незрозумілі джерела коштів.

10 відповідей



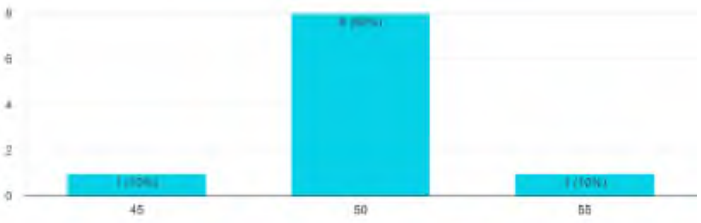
12. Неповна або недостовірна інформація про клієнта.

10 відповідей



13. Кримінальне фінансове минуле клієнтів

10 відповідей



Матриця рангів критеріїв оцінки ризику за ознаками використання ВА у ВК

Показник	Критерії												
	1	2	3	4	5	6	7	8	9	10	11	12	13
Бальна оцінка	100	100	90	60	70	30	90	20	80	10	70	40	50
Рейтингова оцінка	1-2	1-2	3-4	8	6-7	11	3-4	12	5	13	6-7	10	9
Стандартизований ранг	1,5	1,5	3,5	8	6,5	11	3,5	12	5	13	6,5	10	9

Оцінювання показників порівняльної важливості критеріїв

Показник		Сума рангів	Середній ранг	Середнє значення в балах	Частота максимально можливих оцінок	Середня вага (нормована оцінка)	Коефіцієнт активності експертів	Розмах
КРИТЕРІЇ	1	595.0	17.5	88.235	0.3236	0.029	1	30
	2	595.0	17.5	96.765	0.6765	0.032	1	10
	3	596.0	17.52	90.882	0.3530	0.030	1	30
	4	589.5	17.33	48.529	0	0.016	1	50
	5	610.8	17.96	67.941	0	0.023	1	30
	6	582.0	17.11	37.647	0	0.013	1	30
	7	595.0	17.5	90.588	0.2353	0.030	1	20
	8	535.5	15.75	25.882	0	0.009	1	30
	9	620.0	18.23	81.765	0	0.027	1	20
	10	425.0	12.5	16.765	0	0.006	1	20
	11	598.5	17.60	64.706	0	0.022	1	50
	12	595.0	17.5	54.412	0	0.018	1	40
	13	572.0	16.82	50.882	0	0.017	1	50

Джерело: Побудовано автором

Респонденти:

1.	Михайло Тютін	CTO Varager	mihatiutin@gmail.com
2.	Олексій Фісун	CEO Global Ledger	alex@glprotocol.com
3.	Святослав Дубовський	Віце-президент Crystal	sviatoslav.dubovskyi@crystalblockchain.com
4.	Вячеслав Демчук	CEO AMLbot	vycheslav.demchuk@gmail.com
5.	Ганна Терещенко, к.е.н.	Заступник директора ДУ «Інститут освітньої аналітики»	tganna75@gmail.com
6.	Олександр Черних	Адвокат, Національна асоціація адвокатів України	Alexandrchas@gmail.com
7.	Тетяна Гудима, д.ю.н.	Завідувач відділу ДУ «Інститут економіко-правових досліджень імені В.К. Мамутова НАН України»	tsgudima@gmail.com
8.	Євгеній Панченко, майор поліції	Перший заступник Департаменту міжнародного поліцейського співробітництва Національної поліції України	yevhenii.panchenko@cyberpolice.gov.ua
9.	Владислав Цвіркун	Віце-президент Global Ledger	vladyslav.t@globalledger.io
10.	Юрій Королюк, д-р з держ. упр.	професор кафедри менеджменту, маркетингу та міжнародної логістики ДУ «Чернівецький торгово-економічний інститут Київського національного торгово-економічного університету»	yu_kor@ukr.net

Додаток Ґ

ПЕРЕЛІК

постачальників послуг, пов'язаних з оборотом віртуальних активів, які співпрацюють із банками російської федерації та республіки білорусь

Постанова Верховної Ради України від 14.07.2023 № 3260-IX

Про схвалення пропозицій щодо застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) до представників спортивних організацій російської федерації та республіки білорусь

Джерело: URL: https://zakon.rada.gov.ua/laws/show/3260-IX#Text

Назва Інтернет-сайту	Інтернет-сайт	Резидентність	Назва хостинг-провайдера	Обсяг проведених операцій	Криптоадреса
1-online.ru	https://1-online.ru	russia	Cloudflare, EUROHOSTE, ONLINE SAS	300m-100m	0x02Fc99de3EeC90462f5380500E6De02e44eab212 (ETH); rJkHCKFxfAEV4cW3jQD2ksdEnGKm5XonF4 (XPR);
abcobmen.com	https://abcobmen.com	Estonia	Cloudflare, HETZNER-AS	300m-100m	0x0A03A9398E123Ed7891697963a9207c21A2bA905 (ETH)
bankcomat.org	https://bankcomat.org	russia	INCAPSULA, WORLDSTREAM, NFORCE, CLOUDNSNET, PUBLICLOUD, LEASEWEB-USA-WDS	300m-100m	39CkqPSXMa7W3NZx1SXcu5cX6GW55Nuuov (BTC)

bitcoin24.su	https://bitcoin24.su	Kazakhstan	OVH, HETZNER-A, PAGMA-AS, SELECTEL, GD-EMEA-DC-SXB1	300m-100m	bc1qqukp9f7fg78axl83cymr8rkgs8fsxs27vax9c6 (BTC)
bitokk.biz	https://bitokk.biz	russia	Cloudflare, SYTRA, YNDX	300m-100m	
cashex.cc	https://cashex.cc	russia	Cloudflare	300m-100m	14FN5kLZihTh94d4uJ4cXCNaNLuhnQhXku (BTC)
coinpaymaster.com	https://coinpaymaster.com	UAE	Cloudflare, AS-REG	300m-100m	0x0E4010C06Bf637FEB2d37749bB1CfbF6Ace7B9d6
cryptomax.ru	https://cryptomax.ru			cryptomax.ru	https://cryptomax.ru
ex-money.cc	https://ex-money.cc	Estonia	HURRICANE, INCAPSULA, WORLDSTREAM	300m-100m	
exbox.org	https://exbox.org	russia	Cloudflare, Google	300m-100m	
exchangeteam.cc	https://exchangeteam.cc	Switzerland	Cloudflare, Google	300m-100m	0xac509F87420B61Cd4e3bEaC9F541337D4Ab064f0 (ETH)
grandchange.cc	https://grandchange.cc	Estonia	Cloudflare, Namecheap	300m-100m	0x65e4900912A50b7CF07Df5001Eb50AeFE298812f (ETH)

multichange.net	https://multichange.net	Estonia	HURRICANE, LEASEWEB-NL-AMS-01, INCAPSULA	300m-100m	32wNw8XYzesv9xu49DDJ4oLHKWAzNY7bqF
nicechange.net	https://nicechange.net	Estonia	HURRICANE, INCAPSULA, WORLDSTREAM	300m-100m	0x0004c7A4f784816BeaC3bA3DdDD6d8fB13edC983 (ETH)
papa-change.com	https://papa-change.com	Germany	Cloudflare, SYTRA, YNDX	300m-100m	0x5FD2CCc9e2a02666d76fFd6e43779c5cEcc6087b (ETH) (f-change.biz)
wiki-exchange.com	https://wiki-exchange.com	Estonia	NAMECHEAP, AMAZON-02	300m-100m	0x257d3AB276Cf45e835990259E588Bb6223548b5f (ETH)
yochange.com	https://yochange.com	russia	Cloudflare, ZOHO-AS	300m-100m	0x0F22b8164AB4dcD108C3413a0D67d6411c3E8F54 (ETH)
4money.me	https://4money.me	russia	Cloudflare, EUROHOSTER	100m-50m	
100bitcoins.com	https://100bitcoins.com	Ukraine	Cloudflare, GOOGLE, WEBARMOR, DE-FIRSTCOLO	100m-50m	
alfa.exchange	https://alfa.exchange	UAE	Cloudflare, ZOHO-AS, COMPUTERLINE	100m-50m	
bitality.cc	https://bitality.cc	russia	Cloudflare, NAMECHEAP-NET	100m-50m	

bitcoin-24.pro	https://bitcoin-24.pro	russia	Cloudflare, GOOGLE	100m-50m	
bithunter.io	https://bithunter.io	russia	Cloudflare, GOOGLE, AS-REG	100m-50m	rKTvGAubDAist9H9YXW VTUrG6hs4 PgDtgu (XPR)
blablachange.com	https://blablachange.com	Estonia	Cloudflare, NAMECHEAP-NET	100m-50m	rLeDsLUW8hxin3FLc6aqd9 JXeDu8tk 7Xyq (XPR)
cashadmin.ru	https://cashadmin.ru	russia	Cloudflare, DE-FIRSTCOLO	100m-50m	0xcd4E2D22317d8Fc072050 d430E8fe6b1a63b3BBD (ETH)
coinguru.pw	https://coinguru.pw/?rid=7	Romania	Cloudflare	100m-50m	0xB0566237F2D4270186a3 0c727d17104a97E80D49
eggchange.org	https://eggchange.org	russia	Cloudflare	100m-50m	
f-change.biz	https://f-change.biz	russia	Cloudflare, SYTRA, YNDX	100m-50m	0x5FD2CCc9e2a02666d76f Fd6e43779c5cEcc6087b
quickex.io	https://quickex.io	russia	Cloudflare, PROTON	100m-50m	
tiptopobmen.com	https://tiptopobmen.com	Estonia	NAMECHEAP-NET, AMAZON-02	100m-50m	
unicash.pro	https://unicash.pro	Netherlands	AS-REG, OVH, ZOHO-AS, COMPUTERLINE	100m-50m	0x75ECeeC10a62373CFe5E 08B22609393bed1dE878 (ETH)

