doi: https://doi.org/10.33763/finukr2020.03.112

УДК 336.7

Т. Л. Дмитренко
кандидат економічних наук, доцент кафедри фінансів, банківської і страхової справи Навчально-наукового Інституту менеджменту, економіки та фінансів Міжрегіональної академії управління персоналом, Київ, Україна, AML-консультант ОБСЄ, Відень, Австрія, tatianadmytrenko@gmail.com
ORCID ID: https://orcid.org/0000-0002-2632-2986

ОСОБЛИВОСТІ РЕГУЛЮВАННЯ ОПЕРАЦІЙ ІЗ ВІРТУАЛЬНИМИ АКТИВАМИ ЩОДО ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Анотація. Статтю присвячено особливостям запровадження оновлених рекомендацій FATF для забезпечення реалізації положень міжнародних стандартів щодо регулювання операцій із віртуальними активами та діяльності постачальників відповідних послуг. Проаналізовано Керівництво FATF щодо ризик-орієнтованого підходу до обігу віртуальних активів і діяльності провайдерів відповідних послуг, зміни, внесені до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення". Наголошено на необхідності усвідомлення урядами країн, державними наглядовими та правоохоронними органами, підприємствами, залученими до діяльності з віртуальними активами, серйозності ризиків відмивання коштів, що пов'язані з цією активністю, а також формування законодавчої бази щодо регулювання крипторинку і взаємодії на міжнародному рівні. Наведено приклади ризикових трансакцій, що будуть перешкоджати провайдерам послуг із віртуальними активами ідентифікувати клієнтів. Особливу увагу приділено заходам зі зменшення загрози використання таких активів у тіньовій економіці. Надано рекомендації щодо розвитку транспарентного крипторинку й цифрових технологій загалом.

Ключові слова: віртуальні активи, постачальники послуг із віртуальними активами, протидія відмиванню доходів, одержаних злочинним шляхом, ризик-орієнтований підхід, фіатні валюти, віртуальний гаманець.

Рис. 1. **Літ.** 21.

Tetiana Dmytrenko
Ph. D. (Economics), Educational Institute of Management, Economy and Finance of the Interregional Academy of Personnel Management, Kyiv, Ukraine, tatianadmytrenko@gmail.com
ORCID ID: https://orcid.org/0000-0002-2632-2986

FEATURES OF REGULATING VIRTUAL ASSETS OPERATIONS FOR AML/CFT PURPOSES

Abstract. The article deals with the peculiarities of implementing the updated Recommendations of the Anti-Money Laundering Group (FATF) to enforce the provisions of international standards for the regulation of virtual assets transactions and the activities of virtual asset service providers. The purpose of this article is to investigate the classification of virtual assets market instruments and its participants for the further development of this market activity at the legislative level. In addition to drafting a basic national law on the virtual assets market in Ukraine, it is urgently needed to develop regulatory regulations on the interaction of the virtual assets market with the financial market sectors, namely, primarily with the banking sector and the stock market of

Ukraine. It is the regulation of exchange transactions with virtual assets and fiat money that will create a system of monitoring these transactions for the legalization of funds obtained through crime, fraud, manipulation on organized trading platforms, in the settlement of transactions for illegal goods. A particular challenge to regulate this area is to conduct due diligence on the participants of the transaction in accordance with international standards of compliance. The author provides recommendations on the use of software to analyze and determine the risk of transactions in compliance with AML requirements policies and procedures, criteria for assessing the risk of cryptocurrency customers, banking institutions, professional participants of the stock market and other sectors of the economy, the peculiarities of interaction between the supervisory authorities of participants in these markets. At the same time, the author emphasizes the harmonization of the interaction of the supervisory authorities and the implementation of a risk-oriented approach in order to counteract excessive regulation for the development of the virtual assets market and innovations in its activities.

Keywords: virtual assets, virtual asset service providers, counteraction to money laundering, risk-oriented approach, fiat currencies, virtual wallet.

JEL classification: G14, G18, F65.

Т. Л. Дмитренко
кандидат экономических наук, доцент кафедры финансов, банковского и страхового дела Учебно-научного института менеджмента, экономики и финансов Межрегиональной академии управления персоналом, Киев, Украина, AML-консультант ОБСЕ, Вена, Австрия

