ЗАХОДИ БОРОТЬБИ З УХИЛЕННЯМ ВІД САНКЦІЙ НА РИНКУ ВІРТУАЛЬНИХ АКТИВІВ

MEASURES FOR COUNTERING SANCTIONS CIRCUMVENTION IN THE VIRTUAL ASSETS MARKET

У статті розглядаються методи уникнення блокування коштів підсанкційних осіб в системі віртуальних активів та інструменти протидії, які використовують суб'єкти первинного та державного фінансового моніторингу. Виокремлено поширені протиправні методи ухилення від блокування активів на етапі розміщення та нашарування. Встановлено, що на державному рівні ефективними діями, спрямованими на уникнення блокування активів, є постійна актуалізація реєстрів санкцій, ліцензування операторів ринку та співпраця між регуляторами та емітентами криптоактивів. Інтеграція з державними та міжнародними санкційними реєстрами, використання засобів блокчейн-аналітики та здійснення належної перевірки клієнтів є головними інструментами боротьби звітних установ з фінансового моніторингу зі спробами уникненням санкцій на ринку віртуальних активів. Досліджено сучасний стан реалізації санкційної політики в Україні та наголошено на можливостях її вдосконалення шляхом оновлення назв юридичних осіб та включенням цифрових адрес криптоактивів до Державного реєстру санкцій, прийняття нормативно-правового акту стосовно вимог до аналітики блокчейну.

Ключові слова: *санкції, віртуальні активи, фінансовий моніторинг, суб'єкт первинного фінансового моніторингу, аналітика блокчейну.*

УДК 330.1:342.5

DOI: https://doi.org/10.32782/dees.21-39

Акімова Л.М.[1]
д.держ.упр., к.е.н., професор,
Заслужений працівник освіти України,
Національний університет водного господарства та природокористування
Акімов О.О.[2]
д.держ.упр., професор, Заслужений економіст України,
Науково-методичний центр кадрової політики
Міністерства оборони України

Akimova Liudmyla
National University of Water and Environmental Engineering
Akimov Oleksandr
Scientific and Methodological Center for Personnel Policy
of the Ministry of Defense of Ukraine

The article examines methods for evading the freezing of funds belonging to sanctioned persons within the virtual asset system, alongside the counteraction tools employed by primary and state financial monitoring entities. Common illegal methods for evading asset blocking during the placement and layering stages are identified. At the placement stage, funds are transferred to the personal crypto wallets of sanctioned individuals or to the digital addresses of intermediaries located both within and outside sanctioned jurisdictions. The layering stage involves the application of methods similar to those used in money laundering, including cross-border transactions by shell companies. Furthermore, sanctioned crypto-asset exchanges have increased the frequency of changing their operational cryptocurrency addresses to prevent the timely identification of wallet ownership by sanctioned persons. A specific form of sanction evasion at the state level is the creation of sovereign stablecoins in countries subject to international sanctions. The use of stablecoins issued by companies from sanctioned jurisdictions allows businesses and individuals to minimize the risk of asset freezing and conduct export-import operations. It is established that at the state level, effective actions to address the evasion of asset blocking include the constant updating of sanction registries, the licensing of virtual asset market operators, and cooperation between state regulators and crypto-asset issuers to freeze the funds of sanctioned persons on virtual asset exchanges. Integration with state and international sanction registries, the use of blockchain analytics tools, and the implementation of customer due diligence are the primary tools used by reporting financial monitoring entities to combat sanction evasion in the virtual asset market. The current state of sanction policy implementation in Ukraine is explored, highlighting opportunities for its improvement by updating the names of legal entities, including crypto-asset digital addresses in the State Sanctions Registry, and adopting a regulatory act regarding requirements for blockchain analytics.

Key words: *sanctions, virtual assets, financial monitoring, primary financial monitoring entity, blockchain analytics.*

Постановка проблеми. З розвитком міжнародної екосистеми криптоактивів відбувається зростання спроб її використання в незаконних цілях, включно з намаганнями обійти накладені санкції. Перевагами операцій з віртуальними активами, в порівнянні з традиційною фінансовою системою, є швидке здійснення транскордонних платежів, анонімність та можливість використання децентралізованих операторів ринку з низькими стандартами в сфері протидії відмиванню коштів та фінансуванню тероризму. Відповіддю держав, які накладають санкції, стало внесення до санкційних списків осіб та елементів інфраструктури криптоактивів. Зокрема, сучасні санкційні переліки містять імена фізичних осіб, назв ліцензованих та неліцензованих бірж криптоактивів, компаній-змішувачів віртуальних активів, адреси криптогаманців. Постачальники послуг, пов'язаних з обігом віртуальних активів, які є суб'єктами первинного фінансового моніторингу, повинні постійно враховувати зміни як в самих санкційних списках, так і в типологічних дослідженнях, спрямованих на виявлення схем використання криптоактивів в цілях ухилення від санкцій. Невиконання вимог фінансового моніторингу створює для компаній значні репутаційні та фінансові ризики, які можуть призвести до відкликання ліцензії на право здійснювати діяльність.