xchange.cash	https://xchange.cash	Estonia	LEASEWEB-NL-AMS-01, INCAPSULA, CLOUDFLARENE SELECTEL-MSK	100m-50m	0x85512bC76f857B00B2d7b7758DF083B 1F10dDED6 (ETH)
60cek.org	https://60cek.org	Estonia	HURRICANE, LEASEWEB-NL-AMS-01, INCAPSULA	1bil-300m	0xbb4c181398705f9580a27De7afa8a 788e3B448De (ETH)
baksman.org	https://baksman.org	Ebstonia	INCAPSULA, CLOUDFLARENET WORLDSTREAM SELECTEL-MSK	1bil-300m	3K9sS5WNnaV5EjLJ5BXvmrQQQLAEoySz5P
bitok.me	https://bitok.me	belarus	CLOUDFLARENET, AS-REG	1bil-300m	
changeproject.bz	https://changeproject.bz	russia	CLOUDFLARENE, SAFEVALUES-AS, XIM-HK Room704	1bil-300m	
grambit.biz	https://grambit.biz	russia	CLOUDFLARENE, SAFEVALUES-AS, XIM-HK Room704	1bil-300m	
imexchanger.pro	https://imexchanger.pro	russia	Cloudflare, GOOGLE	1bil-300m	1Jcx4DjGwPzmyGuzDy5b14N9CrBm9qRUrs (BTC)
mchange.net	https://mchange.net	Estonia	HURRICANE, INCAPSULA, WORLDSTREAM	1bil-300m	0x5522D5881EB4B0aB6Ef7E392555cd9423c133347

newline.online	https://newline.online	Netherlands	Cloudflare, EUROHOSTER	1bil-300m	3QfwFLgtys6pRm2SpJG85 MAcvPgmHFYjeD
openchange.cash	https://openchange.cash	russia	Cloudflare, GOOGLE	1bil-300m	0xC69012201b0BE5940579 da7Eb0B05129952F7470 (ETH)
prostocash.com	https://prostocash.com	Estonia	INCAPSULA, CLOUDFLARENE, SELECTEL-MSK, OVH	1bil-300m	3KvoSp9qus7aJyPnqn8Wqo sU1TfSzjhSXt; 0x3a02FBe42743D33303 fA154622BeB7Cc9BEc078d
royal.cash	https://royal.cash	Estonia	HURRICANE, INCAPSULA, WORLDSTREAM	1bil-300m	38fhnLXSrcMwUmdZ8yecP if48cgtcuHfpZ; 0xCE663bEbD573e5cd7cF4 DD3289 9763e5d45f0eD8
ychanger.net	https://ychanger.net	Estonia	HURRICANE, INCAPSULA, OVH	1bil-300m	31szKEKqKQLKrizFkvT8a bX3Ufvy1GNG5c; 0x3Fa77a3E48952F3E71A3 2a1AdA93288334ee0 C5C
7money.co	https://7money.co	Estonia	Cloudflare, HETZNER-AS, MAILRU-AS	320000	3Kaew6xP3dnUgp4k5jztSK yrrEsJEbJANx
24paybank.net	https://24paybank.net	Georgia	INCAPSULA, CLOUDFLARENE, WORLDSTREAM	47m	
abcobmen.com	https://abcobmen.com	Estonia	Cloudflare, HETZNER-AS	268m	37rJinPQ4fCsdYi6necsFjpF 1Lepq4eYbm

bonkypay.com	https://bonkypay.com	Czech Republic	Cloudflare, LOGOL-AS	58m	bonkypay.com
cashbank.pro	https://cashbank.pro	USA	PROTON, VIRTUALDC, ITEXPRESS-AS, **DDOS-GUARD**	25m	16mR8QniB9ANuo2RDg6QobZkuxifDFFnWc
changer.club	https://changer.club	Ukraine	Cloudflare, GOOGLE	doesn't work	
cleanbtc.ru	https://cleanbtc.ru	russia	WORLDSTREAM, GOOGLE,OVH, DE-FIRSTCOLO	1,4m	
delets.cash	https://delets.cash	Germany	Cloudflare, GOOGLE	10,4m	
e-obmen.cc	https://e-obmen.cc	russia	Cloudflare, AS-REG	-	16YkUvUJa6ubHWbZTP2aWHZA1KSuz713BP
exchanger1.com	https://exchanger1.com	Ukraine	Cloudflare, YNDX	-	
flashobmen.com	https://flashobmen.com	russia	Cloudflare, SYTRA, YNDX	339000	3AbN3bhZiX6QzJJRPwwSJPFz6EQ17ARt5R; 34c9sGpKfefWoDMwE7kTZwaCTmH d41A1s2
kupibit.me	https://kupibit.me	Georgia	Cloudflare, YNDX	1,5m	

magneticexchange.com	https://magneticexchange.com	Georgia	OVH, GOOGLE, CLOUDNSNET	97000	0x41D8f850F359FCF9a55598F17F07250cE55cb331
mine.exchange	https://mine.exchange	Great Britain	**DDOS-GUARD**, YNDX,GODADDY-DNS	9,6m	14f5DsXVCcrgX2kEzyuQDVyvLpai5ujY3q; 0xeEb339818b58D521C8a864fcc13E6aDD280d4564
multichange.net	https://multichange.net	Estonia	HURRICANE, LEASEWEB-NL-AMS-01, INCAPSULA	155m	0x7d37c6b7a85519EcD408bf11F5a9889eFd41F541 (ETH)
netex24.net	https://www.netex24.net	Ireland	SAFEVALUES-AS, AMAZON-02, GODADDY-DNS, ITSOFT-AS, MICROSOFT-CORP-MSN-AS-BLOCK	989000	1HknzCBfiWq4ggqMJPPoyZUFHVuv3HCmbe
platov.co	https://platov.co	russia	Cloudflare, GOOGLE	13,5m	1BaBuuxUpEA4AkX4CGU4ecMJtQizpkZrXK; 0x339D4afdDDa5f4e3337244844935916804A91305
ramon.money	https://ramon.money	Germany	Cloudflare, GOOGLE	18,6m	
superchange.net	https://superchange.net	Ukraine	Cloudflare, GOOGLE	-	
top-exchange.com	https://top-exchange.com	Ukraine	Cloudflare, SYTRA, YNDX	1,8m	qpjl37aep6p5uhdd8rrdcwe2q3m2tf4fr5pat8ft8n

transfer24.pro	https://transfer24.pro	Estonia	Cloudflare,OVH	20,3m	3NtRMKTTcrL6vygi74bkSXQwMNNHYDRJX1
wmsim.ru	https://www.wmsim.ru	Turkey	AS-REG, **DDOS-GUARD**	doesn’t work	
ww-pay.net	https://ww-pay.net	Great Britain	Cloudflare, HETZNER-AS	96000	3377fMhgXxrrMvyC38AxCHp2dGKazYJSZD; 0xC1864a7A72EE7b3F454FcD143fab 986f43FBf29c
1obmen.net	https://1obmen.net	Ukraine	SAFEVALUE-AS	15m	
24.zone	https://24.zone	moscow, russia	Cloudflare	56m	
24obmen.org	https://24obmen.org	russia	Cloudflare	211000	0xD1FAb8929dAd1f2eF0494f92BFb545E97b41b85B (ETH)
24coin.pro	https://24coin.pro	russia	Cloudflare	67m	24coin.pro
24litecoin.co.ua	https://24litecoin.co.ua	russia	Cloudflare	-	
24online.cc	https://24online.cc	Ukraine	Cloudflare	doesn’t work	19Dbm18wxYGsieLpZPGzWdDyx8uUXJkTHN