Аналіз останніх досліджень і публікацій. Виявлено значний науковий інтерес до тематики екосистеми криптоактивів та застосування

[1] ORCID: https://orcid.org/0000-0002-2747-2775
[2] ORCID: https://orcid.org/0000-0002-9557-2276

санкційних вимог. Зокрема, в роботі K.E. Meyer [1], досліджується, як санкції порушують інституційну основу міжнародного бізнесу та яким чином суб'єкти ринку реагують на санкції. У праці N.P. Thi Hang [2] було розглянуто причинно-наслідковий зв'язок між запровадженням міжнародних санкцій та рівнем прийняття криптоактивів. A. Corobană [3] проаналізував вплив відсутності міжнародного регулювання криптоактивів на ефективність та результативність режимів фінансових санкцій. Використання біткоїну для ухилення від фінансових санкцій була предметом дослідження J. Zhao та J. Miao [4]. У дослідженні A. Hoang [5] розглянуто вплив геополітичних ризиків на зміну вартості криптоактивів. Таким чином, аналіз засобів, які сприяють виявленню фактів ухилення контрагентів суб'єктів первинного фінансового моніторингу від санкцій за допомогою криптоактивів, є недостатньо дослідженим.

Постановка завдання. Метою статті є дослідження типових схем ухилення від санкцій та сучасних інструментів, які можуть бути застосовані постачальниками послуг, пов'язаних з обігом віртуальних активів, для їх ідентифікації. Завданнями дослідження є аналіз методів ухилення від блокування санкційних коштів в екосистемі криптоактивів, ідентифікація ефективних інструментів виявлення та блокування коштів санкційних осіб в транзакціях криптоактивів, а також формування можливих напрямків удосконалення санкційної політики в Україні, з врахуванням міжнародного досвіду застосування санкцій в системі віртуальних активів.

Виклад основного матеріалу дослідження. Держави та суб'єкти, щодо яких накладені санкції, регулярно користуються системою криптоактивів для уникнення фінансових обмежень та стабільної експортно-імпортної діяльності. За даними компанії TRM Labs, яка є одним з лідерів міжнародного ринку блокчейн-аналітики, в 2023 році обсяг санкційних коштів в криптоактивах склав 21,9 млрд. доларів США при загальному незаконному обсязі транзакцій в віртуальних активах в 58,7 млрд. доларів США [6, с. 7]. Тобто 37% всіх ідентифікованих незаконних транзакцій в криптоактивах в 2023 році стосувалися ухилення від санкцій. За версією компанії Chainalysis, яка є іншим світовим лідером в сфері аналізу блокчейну, обсяг транзакцій юрисдикцій та суб'єктів, що перебували під санкціями в 2024 році, становив близько 39% від усіх незаконних операцій з віртуальними активами [7, с. 88].

Найбільш очевидною схемою використання коштів санкційних осіб у віртуальних активах є здійснення транзакцій з криптогаманцями, які належать санкційним особам. Даний підхід має місце, оскільки записи на блокчейні містять лише набір символів, які ідентифікують криптогаманець, без вказання ідентифікаційних даних його власника. Для блокування операцій з санкційними особами держави можуть вносити до переліків санкцій адреси криптогаманців. Зокрема, Управління з контролю за іноземними активами США (Office of Foreign Assets Control – OFAC) в 2024 році запровадило санкції проти 86 криптовалютних адрес, більшість з яких стосувалися осіб з Російської Федерації [6, с. 7]. До інструментів, які виявляють санкційних бенефіціарів криптогаманців, відносять здійснення заходів належної перевірки клієнта звітними установами у сфері фінансового моніторингу та використання регулярних скринінгових процедур, які порівнюють адреси криптогаманців з адресами, що присутні в санкційних переліках. Такі інструменти можуть використовуватися компаніями, які отримали ліцензію на здійснення операцій з криптоактивами та мають статус постачальників послуг, пов'язаних із криптоактивами. В Європейському Союзі ліцензійні оператори крипторинку мають статус CASPs (Crypto-Asset Service Providers) згідно з Регламентом Європейського Союзу 2023/1113 [8]. В юрисдикції США аналогічний статус компанії позначається терміном VASPs (Virtual Asset Service Providers) відповідно до Закону США про банківську таємницю [9]. Відповідно, етап розміщення криптоактивів санкційними особами з використанням власних криптогаманців є можливим лише на децентралізованих криптобіржах або через ліцензованих постачальників послуг, які, однак, не виконують вимоги стосовно адекватної перевірки власних клієнтів.

Для розірвання зв'язку між походженням та призначенням коштів санкційними особами використовуються програми-змішувачі, мости між блокчейнами, приватні монети. Тобто арсенал методів на етапі нашарування не відрізняється від методів, якими користуються злочинці при відмиванні коштів. Боротьбою з інструментами нашарування на державному рівні є накладення санкцій на елементи інфраструктури крипторинку. В 2022 році санкції OFAC були запроваджені проти «змішувачів» Blender.io та Tornado Cash. В 2023 році під санкції OFAC потрапила компанія-«змішувач» Sinbad.io [10, с. 2]. Протидія на рівні суб'єктів первинного фінансового моніторингу заснована на використанні методів блокчейн-аналітики, які дозволяють здійснювати перевірку криптогаманця відправника та отримувача криптоактиву до моменту проведення транзакції. Причому така перевірка включає не лише пряме порівняння адреси криптогаманця з міжнародними санкційними списками, а й відстеження транзакцій з проміжних криптогаманців на криптогаманець відправника.

Логічним розвитком ухилення від санкцій з використанням ринку криптоактивів стало створення торговельних майданчиків, які цілеспрямовано надавали послуги санкційним клієнтам.

Garantex, найбільша криптовалютна біржа Росії, та Nobitex, найбільша криптовалютна біржа Ірану, протягом 2024 року забезпечили понад 85% всіх надходжень коштів до санкційних організацій та юрисдикцій [6, с. 7]. Компанія Garantex була заснована в 2019 році в Естонії та спеціалізувалася на послугах обміну фіатних валют на криптоактиви, зокрема на стейблкоїни. Головними клієнтами компанії були особи з Російської Федерації. У лютому 2022 року Підрозділ фінансової розвідки Естонії провів розслідування щодо Garantex та виявив серйозні порушення правил боротьби з відмиванням грошей та фінансуванням тероризму, а також зв'язки зі злочинними фондами. Наслідком розслідування регулятора стало відкликання у Garantex ліцензії оператора віртуальних активів. Крім того, в квітні 2022 року Управління з контролю за іноземними активами США наклало санкції на Garantex, стверджуючи, що біржа криптоактивів сприяла відмиванню грошей та іншій злочинній діяльності [11].

Незважаючи на втрату ліцензії та санкції OFAC, компанія продовжувала обслуговувати клієнтів, використовуючи свої російські офіси. Для обходу санкцій біржа збільшила частоту зміни операційних криптовалютних адрес, які використовувалися для надходження та виведення криптоактивів. Така тактика ускладнювала здійснення аналітики блокчейну суб'єктами первинного фінансового моніторингу, яка заснована на кластеризації адрес. Замість проведення операцій через невелику кількість статичних криптогаманців, які звітні установи у сфері фінансового моніторингу могли б оперативно ідентифікувати та заблокувати, Garantex постійно генерувала нові адреси, які не використовувалися в минулих транзакціях. Як видно з рис. 1, частота зміни цифрових адрес зросла з одного разу на квартал в квітні 2022 року до одного разу на два дні в лютому 2023 року.

Іншою схемою ухилення від санкцій з використанням стейблкоїнів було створення компанії в юрисдикції США, реєстрація юридичної особи в банках та на регульованих біржах криптоактивів, отримання віртуальних активів від підсанкційних осіб на криптогаманець компанії, обмін криптоактивів на вільноконвертовану валюту з подальшою купівлею на неї товарів, яких потребували замовники з санкційних країн. Прикладом такої діяльності є справа компанії «Евіта», яку було засновано в США громадянином Росії Юрієм Гугніним. Фізичні та юридичні особи, які мали рахунки в підсанкційних російських банках, переказували стейблкоїн Tether (USDT) на криптогаманці «Евіти». Після конвертації в долари США, компанія купувала необхідну продукцію, створюючи фальшиві рахунки-фактури, щоб приховати кінцевих отримувачів товарів. Використовуючи дану схему, компанія «Росатом» придбала чутливе експортно-контрольоване обладнання у компанії зі США. У червні 2025 року Міністерство юстиції США оголосило про обвинувачення Юрію Гугніну в організації схеми ухилення від санкцій, яка спричинила виведення понад 500 мільйонів доларів США [12, с. 39].

Спільною відповіддю регуляторних органів та суб'єктів первинного фінансового моніторингу на використання стейблкоїнів в цілях ухилення від санкцій стало блокування криптоактивів їх емітентами. Протягом 2024 року емітент Tether заморозив 540 195 442 доларів у USDT, емітент Circle заблокував 13 359 597 доларів у USDC. В березні 2025 року емітент стейблкоїна Tether (USDT) заблокував активи на криптогаманцях, щодо яких була ідентифікована належність до криптобіржі Garantex [11]. Блокування призвело до тимчасової зупинки всіх операцій біржі, включаючи виведення коштів. Даний факт засвідчив ефективність контролю централізованих емітентів за обігом випущених криптоактивів.

На рівні ліцензованих CASPs та VASPs протидія використанню стейблкоїнів в цілях уникнення санкцій полягає у створенні системи «червоних

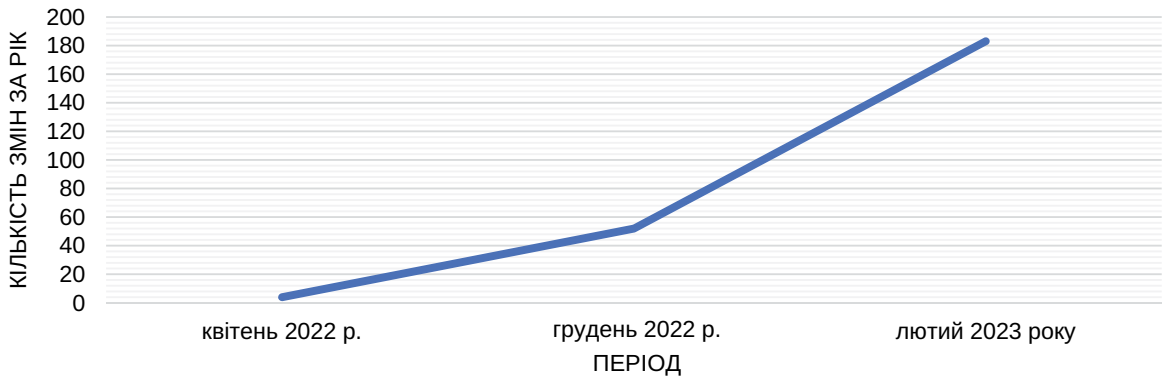

Рис. 1. Частота зміни операційних криптовалютних адрес біржі Garantex з квітня 2022 року по лютий 2023 року

Джерело: сформовано автором на основі [11]

прапорців», які ідентифікують підозрілу діяльність користувача. До таких ідентифікаторів належать: отримання великих обсягів стейблкоїнів без чіткого пояснення джерел походження коштів та мети транзакції; операції користувача в секторі бізнесу, якому притаманний високий ризик ухилення від санкцій; взаємодія з контрагентами, зареєстрованими в підсанкційних юрисдикціях; здійснення спроб приховати слід проведених транзакцій у блокчейні. Додатковим компонентом сучасних автоматизованих систем, які використовуються суб'єктами первинного фінансового моніторингу в сфері віртуальних активів, є аналіз профілів сервісів з обміну цифрових активів. В залежності від якості процедур належної перевірки клієнтів, які здійснюються іншими біржами криптоактивів, ліцензовані CASPs та VASPs можуть встановлювати диференційований рівень ризику для кожної транзакції.