366.cash	https://366.cash	russia	Cloudflare	-	
4pay.in	https://4pay.in	Ukraine	Cloudflare	22000	
8pay.ru	https://8pay.ru	russia	TimeWeb-AS	1,3m	0xfEE3e1F60caF9D6C624c 1f1a1406F7fB01e4dfA8 (ETH)
matbea.com	https://matbea.com	russia	HETZNER-AS	3400	1A3ChP5TddNv31tcQHugk nx9MZXxxyc2xs (BTC)
монетка24.рф	https://монетка24.рф	russia	Cloudflare	122300	
obmenko.org	https://obmenko.org	russia	Cloudflare	5,3m	
sova.gg	https://sova.gg	russia	Cloudflare	744000	
a-exchange.com	https://a-exchange.com	russia	Cloudflare	203000	
aitoz.top	https://aitoz.top	Ukraine	OVH	-	
alfa-trades.com	https://alfa-trades.com	russia	Cloudflare	24m	1FeseUE7wr2VPyJzRgN6x wkxaSa8E c55Gh (BTC)

alltrust.me	https://alltrust.me	Georgia	Cloudflare	3,8m	1Q33Wzo9jtKYJdtAzv6dut EnscdL8a6c7c
allwm.cash	https://allwm.cash	russia	Cloudflare	17600	
arbuz.io	https://arbuz.io	russia	Cloudflare	5,4m	
avanchange.com	https://avanchange.com	Lithuania	**DDOS-GUARD**	41m	
base-exchange.com	https://base-exchange.com	russia	Cloudflare	93000	
best-wallet.net	https://best-wallet.net	russia	Cloudflare	-	
bestcoin.cc	https://bestcoin.cc/	Great Britain	GOOGLE-CLOUD-PLATFORM	3,1m	0x21E62ff791d19562BC852 5e29B6B459805aeFf79 (ETH)
bitcash.cc	https://bitcash.cc	France	WEBZILLA	500300	0xc61a5Df17B8E50ffA947D f5312DE eeE47DB10BF1(ETH)
bitonator.pw	https://bitonator.pw	russia	WIBO-AS	270000	
bittrend.pro	https://bittrend.pro	Ukraine	Cloudflare	35,2m	

btc-obmennik.com	https://btc-obmennik.com	russia	OVH	21m	3NK4jiHMK9QcrS6dGepyneBrz96aumWans
btc2cashin.me	https://btc2cashin.me	USA	**DDOS-GUARD CORP**	89,9	
btcbit.net	https://btcbit.net	Estonia	Cloudflare	9,3	37eYnoB7RyQKPxKcEati8A2kXt6oeYkMgQ (BTC)
btcchange24.org	https://www.btcchange24.org	Portugal	Cloudflare	1,1	
buybit.su	https://buybit.su	russia	Cloudflare	29500	
cashbox.exchange	https://cashbox.exchange	russia	ITLDC-NL		
chby.io	https://chby.io	russia	Cloudflare	51,5m	
coin-bank.co	https://coin-bank.co	russia	Cloudflare	25600	
coindrop.trade	https://coindrop.trade	russia	Cloudflare	-	
coinumm.com	https://coinumm.com	Estonia	HETZNER-AS	1,3m	

cosmochanger.cc	https://cosmochanger.cc	russia	Cloudflare	34,6m	
cripta.cc	https://cripta.cc	russia	cripta.cc	3,9m	rwcDAcoes7zq4kA9rybCV YhX87SUDz2MEL (XPR)
crydos.org	https://crydos.org	russia	OVH	-	
crypik.com	https://crypik.com	russia	DIGITALOCEAN-ASN	2,6m	
crypkon.org	https://crypkon.org	russia	LEASEWEB-NL-AMS-01	256000	
crypto-store.cc	https://crypto-store.cc	russia	Cloudflare	133000	0xBA6C12a05224ce0C8748 A1aD0ef BA6B054CB06B1(ETH)
cryptohome.me	https://cryptohome.me	Georgia	Cloudflare	1,6m	0xc2Dec9eD19Cbaca1bAFc F2993894f6aB8b6C3f B9 (ETH)
cryptohonest.ru	https://cryptohonest.ru	russia	Cloudflare	106m	(CashEx.cc)
cryptokarma.pro	https://cryptokarma.pro	russia	**DDOS-GUARD**	10,4m	
cryptonet.pro	https://cryptonet.pro	russia	Cloudflare	-	

cryptoxchange.ru	https://cryptoxchange.ru	russia		5,3m	iltbnuvenfmc(EOS)
e-money.cc	https://e-money.cc	USA	Cloudflare	2,7m	LN2mgpQnA4vtxBUcM1k3WVwAtvffUTHGa3 (LTC)
easy-changer.ru	https://easy-changer.ru	Ukraine	Cloudflare	76000	
eexchanger.co	https://eexchanger.co	Lithuania	Cloudflare	22m	
el-change.com	https://el-change.com	Turkey	Cloudflare	19,9m	
ex-code.ru	https://ex-code.ru	belarus	Cloudflare	5800	
exhub.io	https://exhub.io	russia	Cloudflare	5,1m	0x4A9F1B9Cf0b409D4e772bF3Fdbb4016B7C3E8436(ETH)
expochange.org	https://expochange.org	russia	Cloudflare	268000	0x65A077Be50e3a2fa7e329EbaC6657DE76D8e4fdb (ETH)
fast-swap.org	https://fast-swap.org	russia	ITLDC-NL	532000	
fastex.su	https://fastex.su	russia	Cloudflare	142000	1FggieZhtAYo7zJ3rz1S7VCKLU7CoxWkgq(ETH)

fastexchange.center	https://fastexchange.center	russia	Cloudflare	274000	0x762c6C7aeaBab105B196A71579C7f8a6214E4a6c(eth)
ferma.cc	https://ferma.cc	russia	SAFEVALUE-AS	48,8m	0xcCC80290346BDbDe342D82b6342f394BE14EB7Ae (ETH)
globalbits.org	https://globalbits.org	russia	Cloudflare	18,9m	
goldobmen.com	https://goldobmen.com	russia	HETZNER-AS	19000	0xd07f6CC29FbE74abC7F40d2E9836816a37881E3c (ETH)
haschange.com	https://haschange.com	russia	SELECTEL-MSK	3,6m	0xcd7DEb419eE7bFB3a02dfffeB6dE0 2a05a80584a (ETH)
internetmoney.exchange	https://internetmoney.exchange	Moldova	Cloudflare	31,6m	1Kdy2TMnZ xBCn2DH4xUU3xawiRe57Eaewv
izibtc.net	https://izibtc.net	France	Cloudflare	5,5m	
jpmarket.cc	https://jpmarket.cc	russia	Cloudflare	128m	0xf09ff5EB57A3c8880934201C91Ee FBD1aCE72033 (ETH)
kassa.cc	https://kassa.cc	Netherlands	SAFEVALUE-AS	313000	0x97FBA21fb4D048a1685Bdb3755a0dF9a68e7d3DB (ETH)
keine-exchange.com	https://keine-exchange.com	russia	TimeWeb-AS	7,3m	0x894Cc0d7A608164d35E643472F3f 664C20A314Db

konvert.im	https://konvert.im	russia	Cloudflare	58000	3FkbdMf1ziFCrf99G4pFFCykWZfD6WnhQV (BTC)
lucpey.com	https://lucpey.com	russia	Cloudflare	717900	
moneymix.org	https://moneymix.org	russia	SERVERS-COM	142000	
mybtc.link	https://mybtc.link	russia	Cloudflare	52,5	
mychange.su	https://mychange.su	russia	sprinthost	-	
n-obmen.net	https://n-obmen.net	russia	WIBO-AS	16800	0x74f712F9517C62677bD6AA5944fA668839052628 (ETH)
natebit.pro	https://natebit.pro	russia	AS-REGRU	-	
nordex.cc	https://nordex.cc	russia	Cloudflare	3,7m	
obama.ru	https://obama.ru	russia	Cloudflare	1,8m	
obmen.guru	https://obmen.guru	Ukraine	THEFIRST-AS	8100	

obmenex.com	https://obmenex.com	russia	Cloudflare	-	
obmenmonet.com	https://obmenmonet.com	russia	**DDOS-GUARD**	8,6m	0x2Fd60b7bf427cd03c7b89E65Cc76f515A0CD309b (ETH)
obmen.money	https://obmen.money	Vietnam	Cloudflare	259000	0x050863b0F44f919A71f81C1Fb14EEdDa358E9F1f (ETH)
obmenn.com	https://obmenn.com	russia	Cloudflare	35000	
obmennik-uz.ru	https://obmennik-uz.ru	Uzbekistan	Cloudflare	8200	
onemoment.cc	https://onemoment.cc	Estonia	Cloudflare	53,7m	
pandpay.net	https://pandpay.net	Georgia	Cloudflare	21,6m	
pay-today.cc	https://pay-today.cc	russia	Cloudflare	19,5m	0x6123401B47c70059bE75464e5F58F2a17509f875 (ETH)
pay2day.top	https://pay2day.top	russia	Cloudflare	-	
paywallet.cc	https://paywallet.cc	russia	Cloudflare	306800	0xC115E82Ac1D4f9D6d7D8c9eE1638 ec37584c463D(ETH)

perfect-change.com	https://perfect-change.com	Netherlands	Cloudflare	15600	3LGRuGgcBrFcNLjGVQEgs6ggCd2TvDJac2 (BTC)
pocket-exchange.com	https://pocket-exchange.com	russia	Cloudflare	53,9m	0x0B3149e2A49C9567c0835acce0F32B4AAb7d3CC4 (ETH)
pure-coin.org	https://pure-coin.org	Cyprus	OVH	493000	
pushpayer.net	https://pushpayer.net	russia	Cloudflare	80800	
rapid-obmen.com	https://rapid-obmen.com	russia	HETZNER-AS	4,4m	0x9abf8ac8842293554fC6e7Bc809236bB2FA700e9(ETH)
ru-change.cc	https://ru-change.cc	russia	Cloudflare	34600	35tNT9djuA3S7KJXiL9mnPEnUBchz5 mHAn (BTC)
sberbit.spb.ru	https://sberbit.spb.ru	russia	CONTABO	709800	142N396dKALXTf8J9gVFvznb83xFgLiVdE
smartmoney.exchange	https://smartmoney.exchange	russia	AS-REGRU	-	
sunduk.su	https://sunduk.su	Ukraine	Cloudflare	438700	0x44624a0d3D76EF8878c15b07196cEef0F771D25f (ETH)
treddr.org	https://treddr.org	russia	**DDOS-GUARD CORP**	665800	1NvSP3Lhq5gtjoMFyyyzdT2ULYyVLpWfEt (BTC)

unicash.pro	https://unicash.pro	Netherlands	OVH	56m	0x75ECeeC10a62373CFe5E08B22609393bed1dE878 (ETH)
ural-obmen.ru	https://ural-obmen.ru	russia	Cloudflare	264100	
wmz.one	https://wmz.one	Ukraine	Ukraine-AS	236400	
sunduk.su	https://sunduk.su	Ukraine	Cloudflare	438700	0x44624a0d3D76EF8878c15b07196cEef0F771D25f (ETH)
treddr.org	https://treddr.org	russia	**DDOS-GUARD CORP**	665800	1NvSP3Lhq5gtjoMFyyyzdT2ULYyVLpWfEt (BTC)
unicash.pro	https://unicash.pro	Netherlands	OVH	56m	0x75ECeeC10a62373CFe5E08B22609393bed1dE878 (ETH)
ural-obmen.ru	https://ural-obmen.ru	russia	Cloudflare	264100	
wmz.one	https://wmz.one	Ukraine	Ukraine-AS	236400	
worldchange.cc	https://worldchange.cc	russia	Appendix177	Cloudflare	107,8m