Важливість потенційної здатності замороження коштів на криптогаманцях зростає, враховуючи динаміку росту популярності стейблкоїнів на міжнародному ринку віртуальних активів. Загальне зростання обсягів транзакцій з використанням даного виду криптоактивів у 2024 році склало близько 77% [7, с. 6]. Обсяг торгівлі стейблкоїнами зростав протягом останніх кількох років та станом на 2024 рік перевищив позначку в 27 трильйонів доларів США, що дозволяє даному виду віртуальних активів конкурувати з традиційними фінансовими інструментами [12, с. 34]. Наочне відображення частки стейблкоїнів в глобальних транзакціях віртуальних активів протягом 2023–2024 років наведено на рис. 2.

Незважаючи на переважне використання стейблкоїнів в законних цілях, їх зростаючий вплив на екосистему віртуальних активів спричинив поширення застосування стейблкоїнів в схемах відмивання коштів та фінансування тероризму. За даними Chainalysis, на частку стейблкоїнів в 2024 році припадало 63% всіх незаконних транзакцій в екосистемі криптоактивів [7, с. 6]. Стейблкоїни використовуються для цілей зберігання вартості, здійснення грошових переказів та розвитку міжнародної торгівлі. Унікальність даного виду криптоактиву полягає в поєднанні переваг блокчейну та стабільності фіатної валюти. Наявність повного резервування випущених в обіг стейблкоїнів офіційною вільноконвертованою валютою, кошиком валют або іншими активами створює стабільний обмінний курс, що разом з відсутніми бар'єрами при переказах за кордон робить даний криптоактив придатним для міжнародних експортно-імпортних розрахунків. Враховуючи переваги стейблкоїна, підсанкційні особи, які не в змозі скористатися класичними інструментами фінансової системи, часто використовують даний криптоактив для оплати товарів та послуг або для отримання виручки від реалізованої продукції, відвантаженої іноземним партнерам.

Зважаючи на ризик блокування емітентами стейблкоїнів на криптогаманцях підсанкційних осіб та виявлення підозрілих транзакцій ліцензованими учасниками ринку за допомогою аналітики блокчейну, подальше ухилення від санкцій набуло загальнодержавного рівня. Дослідження компанії Elliptic виявило переміщення користувачів Garantex на криптобіржу Grinex, зареєстровану в Киргизстані. Транзакції через Grinex здійснювалися з використанням стейблкоїна A7A5, прив'язаного до російського рубля [12, с. 41]. Згідно з дослідженням Центру інформаційної стійкості, емітентом A7A5 є російська компанія «A7», випуск здійснюється на блокчейнах Ethereum та TRON, а його резерви в рублях зберігаються в російському «Промсвязьбанку», на який накладені санкції США, Великої Британії, ЄС, Швейцарії, Канади, України, Австралії, Японії та Нової Зеландії.

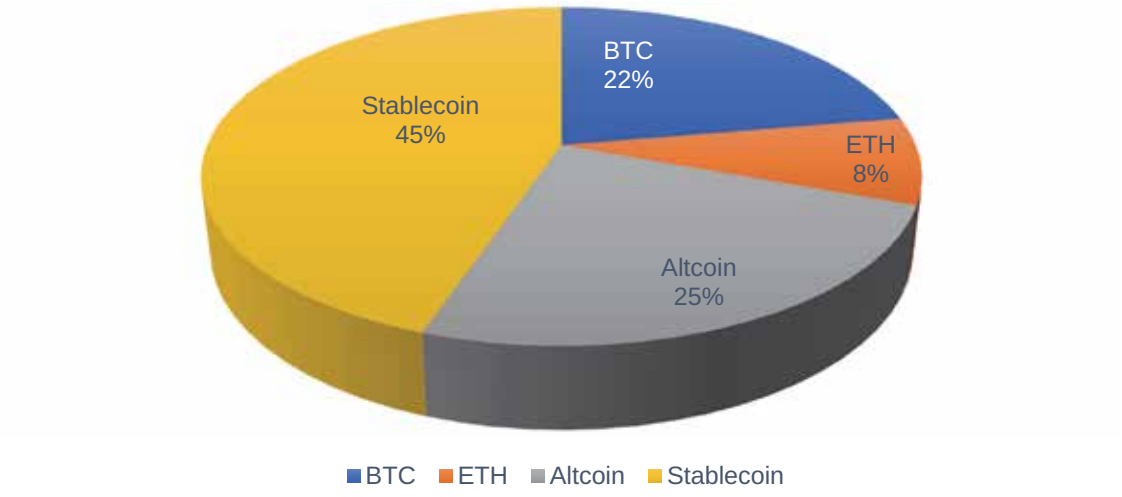

Рис. 2. Глобальні транзакції криптоактивів з липня 2023 року по червень 2024 року

Джерело: сформовано автором на основі [13]

В березні 2022 року «Промсвязьбанк» було виключено з міжнародної платіжної системи SWIFT. На початку 2025 року частка «Промсвязьбанку» в компанії «А7» була передана у заставу компанії «VEB. RF» для забезпечення кредитів, наданих компанії «А7». На «VEB.RF» накладені санкції з боку США, Великобританії, Європейського Союзу, Швейцарії, Канади, України, Австралії та Нової Зеландії. Діяльність «VEB.RF» спрямована на здійснення інвестицій, які просувають стратегічні російські державні інтереси [14, с. 6].

Використання власного стейблкоїну дозволяє країнам, які знаходяться під міжнародними санкціями, мінімізувати ризик замороження коштів та здійснювати зовнішньоекономічну діяльність, обмінюючи такий криптоактив на відомі міжнародні стейблкоїни безпосередньо перед здійсненням розрахунків з іноземними постачальниками. Крім того, такий підхід дозволяє підсанкційним особам не використовувати при розрахунках банківські установи третіх країн, нівелюючи ризик застосування до таких банків вторинних санкцій. Практика ухилення від санкцій за допомогою створення власного стейблкоїну країною, яка перебуває під санкціями, використовується вже декілька років. У грудні 2017 року Венесуела випустила криптоактив Petro, а наступного року ліцензувала 16 криптовалютних бірж для обслуговування його обігу. Деякі з ліцензованих бірж знаходились в державній власності та дозволяли користувачам здійснювати обмін інших криптоактивів, включно з Bitcoin, на Petro. У відповідь, в 2017 році США заборонили власним громадянам здійснювати операції з криптоактивами уряду Венесуели, а в 2019 році заблокували операції з будь-якою власністю Венесуели [10, с. 19].

Крім створення власних криптоактивів, санкційні режими створюють механізми ухилення від санкцій, засновані на відмиванні коштів на основі торгівлі. Головним елементом такого механізму є компанії-брокери, які активно пропонують юридичним та фізичним особам з санкційних юрисдикцій здійснення міжнародних платежів з використанням компаній-оболонок. Для імпортерів, які знаходяться в юрисдикції під міжнародними санкціями, компанія-брокер пропонує після укладення угоди з іноземним постачальником перерахувати платіж, вказаний в угоді, на рахунок брокера. На наступному етапі брокер здійснює трансфер коштів на рахунки контрольованих компаній-оболонок в іноземних юрисдикціях, які, в свою чергу, надсилають кошти іноземним постачальникам з власних розрахункових рахунків в іноземних банках. Враховуючи моніторинг транзакцій іноземними суб'єктами первинного фінансового моніторингу, брокер потребує наявності великої кількості компаній-оболонок, оскільки призначення платежу має відповідати профілю діяльності компанії. Для експорту з санкційних юрисдикцій схема здійснюється в зворотному порядку: іноземна компанія сплачує кошти компанії-оболонці, після чого кошти від такої компанії перераховуються на рахунки брокера, а в кінцевому рахунку – експортеру. Такий алгоритм ухилення від санкцій, відповідно до дослідження Центру інформаційної стійкості, використовувала російська компанія «А7» [14, с. 10].

Протидією відмиванню коштів на основі торгівлі є здійснення звітними установами в сфері фінансового моніторингу ефективних заходів належної перевірки клієнтів. Така перевірка має бути заснованою на використанні ризик-орієнтованого підходу та включати не лише аналіз відправника та отримувача коштів, але й використання критеріїв ризику та ідентифікаторів підозрілості, які можуть вказувати на здійснення фіктивної діяльності. Серед таких критеріїв, які допомагають встановити факт обслуговування компанії-оболонки, належать: невідповідність масштабу діяльності наявним в компанії активам, не характерна для специфічного ринку бізнес-діяльність компанії, відсутність у клієнтів необхідних дозволів та ліцензій [19-20]. На національному рівні протидія здійснюється за допомогою замороження коштів компаній-оболонок службами фінансової розвідки на основі аналізу повідомлень про підозрілі операції від суб'єктів первинного фінансового моніторингу.

Санкційна політика в Україні реалізується через актуалізацію Державного реєстру санкцій. Кількість та структура підсанкційних осіб, внесених в Державний реєстр санкцій станом на січень 2026 року, вказана на рис. 3.

Крім національних санкцій, Україною визнаються міжнародні санкції відповідно до визначень Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» № 361-IX (далі – Закон № 361-IX). Міжнародні санкції передбачають замороження активів, які пов'язані з фінансуванням тероризму або розповсюдженням зброї масового знищення, обмеження доступу до активів чи заборону проведення фінансових операцій [16].

Стаття 7 Закону № 361-IX зобов'язує суб'єктів первинного фінансового моніторингу встановлювати високий рівень ризику ділових відносин клієнтам, щодо яких були застосовані національні санкції. Ідентична вимога стосується кінцевих бенефіціарних власників клієнтів, які знаходяться під національними українськими санкціями. Високий рівень ризику також має бути встановлений клієнтам та представникам клієнтів, кінцеві бенефіціарні власники яких включені до переліку міжнародних терористів. Адміністратором переліку є Державна служба фінансового моніторингу України.