ДОДАТОК Д

Підходи до податкового регулювання віртуальних валют в різних країнах

характеристика	Японія	США *	Великобританія	Сінгапур	Німеччина	російська федерація
Визнання платіжним засобом	Так	немає	немає	немає	Так	-
Початок податкового регулювання	2014 р	2014 р	2014 р	2014 р	2013 р	немає
Прямі податки з юридичних осіб						
Майнінг віртуальних валют	Не обкладається, податок при реалізації	Податок на прибуток за базовою ставкою 21%	Податок на прибуток за базовою ставкою 19%. Порядок визначення оподатковуваного бази не уточнений	Податок на доходи за базовою ставкою 17%	Не обкладається	Податок на прибуток за базовою ставкою 20%
Доходи від купівлі / продажу віртуальної валюти як основна діяльність	Оподатковується за ставкою 34%				Чи оподатковується податком на приріст капіталу. При володінні більше року	
Придбання криптовалюти з інвестиційними цілями				Не обкладається. Відсутня податок на приріст		
Трактування для цілей прямого оподаткування	Валюта	майно	майно	актив	Валюта	майно
Прямі податки з фізичних осіб						
Майнінг віртуальних валют	Не обкладається, податок при реалізації	Чи оподатковується за базовою ставкою прибуткового податку (від 10	Чи оподатковується за базовою ставкою прибуткового податку (від 10 до 45%)	Не обкладається податком на доходи фізичних осіб	Не обкладається	Звільнено від оподаткування
Придбання віртуальних валют для особистого споживання (придбання товарів, робіт,	Оподатковується за прогресивною ставкою від 15 до 55%	Чи оподатковується: при володінні більше 1 року - податком на приріст капіталу за ставкою від 15 до 20%; при володінні менше 1 року - базова ставка прибуткового податку			Чи оподатковується податком на приріст капіталу. При володінні більше року ставка податку 0%	
Придбання віртуальних валют з інвестиційними цілями (приріст капіталу)			Оподатковується за ставками - від 10 до 20%	Не обкладається. Відсутня податок на приріст капіталу		
Трактування для цілей прямого оподаткування	майно	майно	майно	актив	Валюта	майно
непрямі податки						

Купівля-продаж віртуальних валют	Не обкладається	Н.д.	Не обкладається	Податок на товари і послуги 7%. Оплата	Не обкладається	Звільнено від оподаткування
Трактування для цілей непрямого оподаткування	Валюта		Валюта	послуга	Валюта	Валюта (або пільговані операції)

Примітка: * для США розглянуто тільки федеральне податкове законодавство.

Складено за: [PWC, 2018; EY, 2018]

- Income Tax Treatment of Virtual Currencies // Inland Revenue Authority of Singapore. URL: https://vmmciras.gov.sg/irashome/ Businesses / Companies / Working-out-Corporate-Income-Taxes / Specific-topics / Income-Tax-Treatment-of-Virtual-Currencies
- GST Treatment: Sale of Virtual Currency // Inland Revenue Authority of Singapore. URL: https://www.iras.gov.sg/IRASHome/GST/GST-registered-businesses/Specific-business-sectors/e-Commerce/#title5
- Revenue and Customs Brief 9 (2014 року): Bitcoin and Other Cryptocurrencies // HM Revenue & Customs. URL: https://www.gov.uk/government/publica- tions / revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies
- Cryptoassets for Individuals // HM Revenue & Customs. URL: https: // www.gov.uk/ government / publications / tax-on-cryptoassets / cryptoassets-for-individuals
- Notice 2014-21 // Internal Revenue Service. URL: https: // Vvmmcirs.gov/pub/irs-drop/n-14-21.pdf
- Taxation Relationship When Profit Arises by Using No. 1524 Bitcoin. Corporate Profit Tax. URL: https: // www. nta.go.jp/ni/taxanswer/1524.html
- Taxation Relationship When Profit Arises by Using No. 1524 Bitcoin. Income Tax. URL: https://vvmmcnta.go.jp/ taxes / shiraberu / taxanswer / shotoku / 1524.htm
- Umsatzsteuerliche Behandlung von Bitcoin und anderen sog. virtuellen Währungen; EuGH-Urteil vom 22. Oktober 2015 року, C-264/14, Hedqvist // Bundesministerium der Finanzen. 27.02.2018. URL: https://wvvmcbundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/ Steuerarten / Umsatzsteuer / Umsatzsteuer-Anwendungserlass / 2018-02-27-umsatzsteuerliche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.html
- Tax Rates (Germany) // KPMG.URL: https://home.kpmg/xx/en/home/insights/ 2011/12 /germany-income-tax.html

ДОДАТОК Е

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях

1) Дмитренко Т. Л. Упровадження міжнародних стандартів регулювання ринку віртуальних активів в Україні / Т. Л. Дмитренко, О. О. Любіч // Фінанси України. - 2020. - № 9. - С. 65-79. DOI: https://doi.org/10.33763/finukr2020.09.065 (0,71 друк. арк.). *Особистий внесок: обґрунтовано концептуальні засади управління якістю в умовах інформаційного суспільства (0,6 друк. арк.)*
2) Дмитренко Т. Л. Регулювання ринку віртуальних активів: глобальний та національний рівні імплементації міжнародних стандартів ПВК/ФТ / Т. Л. Дмитренко, О. О. Любіч, Ю. В. Пархоменко // Фінанси України. - 2021. - № 7. - С. 31-52. DOI: https://doi.org/10.33763/finukr2021.07.031 (1,06 друк. арк.). *Особистий внесок: проаналізовано міжнародне та європейське законодавство (0,9 друк. арк.)*
3) Дмитренко Т. Л. Особливості регулювання операцій із віртуальними активами щодо діяльності у сфері майнінгу / Т. Л. Дмитренко, В. М. Волкова // Наукові праці НДФІ. - 2021. - № 2. - С. 85-95. https://doi.org/10.33763/npndfi2021.02.085 (0,61 друк. арк.). *Особистий внесок: проаналізовано міжнародне та європейське законодавство щодо майнінгової діяльності (0,5 друк. арк.)*
4) Дмитренко Т.Л., Волкова В.М. «Децентралізовані фінанси: їх розвиток у сучасній фінансовій системі та ризики, які вони спричиняють.» // Наукові праці НДФІ. - 2022. - № 1. - С. 55-68. DOI: https://doi.org/10.33763/npndfi2022.01.055 (0,75 друк. арк.). *Особистий внесок: проаналізовано сучасні тенденції розвитку децентралізованих фінансів (0,6 друк. арк.)*
5) Дмитренко Т. Л. Регулювання ринку віртуальних активів як інструмент протидії уникненню міжнародних санкцій проти рф / Т. Л. Дмитренко // Фінанси України. - 2022. - № 4. - С. 107-128. DOI: https://doi.org/10.33763/finukr2022.04.107 (1,14 друк. арк.)
6) Єфименко Т.І., Дмитренко Т.Л. «Сучасні пріоритети у сфері протидії відмиванню коштів та фінансуванню тероризму» // «Наукові праці НДФІ » № 2 – 2022. DOI: https://doi.org/10.33763/npndfi2022.02.005 (0,80 друк. арк.). *Особистий внесок: проаналізовано критерії ризиків використання віртуальних активів в злочинній діяльності (0,7 друк. арк.)*
7) Дмитренко Т.Л. «Особливості імплементації Європейських Директив щодо обігу віртуальних активів в національне законодавство України» Т. Л. Дмитренко // Фінанси України. - 2022. - № 10. DOI: https://doi.org/10.33763/finukr2022.12.056 (0,92 друк. арк.)
8) Дмитренко Т. Л., Терещенко Г. М. «Підвищення рівня освіти у сфері кібербезпеки, фінансової та цифрової грамотності як чинник зниження ризиків

на ринку віртуальних активів» Науково-практичний журнал «Освітня аналітика України», №1(22) 2023. DOI: https://doi.org/10.32987/2617-8532-2023-1-38-50 (0,62 друк. арк.) *Особистий внесок: розкрито міжнародний та європейський досвід розробки і впровадження освітніх проєктів щодо протидії використання криптоактивів в злочинній діяльності (0,5 друк. арк.)*