Встановлення високого рівня ризику передбачає застосування до клієнтів посилених заходів

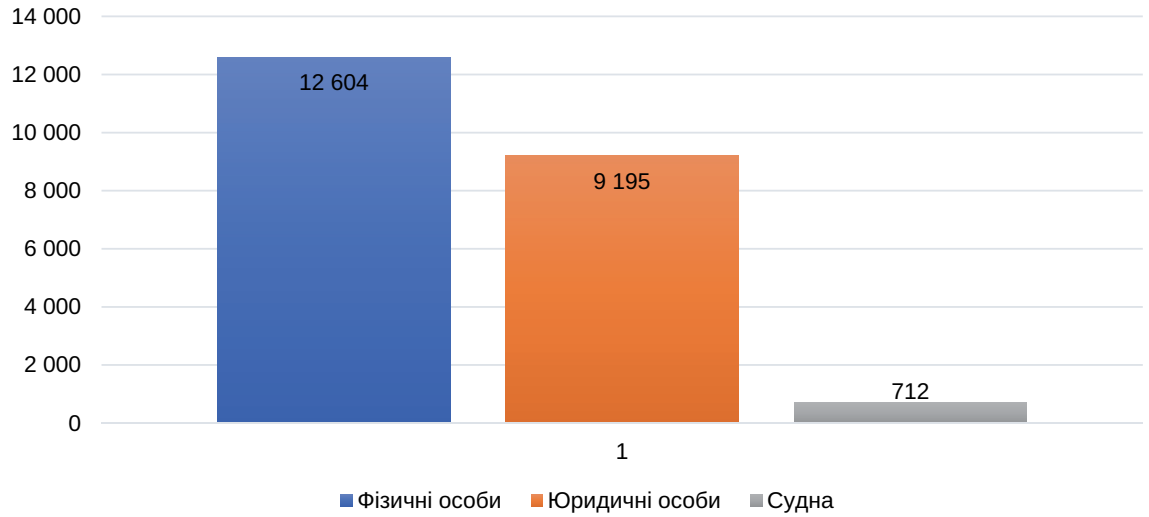

Рис. 3. Інформація про суб'єктів санкцій Державного реєстру санкцій станом на січень 2026 року

Джерело: сформовано автором на основі [15]

належної перевірки, які здійснюються до встановлення ділових відносин з клієнтом, при проведенні моніторингу фінансових операцій клієнта та при актуалізації інформації щодо клієнта. Звітна установа у сфері фінансового моніторингу самостійно обирає набір таких заходів, ціллю яких є отримання повної та достовірної інформації про діяльність клієнта. До поширених варіантів посиленої перевірки належать: встановлення кінцевих бенефіціарних власників, які здійснюють непрямий вплив на клієнта; отримання додаткових даних про клієнта з відкритих джерел; з'ясування причин використання юридичною особою складної структури власності; з'ясування джерел коштів та джерел статків; перевірка наявності ліцензій клієнта та їх чинності. Вимоги Закону № 361-IX розповсюджуються на постачальників послуг, пов'язаних з обігом віртуальних активів, оскільки дані установи, відповідно до закону, мають статус суб'єктів первинного фінансового моніторингу.

Водночас, існують напрямки вдосконалення санкційної політики в Україні, які б враховували міжнародний досвід боротьби з санкційним ухиленням, використовуючи екосистему криптоактивів. Зокрема, відсутність динамічного оновлення інформації в санкційному реєстрі України призводить до труднощів з ідентифікацією санкційної особи за її назвою. Наприклад, криптовалютна біржа Garantex присутня в Державному реєстрі санкцій, однак під назвою Kihonzi Buzhaga OU [15]. Альтернативні назви з реєстру також не містять назви Garantex, тому її виявлення є можливим лише через пошук реєстраційного номеру установи в реєстрі компаній Естонії.

Іншим напрямом підвищення ефективності санкційної політики України є впровадження обліку цифрових адрес криптоактивів в національному санкційному реєстрі. Наразі Державний реєстр санкцій містить інформацію лише про імена фізичних осіб, назви юридичних осіб та дані, які дозволяють суб'єктам первинного фінансового моніторингу ідентифікувати таких осіб серед своїх клієнтів. Водночас, в подібних реєстрах США та Європейського Союзу в картці об'єкта санкцій містяться набори даних під назвою «ідентифікатори», в яких вказані криптогаманці особи [17]. Такий підхід дозволяє постачальникам послуг, пов'язаних з обігом віртуальних активів, виявляти санкційних осіб або пов'язаність інших осіб з санкційними особами у випадку співпадіння цифрової адреси в транзакції з даними, які містяться в санкційному реєстрі. Подібна практика відрізняється від загальноприйнятого підходу, згідно з яким в реєстрах санкцій вказані лише особи та їх ідентифікаційні дані, а звітні установи в сфері фінансового моніторингу зобов'язані ідентифікувати та блокувати всі активи санкційних клієнтів. Причиною винятку для цифрових адрес є анонімна природа блокчейну, яка не дозволяє регульованим VASPs/CASPs отримувати дані про фактичне ім'я власника гаманця. В таких умовах цифрова адреса криптогаманця є головним ідентифікатором, що здатен виявити актив, до якого застосовані санкції.

Крім того, ефективність виявлення транзакцій, які пов'язані з санкційними особами, прямо залежить від якості аналітики блокчейну. Тому важливим чинником дотримання накладених санкцій є використання адекватних та сучасних методів блокчейн-аналітики, які б не були засновані на жорстких правилах обробки даних, а враховували ризик-орієнтований підхід [21–22]. Такі методи стосуються аналізу кількості проміжних гаманців перед транзакцією клієнта; часу, протягом якого такі переходи відбувалися; ідентифікації використання

приватних монет, мостів між блокчейнами та програм-змішувачів перед здійсненням транзакції; аналізу цифрової адреси отримувача криптоактивів. Для впевненості в якості перевірки необхідне прийняття нормативно-правового акту регулятора ринку цифрових активів, в якому були б зазначені мінімальні вимоги до блокчейн-аналітики звітних установ в сфері фінансового моніторингу та заходи впливу за порушення встановлених вимог.

Висновки. Типові методи ухилення підсанкційних осіб від блокування активів на ринку віртуальних активів не відрізняються від методів відмивання нелегальних коштів та включають використання програм-змішувачів, мостів між блокчейнами, приватних монет. В окремих країнах, що перебувають під санкціями, створені біржі криптоактивів, головною метою яких є надання послуг підсанкційним клієнтам. Для ускладнення ідентифікації санкційних активів суб'єктами первинного фінансового моніторингу такі біржі суттєво збільшували частоту зміни операційних криптовалютних адрес. Крім того, поширеною практикою є створення компаній-оболонок в розвинутих країнах світу, які здійснюють експортно-імпортні операції від власного імені та в інтересах санкційних осіб. Оскільки найбільш популярним джерелом міжнародних розрахунків в криптоактивах є стейблкоїни, підсанкційні країни створюють власні стейблкоїни.

На первинному рівні фінансового моніторингу ефективними інструментами виявлення коштів підсанкційних осіб в транзакціях криптоактивів є інтеграція з реєстрами санкцій, використання регулярних скринінгових процедур, блокчейн-аналітика та здійснення всіх елементів належної перевірки клієнтів. Методами суб'єктів державного фінансового моніторингу щодо блокування коштів осіб під санкціями є актуалізація реєстрів санкцій, надання постачальникам послуг, пов'язаних із криптоактивами, статусу суб'єктів первинного фінансового моніторингу, співпраця з емітентами стейблкоїнів щодо блокування активів на криптогаманцях.

Для підвищення ефективності санкційної політики в Україні пропонується розширити наповнення Державного реєстру санкцій. Зокрема, здійснювати динамічне оновлення назв юридичних підсанкційних осіб та запровадити облік цифрових адрес криптоактивів, які належать підсанкційним фізичним особам та компаніям. Засобом впевненості в стабільній якості процесу виявлення активів підсанкційних осіб постачальниками послуг криптоактивів є прийняття регуляторного нормативно-правового акту щодо мінімальних вимог до використання аналітики блокчейну.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Meyer K. E. et al. International business under sanctions. *Journal of World Business*. 2023. P. 101426. DOI: https://doi.org/10.1016/j.jwb.2023.101426

2. Thi Hang N. P. Sanctions and cryptocurrency: a catalyst for digital adoption? *Journal of Financial Regulation and Compliance*. 2025. № 33 (3). P. 406–424. DOI: https://doi.org/10.1108/JFRC-08-2024-0156

3. Corobană, A. Financial international sanctions and cryptocurrencies. Challenges and solutions. *European Business Law Journal*. 2022. №1(1). P. 71–80. DOI: https://doi.org/10.24818/eblj/2022/1/1.06

4. Zhao J., Miao J. Is Bitcoin used to evade financial sanction? *Finance Research Letters*. 2023. P. 104005. DOI: https://doi.org/10.1016/j.frl.2023.104005

5. Hoang A. T. P., To B. C. N., Tran H. D. Safe havens in the digital age: Cryptocurrencies and geopolitical risks. *Ho Chi Minh city open university journal of science – economics and business administration*. 2024. №15 (3). P. 160–180. DOI: https://doi.org/10.46223/hcmcoujs.econ.en.15.3.3875.2025

6. TRM Labs. 2025 Crypto Crime Report. URL: https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/68a391925a8dd785f5430482_TRM%20-%20Report%20-%202025%20Crypto%20Crime%20Report.pdf

7. Chainalysis. The 2025 Crypto Crime Report. URL: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf

8. Regulation (EU) 2023/1113 of the European Parliament and of the Council. URL: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

9. The Currency and Foreign Transactions Reporting Act of 1970. URL: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act

10. Elliptic Report 2024. Sanctions Compliance in Cryptocurrencies. URL: https://www.elliptic.co/resources/sanctions-compliance-in-cryptocurrencies

11. SlowMist Report. URL: https://slowmist.medium.com/repeatedly-sanctioned-what-has-the-russian-exchange-garantex-done-over-the-past-three-years-5c8e4bfb4851

12. Elliptic. The Typologies Report: Innovating to fight financial crime in an age of rapid change. URL: https://www.elliptic.co/blog/elliptics-typologies-report-innovating-to-fight-financial-crime-in-an-age-of-rapid-change

13. Chainalysis. Geography of Cryptocurrency report. URL: https://www.chainalysis.com/wp-content/uploads/2024/10/the-2024-geography-of-crypto-report-release.pdf

14. The Centre for Information Resilience (CIR): A7 Abroad: Sanctions evasion as a service. URL: https://www.info-res.org/cir-2/reports/a7-abroad-sanctions-evasion-as-a-service/

15. Державний реєстр санкцій. URL: https://drs.nsdc.gov.ua/export/subjects

16. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text

17. Elliptic. The Typologies Report: Innovating to fight financial crime in an age of rapid change. URL: https://www.elliptic.co/blog/elliptics-typologies-report-innovating-to-fight-financial-crime-in-an-age-of-rapid-change

18. Office of Foreign Assets Control (OFAC). URL: https://sanctionssearch.ofac.treas.gov/

19. Акімова Л. М. (2018). Механізм державного управління забезпеченням економічної безпеки в Україні: монографія. Київ : «Центр учбової літератури», 2018. 323 с.