9) Дмитренко Т.Л., Волкова В.М., Гавриленко С.В., Пархоменко Ю.В. «Огляд нових пропозицій щодо регулювання ринку криптоактивів в Європі та шляхи імплементації їх в Україні». Наукові праці НДФІ №2 (23) 2023. DOI: https://doi.org/10.33763/npndfi2023.01.030 (0,66 друк. арк.) *Особистий внесок: проаналізовано міжнародне та європейське законодавство щодо впровадження зарубіжної законодавчої бази в національне законодавство (0,5 друк. арк.)*

10) Hudima, T., Kamyshanskyi, V., Dmytrenko, T., & Shmyhov, M. (2023). Optimal CBDC design for Ukraine through the lens of privacy and security. Amazonia Investiga, 12(69), 73-83. URL: https://doi.org/10.34069/AI/2023.69.09.6 (0,80 друк. арк.). *Особистий внесок: досліджено можливі напрямки впровадження е-гривні в фінансово-економічні процеси (0,3 друк. арк.)*

11) Олійник, Я., Кучерява, М., Коритник, Л., Дмитренко, Т., Кузьмінська, О., & Лагунов, К. (2023). Формування інформаційного забезпечення управління фіскальними ризиками в умовах криз. Financial and Credit Activity Problems of Theory and Practice, 6(53), 432–450. URL: https://doi.org/10.55643/fcaptp.6.53.2023.4219 (1,48 друк. арк.). *Особистий внесок: викладено європейські стандарти щодо обміну інформацією про оподаткування операцій з віртуальними активами (0,5 друк. арк.)*

12) Дмитренко Т. Л. Географічні кореляції щодо контролю над капіталом, криптоактивами та корупцією / Т. Л. Дмитренко, Ю. В. Пархоменко, В. М. Волкова, С. В. Гавриленко // Фінанси України. - 2023. - № 12. - С. 114-128. DOI: https://doi.org/10.33763/finukr2023.12.114 (0,68 друк. арк.) *Особистий внесок: досліджено вплив діяльності ринку віртуальних активів на макропоказники глобальної економіки (0,5 друк. арк.)*

13) Iefymenko, T., Dmytrenko, T., (2024). Development and integration of digital currencies in the activity of the virtual asset market. Science and Innovation. DOI: https://doi.org/10.15407/scine21.02.003 (0,70 друк. арк.). *Особистий внесок: зроблено огляд міжнародних пілотних проєктів щодо розвитку CBDC країн, які їх розробляють; надані пропозиції щодо ефективного впровадження е-гривні (0,5 друк. арк.)*

14) Dmytrenko, T. Методологічні підходи до розробки моделей оцінки ризиків використання цифрових активів у легалізації та злочинних операціях. Фінанси України (12), (2024). 75-92. DOI: https://doi.org/10.33763/finukr2024.12.075 (0,94 друк. арк.)

15) Дмитренко Т. Л., Терещенко Г. М. «Підвищення інвестиційної грамотності на крипторинку» Науково-практичний журнал «Освітня аналітика України», № 5’2024. DOI: https://doi.org/10.32987/2617-8532-2024-5-55-65 (0,54 друк. арк.) *Особистий внесок: розкрито зв'язок між цифровою та фінансовою інклюзією з*

метою протидії шахрайству з використанням криптоактивів (0,4 друк. арк.)
16) Дмитренко Т.Л., Волкова В.М. Сучасні проблеми/прогалини у регуляторній політиці щодо майнінгу криптовалют в системі віртуальних активів, наслідки та шляхи подолання їх. Наукові праці НДФІ №3 (28) 2024. DOI: (0,88 друк. арк.) *Особистий внесок: надано пропозиції щодо впровадження економічної класифікації майнінгової діяльності (0,45 друк. арк.)*
17) Дмитренко, Т. Л. Визначення сутності віртуальних активів як чинник формування методологічних підходів до оподаткування їх обороту. Вісник Чернівецького торговельно-економічного інституту. 2024. Вип. IV (96). С. 125-150. DOI: http://doi.org/10.34025/2310-8185-2024-4.96.08 (1,13 друк. арк.)
18) Dmytrenko T., Hudima T. Risk assessment models for cryptocurrency use in fraud and criminal proceeds legalization. (1), (2025). 75-92. DOI: https://doi.org/10.33763/finukr2025.01.110 (1,13 друк. арк.) *Особистий внесок: застосовано математичну модель оцінки ризику використання криптоактивів в злочинних легалізаційних операціях (1 друк. арк.)*
19) Волкова, В., & Дмитренко, Т. (2022). Децентралізовані фінанси: їх розвиток у сучасній фінансовій системі та ризики, які вони спричиняють. Grail of Science, (12-13), 71–80. DOI: https://doi.org/10.36074/grail-of-science.29.04.2022.007 (0,33 друк. арк.) *Особистий внесок: проаналізовані загрози та вразливості операцій з токенами на децентралізованих платформах (0,2 друк. арк.)*
20) Дмитренко Т. Л. Особливості регулювання операцій із віртуальними активами щодо протидії легалізації доходів, отриманих злочинним шляхом / Т. Л. Дмитренко // Фінанси України. - 2020. - № 3. - С. 112-126. DOI: https://doi.org/10.33763/finukr2020.03.112 (0,72 друк. арк.)

Наукові праці, які засвідчують апробацію матеріалів дисертації

21) Актуальні проблеми безпеки застосування віртуальних активів в Україні / О.О. Любіч, Т.Л. Дмитренко. Матеріали І Міжнародної науково-практичної конференції (м. Херсон, 08–11 вересня 2021 р.).

22) Розвиток майнінгу віртуальних активів в національній економічній системі / Т.Л. Дмитренко, Волкова В. М. Матеріали І Міжнародної науково-практичної інтернет-конференції «Вплив пандемії COVID-19 на розвиток сучасного світу: загрози та можливості» (м. Дніпро, 9–10 вересня 2021 р.)

23) Ризики від майнінгу криптовалют в економічній системі України / Т .Л. Дмитренко, Волкова В. М. Матеріали ІІ Міжнародної науково-практичної конференції Multidisziplinäre forschung: perspektiven, probleme und muster (м. Відень, 26 листопада 2021 р.)

24) Дмитренко Т. Л. Протидія глобальним викликам, пов’язаним з використанням інноваційних технологій у злочинних цілях, шляхом підвищення стандартів кримінального аналізу. Матеріали Міжвідомчої науково-практична конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, серпень, 2022р.).

25) Дмитренко Т.Л. «Впровадження міжнародних стандартів FATF щодо легалізації ринку віртуальних активів як складова економічного зростання України». Матеріали Всеукраїнської науково-практичної інтернет-конференції «Актуальні питання бухгалтерського обліку, аналізу, аудиту та оподаткування в умовах воєнного стану і післявоєнного відновлення» (м. Київ, 15.06.2023р.)

26) Дмитренко Т. «Оцінка макрофінансових ризиків щодо діяльності з криптоактивами». Матеріали Міжнародної науково-практичної конференції «Фіскальна та монетарна безпека національної економіки в умовах глобальних викликів і загроз» (м. Київ, 31 жовтня 2023 р.)

27) Dmytrenko T. «Legalization of the virtual assets market is often considered a crucial element in enhancing Ukraine's financial security». Матеріали Науково-практичної конференції аспірантів та докторантів «Забезпечення резилієнтності економіки України в умовах військової агресії та повоєнного відновлення» (м. Київ, 12 грудня 2023р.)

28) Дмитренко Т.Л. «Інноваційні підходи до розвитку теорії грошей Михайла Туган-Барановського та сучасність». Матеріали академічних читань «Наукова спадщина Михайла Туган-Барановського для відбудови України», ДУ «Інститут економіки та прогнозування НАН України», (м. Київ, 18 січня 2024р.)

29) Дмитренко Т.Л., Волкова В.В. «Аналіз ризиків безпеки у використанні майнінгу криптовалют в операціях з відмиванням доходів, отриманих злочинним шляхом, та перспективи їх подолання». Матеріали Першого Міжнародного фінансового форуму «Модерні фінанси: глобальні виклики і сучасні тренди». (м. Тернопіль, 19-23 червня 2024р.)

30) Дмитренко Т.Л. «Пруденційний нагляд та оподаткування діяльності криптовалют в Україні» Матеріали ІІ Науково-практична конференція аспірантів та докторантів «Забезпечення резилієнтності економіки України в умовах військової агресії та повоєнного відновлення», ДННУ Академія фінансового управління (м. Київ, 17 липня 2024 року)

31) Дмитренко Т.Л., Волкова В.В. «Пруденційний нагляд та оподаткування діяльності майнінгу криптовалют в Україні». Матеріали Х Міжнародній науково-практичній конференції «Актуальні проблеми управління соціально-

економічними системами», Луцький національний технічний університет (м. Луцьк, 6 грудня 2024 р.)

32) Дмитренко Т.Л., Волкова В.В. «Європейська інтеграція майнінгу криптовалют та ринку віртуальних активів в Україні та національний аспект імплементації європейських стандартів щодо протидії відмиванню доходів, отриманих злочинним шляхом». Матеріали ІІ Міжнародної науково-практичної конференції «Економічна аналітика: сучасні реалії та прогностичні можливості», Київський національний економічний університет імені Вадима Гетьмана (м. Київ, 24 січня 2025р.)

33) Дмитренко Т.Л., Волкова В.В. «Теорія криз Туган-Барановського як підґрунтя розвитку цифрової економіки та регулювання на глобальному рівні». Матеріали Міжнародної науково-практичній конференції «Наукова спадщина Михайла Туган-Барановського як концептуальне підґрунтя суспільного розвитку» ДУ «Інститут економіки та прогнозування НАН України» (м. Київ, 29 січня 2025р.)

ДОДАТОК Є

Наукові результати дисертаційної роботи знайшли своє практичне застосування, що підтверджується відповідними довідками про впровадження:

НАЦІОНАЛЬНА КОМІСІЯ З ЦІННИХ ПАПЕРІВ ТА ФОНДОВОГО РИНКУ

вул. Князів Острозьких, 8, корпус 30, м. Київ, 01010, тел.: (044) 280-40-95, 254-23-31

E-mail: info@nssmc.gov.ua, сайт: www.nssmc.gov.ua, код згідно з ЄДРПОУ 37956207

від __ ____ 20__ р. № _______ На № ________ від ______ 20 р.

<u>ДОВІДКА</u>

про впровадження результатів дисертаційного дослідження
Дмитренко Тетяни Леонідівни
на тему:
«Ризик-орієнтований підхід до регулювання обороту цифрових активів в сфері ПВК/ФТ»
за спеціальністю 072 Фінанси, банківська справа та страхування

Науково-практичні висновки та рекомендації, викладені у дисертаційній роботі Дмитренко Т.Л., зокрема в частині визначення критеріїв та оцінці ризиків використання віртуальних активів в схемах відмивання коштів, отриманих злочинним шляхом, запровадження прозорого обігу віртуальних активів шляхом легалізації діяльності ринку віртуальних активів, запровадження ліцензування та пруденційного нагляду щодо професійних операторів ринку віртуальних активів, використані в аналітичній та законотворчій роботі Національної комісії з цінних паперів та фондового ринку України, а саме в обговорюванні пропозицій щодо зменшення ризиків та загроз відповідно до Звіту про проведення Національної оцінки ризиків, підготовленої з урахуванням міжнародних стандартів і відповідно до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та Стратегії розвитку фінансового сектору України до 2025 року, що мали відображення в зазначеному документі, а також визначення шляхів розбудови обігу цифрових активів в цілому.

Отримані в дисертаційній роботі результати мають важливе значення для впровадження ризик-орієнтованого підходу щодо підвищення фінансової безпеки в системі антикризового регулювання розвитку негрошового фінансування економіки та можуть бути в подальшому рекомендовані до використання у практичні діяльності всіх суб'єктів фінансового моніторингу, можуть бути в подальшому рекомендовані

ДОКУМЕНТ СЕД АСКОД
Сертифікат 6ГА978А9Е1825 [illegible]
Підписувач Лібанов Максим Олександрович
Дійсний з 07.06.2023 11:31:36 по 07.06.2025 11:31:36

Національна комісія з цінних паперів та фондового ринку
№ 04/6025 від 07.03.2024

до використання у практичні діяльності визначеного кола структурних підрозділів НКЦПФР.

Член Національної комісії
з цінних паперів та фондового ринку **М.О. Лібанов**

«___» _____ 20___ р.

АПАРАТ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50, телефакс: (044) 255-05-85

_____ № _____

Спеціалізованій вченій раді
Інституту післядипломної освіти
ДННУ «Академія фінансового управління»
Міністерства фінансів України

бульв. Дружби Народів, 38, м. Київ, 01014
afu@afu.kiev.ua

Про впровадження результатів дисертаційного дослідження

Висновки та пропозиції дисертаційної роботи Дмитренко Тетяни Леонідівни на тему «Ризик – орієнтований підхід до регулювання обороту цифрових активів» використані під час проведення тематичних зустрічей і обговорень щодо вдосконалення національного законодавства з питань застосування спеціальних економічних та інших обмежувальних заходів (санкцій) до постачальників послуг, пов'язаних з оборотом віртуальних активів, які співпрацюють із банками російської федерації та республіки білорусь.

Також були розглянуті й узяті до уваги матеріали розділу дисертаційної роботи «Санкційна політика як інструмент забезпечення фінансової та цифрової безпеки» щодо можливих шляхів обходу санкцій з використанням криптоактивів та неліцензованих (нездареєстрованих) обмінників криптовалют, пропозицій щодо підвищення впливу і ефективності впроваджених міжнародних санкцій, першочергових дій щодо легалізації діяльності крипторинку та впровадження ризик-орієнтованого підходу в питаннях взаємодії операторів крипто- та фінансового ринку в Україні на основі аналізу схем обходу міжнародних санкцій, застосованих до банків, компаній та фізичних осіб російської федерації.

У розділі дисертаційного дослідження щодо стимулювання сталого економічного зростання через розвиток діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів в Україні, доцільно відмітити обґрунтування щодо можливості наповнення державного бюджету ресурсами

Апарат РНБО України
№ 4524/14-15/2-24 від 26.12.2024

для повоєнного відновлення України та справедливої компенсації скоєних злочинів проти українського народу за рахунок заморожених та повернутих віртуальних активів суб'єктів рф та рб, які знаходяться під санкціями міжнародних організацій, іноземних держав та України.

Заступник Керівника Апарату
Ради національної безпеки
і оборони України **Максим ШОЙКО**

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Дмитренко Тетяни Леонідівни
на тему:
«Ризик-орієнтований підхід до регулювання обороту
цифрових активів в сфері ПВК/ФТ»
за спеціальністю 072 Фінанси, банківська справа та страхування

Науково-практичні висновки та рекомендації, викладені у дисертаційній роботі Дмитренко Т.Л., зокрема в частині визначення критеріїв та оцінці ризиків використання віртуальних активів в схемах корупційних злочинів, запровадження прозорого обігу віртуальних активів шляхом легалізації діяльності ринку віртуальних активів, запровадження процедур підтвердження справжності задекларованих віртуальних активів декларантами, проведення розслідувань корупційних злочинів з використанням програмних продуктів аналітичних компаній дослідження операцій в блокчейнах та збору доказів (артефактів) використання віртуальних активів в злочинній діяльності.

Також, в дисертаційних матеріалах надані пропозиції щодо зменшення ризиків та загроз відповідно до Звіту про проведення Національної оцінки ризиків, підготовленої з урахуванням міжнародних стандартів і відповідно до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», а також визначення шляхів розбудови транспарентного обігу цифрових активів в цілому.

Дисертаційні матеріали були апробовані шляхом використання їх в проведенні базового тренінгу Спільного проекту ОБСЕ та УПН ООН «Рішення запропоновані інноваційними підходами для зменшення ризиків відмивання грошей віртуальних активів» для представників влади та правоохоронних органів України, серед яких прийняли участь представники НАБУ та тренінгу CryptoEDGE для представників правоохоронних органів, в тому числі Національного антикорупційного бюро України.

Отримані в дисертаційній роботі результати мають важливе значення для впровадження ризик-орієнтованого підходу щодо підвищення фінансової безпеки в системі антикризового регулювання розвитку негрошового

фінансування економіки, розвитку Антикорупційної стратегії України на 2021-2025 роки та можуть бути в подальшому рекомендовані до використання у практичні діяльності правоохоронних та судових органів антикорупційної системи України.

Заступник Керівника
Головного підрозділу детективів –
Керівник Другого підрозділу детективів
Головного підрозділу детективів
Національного антикорупційного бюро України **О.В. Скомаров**

«12» 01 2024 р.



UNODC
United Nations Office on Drugs and Crime

22 February 2024

I hereby certify the following in regards of the **implementation of the results of the dissertation research on the topic: "Risk-oriented approach to turnover of digital assets in the AML/CFT field" in the specialty 072 Finance, banking, and insurance, author Tetiana Dmytrenko**

Scientific and practical conclusions and recommendations presented in the dissertation of T. Dmytrenko, in particular in terms of typology and risk assessment of the use of virtual assets in money laundering schemes, the introduction of transparent circulation of digital assets by legalizing the circulation of such assets, the introduction of prudential supervision over professional operators of the virtual assets market and circulation of digital currencies of central banks, were used in the development and conducting of training for representatives of the law enforcement system and state regulators as part of the UNODC Global Program on Cybercrime activities.

The arguments given regarding the improvement of the effectiveness of the National System for Combating the Legalization (Laundering) of Criminal Proceeds, the Financing of Terrorism, and the Financing of the Distribution of Weapons of Mass Destruction were used in conducting educational activities with the participation of the author within the framework of the project.

The results obtained in the dissertation are important for the implementation of International and European AML/CFT standards, increasing financial security in the system of anti-crisis regulation of the development of non-monetary financing of the economy, and are recommended for the development of a sequence of actions

United Nations Office on Drugs and Crime | Vienna International Centre | PO Box 500 | 1400 Vienna | Austria
Tel.: (+43-1) 26060-0 | Fax: (+43-1) 26060 5866 | Email: unodc@unodc.org | www.unodc.org

regarding the legalization and development of the virtual assets market in the countries of Europe and Central Asia.