20. Докієнко Л. М., Клименко В. В., Акімова Л. М. (2011). Інвестиційний менеджмент: навч. посіб. Київ: Академвидав. 2011. 405 р.

21. Клименко В. В., Акімова Л. М., Докієнко Л. М. Фінансовий ринок: навч. посіб. для студентів ВНЗ. Київ: Центр учбової літератури, 2015. 357 с.

22. Rumyk I., Laptev S., Seheda S., Akimova L., Akimov O., Karpa M. Financial support and forecasting of food production using economic description modeling methods. *Financial and Credit Activity: Problems of Theory and Practice*. 2011. Vol. 5(40). P. 248–262. DOI: https://doi.org/10.18371/fcaptp.v4i35.245098

REFERENCES:

1. Meyer K. E. et al. (2023). International business under sanctions. *Journal of World Business*, p. 101426. DOI: https://doi.org/10.1016/j.jwb.2023.101426

2. Thi Hang N. P. (2025). Sanctions and cryptocurrency: a catalyst for digital adoption? *Journal of Financial Regulation and Compliance*, no 33 (3), pp. 406–424. DOI: https://doi.org/10.1108/JFRC-08-2024-0156

3. Corobană, A. (2022). Financial international sanctions and cryptocurrencies. Challenges and solutions. *European Business Law Journal*, no 1(1), pp. 71-80. DOI: https://doi.org/10.24818/eblj/2022/1/1.06

4. Zhao J., Miao J. (2023). Is Bitcoin used to evade financial sanction? *Finance Research Letters*, p. 104005. DOI: https://doi.org/10.1016/j.frl.2023.104005

5. Hoang A. T. P., To B. C. N., Tran H. D. (2024). Safe havens in the digital age: Cryptocurrencies and geopolitical risks. *Ho Chi Minh city open university journal of science – economics and business administration*, no 15 (3), pp. 160–180. DOI: https://doi.org/10.46223/hcmcoujs.econ.en.15.3.3875.2025

6. TRM Labs. 2025 Crypto Crime Report. Available at: https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/68a391925a8dd785f5430482_TRM%20-%20Report%20-%202025%20Crypto%20Crime%20Report.pdf

7. Chainalysis. The 2025 Crypto Crime Report. Available at: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf

8. Regulation (EU) 2023/1113 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

9. The Currency and Foreign Transactions Reporting Act of 1970. Available at: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act

10. Elliptic Report 2024. Sanctions Compliance in Cryptocurrencies. Available at: https://www.elliptic.co/resources/sanctions-compliance-in-cryptocurrencies

11. SlowMist Report. Available at: https://slowmist.medium.com/repeatedly-sanctioned-what-has-the-russian-exchange-garantex-done-over-the-past-three-years-5c8e4bfb4851

12. Elliptic. The Typologies Report: Innovating to fight financial crime in an age of rapid change. Available at: https://www.elliptic.co/blog/elliptics-typologies-report-innovating-to-fight-financial-crime-in-an-age-of-rapid-change

13. Chainalysis. Geography of Cryptocurrency report. Available at: https://www.chainalysis.com/wp-content/uploads/2024/10/the-2024-geography-of-crypto-report-release.pdf

14. The Centre for Information Resilience (CIR): A7 Abroad: Sanctions evasion as a service. Available at: https://www.info-res.org/cir-2/reports/a7-abroad-sanctions-evasion-as-a-service/

15. Derzhavnyy reyestr sanktsiy [State Sanctions Register]. Available at: https://drs.nsdc.gov.ua/export/subjects

16. Zakon Ukrainy «Pro zapobihannia ta protydiiu lehalizatsii (vidmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, finansuvanniu teroryzmu ta finansuvanniu rozpovsiudzhennia zbroi masovoho znyshchennia» № 361-IKh [Law of Ukraine "On Prevention and Counteraction to the Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction" No. 361-IX]. Available at: https://zakon.rada.gov.ua/laws/show/361-20#Text

17. Elliptic. The Typologies Report: Innovating to fight financial crime in an age of rapid change. Available at: https://www.elliptic.co/blog/elliptics-typologies-report-innovating-to-fight-financial-crime-in-an-age-of-rapid-change

18. Office of Foreign Assets Control (OFAC). Available at: https://sanctionssearch.ofac.treas.gov/

19. Akimova L. M. (2020) Mekhanizm derzhavnoho upravlinnia zabezpechenniam ekonomichnoi bezpeky v Ukraini: monohrafiia [Mechanism of state management of ensuring economic security in Ukraine: monograph]. Kyiv: Tsentr uchbovoi literatury, 324 p. (in Ukrainian)

20. Dokiyenko L. M., Klymenko V. V., Akimova L.M. (2011). Investytsiynyy menedzhment: navch.posib [Investment management: tutorial]. Kyiv: Akademvydav. 405 p. (in Ukrainian)

21. Klymenko V. V., Akimova L. M., Dokiienko L. M. (2015) Finansovyi rynok: navch. posib. dlia studentiv VNZ [Financial market: a textbook for university students]. Kyiv: Tsentr uchbovoi literatury, 357 p. (in Ukrainian)

22. Rumyk I., Laptev S., Seheda S., Akimova L., Akimov O., Karpa, M. (2021). Financial support and forecasting of food production using economic description modeling methods. *Financial and Credit Activity: Problems of Theory and Practice*, vol. 5(40), p. 248–262. https://doi.org/10.18371/fcaptp.v4i35.245098 (in Ukrainian)

Дата надходження статті: 24.10.2025
Дата прийняття статті: 07.11.2025
Дата публікації статті: 24.11.2025