Also, according to the provided recommendations, it is proposed to create permanent interagency advisory bodies to discuss and make joint effective decisions by the national security and law enforcement agencies on financial and national security issues regarding the misuse of virtual assets in criminal operations and evasion of sanctions.



Oleksiy Feshchenko

Advisor, UNODC Global
Program on Cybercrime

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЦИФРЛЫҚ ДАМУ, ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІ

Қазақстан Республикасы 010000, Астана қ.,
Мәңгілік Ел даңғылы 55/5 С 2.4
тел.: 8 (7172) 61-33-25, 61-33-23
электрондық мекенжайы: mooperemdai.gov.kz

MINISTRY OF DIGITAL DEVELOPMENT, INNOVATIONS AND AEROSPACE INDUSTRY OF THE REPUBLIC OF KAZAKHSTAN

Republic of Kazakhstan 010000, Astana city,
Mangilik El avenue 55/14 C 2.4
phone: 8 (7172) 61-33-25, 61-33-23
e-mail: mooperemdai.gov.kz

CERTIFICATE

on the implementation of the results of the dissertation research of

Tetyana Dmytrenko

on the topic:

"Risk-oriented approach to turnover regulation digital assets in the field of AML/CFT"

in the specialty 072 Finance, banking and insurance

Scientific and practical conclusions and recommendations presented in the dissertation work of Tetiana Dmytrenko, in particular in the part of the terminology and taxonomy of digital assets, international and European standards regarding AML/CFT in operations with digital assets and the activities of service providers related to the turnover of virtual assets and risk assessment of the use of virtual assets in money laundering schemes, the introduction of transparent circulation of digital assets by legalizing the circulation of such assets, the introduction of prudential supervision over professional operators of the virtual assets market and the circulation of digital currencies of central banks, used in the current activities of the Ministry of Digital Development, innovation and aerospace industry of the Republic of Kazakhstan, namely in the preparation and implementation in cooperation with the Department of Combating Organized Crime and Illicit Money Laundering of the United Nations Office on Drugs and Crime (UNODC) for representatives of the law enforcement system, state regulators, banks, of financial institutions and the crypto industry of the Republic of Kazakhstan of the international training "Risks associated with advanced blockchain technologies: DeFi, Smart contracts, NFT" in Astana, Republic of Kazakhstan.

Arguments are presented regarding the improvement of national legislation in accordance with the taxonomy of digital assets of European legislation in order to increase the transparency of cooperation between representatives of state supervisory bodies and representatives of the crypto business and banks of Central Asian countries with foreign ones, including European partners.

The results obtained in the dissertation work are important for the introduction of a risk-oriented approach to increasing financial security in the system of anti-crisis regulation of the development of non-monetary financing of the economy.

Also, according to the provided recommendations, it is proposed to create a platform for discussion and joint decision-making on financial and national security issues regarding the use of virtual assets in criminal operations and evasion of sanctions at the National Security Committee of the Republic of Kazakhstan.

Director of the Department for Development of the Electronic Industry and Digital Assets Industry of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan **Gizzat Baitursynov**

18 April 2024 p.

РАДА

НАРОДНИЙ ДЕПУТАТ УКРАЇНИ

вул. М.Грушевського, 5, м. Київ, 01008, www.rada.gov.ua

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Дмитренко Тетяна Леонідівна

на тему:

«Ризик-орієнтований підхід до регулювання обороту

цифрових активів в сфері ПВК/ФТ»

за спеціальністю 072 Фінанси, банківська справа та страхування

Науково-практичні висновки та рекомендації, викладені у дисертаційній роботі Дмитренко Т.Л., зокрема в частині розроблення підходів до впровадження оновлених Рекомендацій Міжнародної групи з протидії відмиванню брудних грошей (FATF), а саме ризик-орієнтованого підходу до обігу віртуальних активів і діяльності провайдерів послуг із віртуальними активами, взаємодії шляхом розробки та впровадження "Правила подорожей" (16 Рекомендація FATF) для фінансового сектору та ринку віртуальних активів щодо зменшення ризику використання їх у злочинних операціях (зокрема, ідентифікації й верифікації клієнтів, визначення інформації про відкриті ключі ініціаторів трансакцій із віртуальними активами та їх бенефіціарних власників), у законодавство України та практику Національної системи протидії відмиванню коштів, одержаних злочинним шляхом, та фінансуванню тероризму (ПВК/ФТ), спрямовані на підвищення ефективності процедур взаємодії представників правоохоронної та судової системи, державних наглядових органів і учасників ринку віртуальних активів шляхом цифровізації цих процесів.

Останні досягнення у сфері цифрових технологій надають фінансовим установам можливість більш ефективно аналізувати великі обсяги структурованих і неструктурованих даних, а також краще виявляти закономірності та тенденції. Збір даних та спільна аналітика допомагають фінансовим установам розуміти, оцінювати та знижувати ризики ВК/ФТ, що сприяє більш простому, динамічному та ефективному виявленню таких видів діяльності, а також зменшенню кількості хибних сигналів, що дозволяє приватному сектору своєчасно та з меншими труднощами дотримуватися вимог. Це також може перешкодити злочинцям використовувати інформаційні прогалини, оскільки вони взаємодіють із різними національними та

міжнародними фінансовими службами, кожна з яких має обмежену й часткову картину операцій.

Однак це може мати негативний вплив на захист особистих даних і основних прав. Тому важливо, щоб обмін інформацією здійснювався з урахуванням національних і міжнародних правових норм щодо захисту даних і конфіденційності.

Наведена аргументація щодо оптимізації процедур збору статистичних даних діяльності правоохоронної, судової, державної наглядової систем та операторів ринку віртуальних активів сприятиме загальному прогресу оцінки ефективності заходів у сфері ПВК/ФТ (33 Рекомендація FATF).

Результати проведеного дослідження дозволяють сформулювати рекомендації щодо розвитку ринку віртуальних активів в Україні, впровадження міжнародних стандартів FATF та ЄС у діяльність провайдерів послуг, пов'язаних з віртуальними активами, а також сприяти налагодженню співпраці між бізнесом, законодавчими й виконавчими органами, правоохоронними органами та громадянським суспільством на національному і глобальному рівнях.

Отримані в дисертаційній роботі результати мають важливе значення для впровадження ризик-орієнтованого підходу щодо підвищення фінансової безпеки в системі антикризового регулювання розвитку фінансування економіки та рекомендовані до проекту Плану заходів з післявоєнного відновлення та розвитку України.

Депутат Верховної Ради України,

Член Комітету Верховної Ради України

з питань цифрової трансформації **В.І. Ар'єв**

21 листопада 2024р.

ЄАС ВЕРХОВНОЇ РАДИ УКРАЇНИ
Підписувач: Ар'єв Володимир Ігорович
Сертифікат: 3FAA92883588C003040000001DC2900638E9000
Дійсний до: 23.01.2025 0:00:00

Апарат Верховної Ради України
2022д9/9-2024/259462 від 21.11.2024
1722956

ВИКОНАВЧИЙ КОМІТЕТ КРЕМЕНЧУЦЬКОЇ МІСЬКОЇ РАДИ
КРЕМЕНЧУЦЬКОГО РАЙОНУ ПОЛТАВСЬКОЇ ОБЛАСТІ
площа Перемоги, 2, м.Кременчук, 39600, тел.(0536) 74-37-75, 74-39-87
E-mail: kremenchuk@kremen.gov.ua, Web: www.kremen.gov.ua, Код ЄДРПОУ 04057287

09.07.2024 № 01-92/1 На № _____ від _____

До спеціалізованої вченої ради

ДОВІДКА

про впровадження результатів дисертаційного дослідження Дмитренко Тетяни Леонідівни

В роботі виконавчого комітету Кременчуцької міської ради Кременчуцького району Полтавської області використовуються наукові розробки, викладені та обґрунтовані в дисертаційній роботі Дмитренко Т.Л.

Авторкою проведено дослідження в частині антикорупційної політики щодо декларування цифрових активів в операціях з цифровими активами та оцінці ризиків використання віртуальних активів в схемах відмивання коштів, отриманих злочинним шляхом, запровадження прозорого обігу цифрових активів шляхом легалізації обігу таких активів та використання цифрових активів для підвищення прозорості формування місцевих бюджетів, особливо їх витратної складової, впровадження пруденційного нагляду обігу цифрових активів та методологічних підходів до оподаткування операцій з віртуальними активами.

Наведена аргументація щодо вдосконалення національного законодавства у відповідність до таксономії цифрових активів європейського законодавства для зростання прозорості співпраці представників державних наглядових органів та представників криптобізнесу регіонального рівня.

Отримані в дисертаційній роботі результати мають важливе значення для впровадження ризик-орієнтованого підходу щодо підвищення фінансової безпеки в системі антикризового регулювання розвитку негрошового фінансування економіки, розвитку антикорупційної діяльності місцевих рад.

Результати дослідження Дмитренко Т.Л. дають можливість створити при виконавчому комітеті Кременчуцької міської ради Кременчуцького району Полтавської області платформу для обговорення та прийняття спільних рішень з питань антикорупційної діяльності з використанням DLT-технологій, інновацій використання інструментів цифрової економіки, фінансової та цифрової безпеки щодо використання віртуальних активів в злочинних операціях.

Міський голова **Віталій МАЛЕЦЬКИЙ**

Державна установа
«ІНСТИТУТ ЕКОНОМІКО-ПРАВОВИХ ДОСЛІДЖЕНЬ ІМЕНІ В.К. МАМУТОВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ»

бульвар Тараса Шевченка, 60
Київ, 01032, Україна
Код ЄДРПОУ 13310946
e-mail: office.iepd@nas.gov.ua
www.iepd.kiev.ua
тел.: (044) 200-55-68

State Organization
«V. MAMUTOV INSTITUTE OF ECONOMIC AND LEGAL RESEARCH OF THE NATIONAL ACADEMY OF SCIENCES OF UKRAINE»

60 Taras Shevchenko Blvd.
Kyiv, 01032, Ukraine
Code 13310946
e-mail: office.iepd@nas.gov.ua
www.iepd.kiev.ua
tel.: (044) 200-55-68

№ 299/32/25 від 21.01.2025

Спеціалізованій вченій раді
Д 26.853.01
ДННУ «Академія фінансового управління»
бульв. Дружби Народів, 38,
м. Київ, 01014

ДОВІДКА

Цим підтверджується, що науково-аналітичні матеріали підготовлені Дмитренко Тетяною Леонідівною при підготовці дисертаційної роботи «Ризик-орієнтований підхід до регулювання обороту цифрових активів» містять низку наукових пропозицій по впровадженню ризик-орієнтованого підходу, спрямованого на підвищення фінансової безпеки в процесі антикризового регулювання та розвитку негрошових методів фінансування економіки.

Деякі з таких пропозицій було використано в роботі Інституту, зокрема: при викладанні наукових дисциплін для аспірантів в рамках дисципліни «Актуальні питання банківського права»; при проведенні спільних наукових досліджень з питань обігу цифрової валюти центрального банку, зокрема щодо вибору її оптимальної моделі для України, при формуванні спільних пропозицій для органів державної влади по застосуванню секторальних спеціальних економічних та інших обмежувальних заходів (санкцій) до постачальників послуг, пов'язаних з обігом віртуальних активів, які співпрацюють із банками Російської Федерації та Республіки Білорусь.

Директор Інституту
член-кореспондент НАН України,
член-кореспондент НАПрН України,
доктор юридичних наук, професор
Заслужений юрист України **Володимир УСТИМЕНКО**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ОСВІТНЬОЇ АНАЛІТИКИ»
STATE SCIENTIFIC INSTITUTION «INSTITUTE OF EDUCATIONAL ANALYTICS»
вул. Володимира Винниченка, 5, м. Київ, 04053, тел. (044) 486 98 70
info@iea.gov.ua, http://iea.gov.ua/, ЄДРПОУ 39817791

23.10.2024 № 05-12/429 На № _____ від _____

Спеціалізованій вченій раді
ДННУ «Академія фінансового управління»

Про впровадження результатів
дисертаційного дослідження

Висновки та пропозиції дисертаційної роботи Дмитренко Тетяни Леонідівни на тему «РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ДО РЕГУЛЮВАННЯ ОБОРОТУ ЦИФРОВИХ АКТИВІВ», використані при підготовці науково-дослідної роботи «Удосконалення механізму фінансування системи освіти як чинника розвитку людського капталу та його роль у повоєнному відновленні України» (номер державної реєстрації 0124U001973), в частині обґрунтування впливу рівня фінансово-цифрової грамотності на розвиток людського капталу, а також наявності взаємозв'язку рівня фінансово-цифрової грамотності та ризиків операцій на ринку цифрових активів. В розділі дисертаційного дослідження «Кластерно-порівняльний аналіз ризиків використання цифрових активів в злочинній діяльності» обґрунтовано, що низький рівень фінансово-цифрової грамотності зумовлює ризик інвестицій в шахрайські проєкти; панічний продаж/купівлю цифрових активів через нерозуміння ринкової волатильності ринку; ризик втрати персональних даних; ризик стати жертвами фальшивих криптовалютних платформ або ненадійних криптовалютних гаманців, що призводить до втрати коштів. Доведено, що підвищення рівня фінансово-цифрової грамотності дозволяє людям краще розуміти ризики операцій з цифровими активами та загалом є ключовими елементами у розвитку людського капіталу, оскільки вони сприяють економічній активності, підвищенню кваліфікації, розвитку підприємництва та інновацій, а також захищають людей від ризиків. Вони також допомагають зменшити нерівність і сприяють соціальній інклюзії, роблячи людей більш конкурентоспроможними в сучасному світі.

Директор **Андрій ЛИТВИНЧУК**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ЧЕРНІВЕЦЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ ІНСТИТУТ

Центральна площа,7, м. Чернівці, 58002, тел.: (0372) 51-11-58, факс: (0372) 52-21-12
E-mail: main@chtei-knteu.cv.ua, код СДРПОУ 05476322

19.12.2024 № 818/01-18
На _____ від _____

Довідка

Видана Дмитренко Тетяні Леонідівні, к.е.н., ст. дослідниці, завідувачу відділу міжнародних фінансів та фінансової безпеки відділення глобальної економіки і міжнародних фінансів НДФІ ДННУ «Академія фінансового управління», Голові правління громадської організації «Українська сучасна цифрова наука», про те, що результати її дисертаційного дослідження на тему «Ризик-орієнтований підхід до регулювання обороту цифрових активів в сфері ПВК/ФТ» застосовуються в освітньому процесі при викладанні дисциплін «Фінансовий ринок», «Аналіз фінансових ринків», «Фінансовий моніторинг», «Державна фінансова стратегія» та «Державний фінансовий контроль». Це стосується студентів, які здобувають освітній ступінь «бакалавр» за напрямом підготовки освітньої програми «Фінанси, банківська справа, страхування та фондовий ринок» та студентів, які здобувають освітній ступінь «магістр» за напрямом підготовки освітньої програми «Фінансовий моніторинг та податковий менеджмент» спеціалізації 072 «Фінанси, банківська справа, страхування та фондовий ринок».

Довідка підготовлена для подання до спеціалізованої вченої ради Науково-дослідного фінансового інституту ДННУ «Академія фінансового управління».

Директор Чернівецького торговельно-економічного інституту ДТЕУ **А.А. Вдовічен**

З метою ознайомлення студентів із сучасними тенденціями у сфері цифрових фінансів, 1 грудня 2023 року на третій парі з 11:40 спеціаліст-практик, міжнародний експерт в сфері ПВК/ФТ УНП ООН, завідувач відділу міжнародних фінансів та фінансової безпеки відділення глобальної економіки і міжнародних фінансів НДФІ ДННУ «Академія фінансового управління», Голова правління громадської організації «Українська сучасна цифрова наука», к.е.н., ст. дослідник Тетяна Леонідівна Дмитренко провела відкриту лекцію для студентів 3-4 курсів спеціальності 072 «Фінанси, банківська справа, страхування та фондовий ринок» на тему: «Ризик-орієнтований підхід до операцій з віртуальними активами».

На лекції були присутні представники Консультаційної місії ЄС, національних правоохоронних органів, експерти ГО «Українська сучасна цифрова наука», а також викладачі Кафедра фінансів, обліку і оподаткування Чернівецький торговельно-економічний інститут ДТЕУ.

Тематика відкритої лекції охоплювала такі питання:

- правові основи протидії відмивання коштів та фінансування тероризму (ПВК/ФТ) обігу віртуальних активів в Україні та світі;
- розвиток та еволюція вимог у сфері ПВК/ФТ та новітні європейські стандарти регулювання цифрової економіки;
- функціонування систем міжнародних організацій у сфері ПВК/ФТ та розподіл повноважень між органами фінансового контролю й нагляду України;
- антикорупційна та санкційна політика в сфері регулювання національного крипто ринку
- стимулювання сталого економічного зростання через розвиток діяльності постачальників послуг, пов'язаних з оборотом віртуальних активів в Україні.

Завідувачка кафедри фінансів,
обліку і оподаткування,
доктор економічних наук, професор **А.О. Чорновол**

UNOV UNODC

United Nations Office at Vienna — United Nations Office on Drugs and Crime

CERTIFICATE

awarded to

Tetiana Dmytrenko

in recognition of completing the International scientific and methodological internship "Development and conducting trainings on the creation of analytical systems for combating cybercrime"

22 ECTS credits (672 hours) at the United Nations Global Program on Cybercrime

Internship program

1. Kazakhstan – policy advice on cryptocurrencies: Online and face-to-face consultations and review of draft regulations are provided at the request of the MinDigital. Key recommendations are communicated to the UNODC, comments are addressed.
2. AIFC supervisory framework: Online and face-to-face consultations and review of draft regulations are provided on request of the AIFC. Key recommendations are communicated to the UNODC, comments are addressed.
3. NIS training: Materials cover the prevalent cybercrime threats for Kazakhstan schoolchildren (6 grade and older). Materials follow the basic pedagogic principles
4. Cybercrime prevention: Materials cover the prevalent cybercrime threats for Kazakhstan schoolchildren (6 grade and older). Materials are optimized for mass media and social networks.

In accordance with the work performed and the recommendations provided, it is proposed to create permanent interdepartmental advisory bodies to discuss and make joint effective decisions on financial and national security issues

regarding the use of virtual assets in criminal operations and the evasion of sanctions at the state bodies of national security with the participation of other national law enforcement agencies.

Oleksiy Feshchenko

Adviser of

UNODC Global Program on Cybercrime

February, 22, 2024