ОСОБЕННОСТИ РЕГУЛИРОВАНИЯ ОПЕРАЦИЙ С ВИРТУАЛЬНЫМИ АКТИВАМИ ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ

Аннотация. Статья посвящена особенностям внедрения обновленных рекомендаций FATF для обеспечения реализации положений международных стандартов по регулированию операций с виртуальными активами и деятельности поставщиков соответствующих услуг. Проанализировано Руководство FATF относительно риск-ориентированного подхода к обращению виртуальных активов и деятельности провайдеров соответствующих услуг, изменения, внесенные в Закон Украины "О предотвращении и противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения". Подчеркнута необходимость осознания правительствами стран, государственными надзорными и правоохранительными органами, предприятиями, вовлеченными в деятельность с виртуальными активами, серьезности рисков отмывания денег, связанных с данной активностью, а также формирования законодательной базы по регулированию крипторынка и взаимодействия на международном уровне. Приведены примеры рисковых трансакций, которые будут препятствовать провайдерам услуг с виртуальными активами идентифицировать клиентов. Особое внимание уделено мерам по уменьшению угрозы использования таких активов в теневой экономике. Представлены рекомендации по развитию транспарентного крипторынка и цифровых технологий в целом.

Ключевые слова: виртуальные активы, поставщики услуг с виртуальными активами, противодействие отмыванию доходов, полученных преступным путем, риск-ориентированный подход, фиатные валюты, виртуальный кошелек.

Нові технології, продукти та пов'язані з ними послуги можуть стимулювати фінансові інновації й продуктивність і поліпшити доступ до фінансів, але водночас створюють нові можливості для відмивання доходів або фінансування незаконної діяльності. Відстежуючи розвиток технологій, транснаціональні організовані злочинні угруповання використовують інтернет для скоєння протиправних дій, передання або приховування доходів від незаконної діяльності. Завдяки своїй природі та глобальній доступності через комп'ютерні мережі ринок віртуальних активів має транснаціональний вимір.

Такі обставини потребують адекватного реагування з боку державного й приватного секторів, а саме розуміння ризиків і здійснення скоординованих заходів. При цьому слід враховувати положення щодо регулювання ринку віртуальних активів, вжиття заходів боротьби з відмиванням грошей, відповідно до останніх рекомендацій FATF [1], змін, внесених до Директиви ЄС про боротьбу з відмиванням грошей [2] та найкращої міжнародної практики, а також докласти зусиль для зміцнення потенціалу правоохоронних і наглядових органів, їх співпраці з приватним сектором і блокчейн-спільнотами.

Проблематика регулювання обігу нових інструментів привертає увагу вітчизняних і зарубіжних фахівців. Відсутність єдиного тлумачення таких ключових понять, як цифрові активи, віртуальні активи та валюти, криптовалюти, цифрові гроші, нерідко призводить до того, що вони вживаються як синоніми. Це ускладнює регулювання операцій із використанням віртуальних активів та взаємодію з правоохоронними органами й приватним сектором, а також дотримання вимог стосовно фінансового моніторингу.

Питанням віртуальних активів присвячено спеціальні дослідження фахівців центральних банків Євросоюзу, ФРС США та країн Східної Азії, Австралії, таких як П. Бхаргав, З. К. Голдман, Ф. Паесано, Н. ван Сабергаген, Ш. Скотт, Б. Слоан [3–7] та ін.

При цьому особлива увага приділяється ризикам, що виникають при використанні віртуальних активів як засобу платежу й об'єкта інвестування, та управлінню ними. Питання полягає в тому, як регулятори реагуватимуть на таку загрозу. Вітчизняні дослідники поки що приділяють недостатню увагу потенційному й реальному використанню віртуальних активів, у т. ч. віртуальних валют, із метою відмивання грошей і фінансування тероризму. В Україні такі валюти вивчають, зокрема, О. В. Дзюблюк, Г. Т. Карчева, В. І. Міщенко, С. В. Науменкова [8–11] та ін., на предмет розуміння їх сутності й довіри до них. Разом із тим протидія використанню віртуальних валют для відмивання грошей розглядається в загальних рисах.

Метою статті є дослідження розвитку інструментів ринку віртуальних активів та активності його учасників, а також застосування ризик-орієнтованого підходу відповідно до Першої рекомендації FATF щодо використання віртуальних активів при легалізації злочинних доходів.

З точки зору регулювання, ціла низка ризиків, пов'язаних із віртуальними валютами [12], перегукуються з новими викликами внаслідок поєднання існуючих фінансових інструментів із новими технологіями, а саме: неперевірені бізнес-моделі та потенціал для зловживань і шахрайства, нечітке розуміння того, яким чином криптовалюти торгуються через DLT (*distributed ledger technologies* – технологія розподіленої книги) [3], а головне – невизначеність регуляторного середовища, котре стрімко розвивається.

Водночас спостерігається багатоаспектність екосиситеми криптовалюти, а також велика кількість інструментів і платформ, що застосовуються на фінансовому ринку. Аутентифікація однорангових (P2P – Peer-to-peer) трансакцій була створена для того, щоб власники електроннних грошей могли обходити інституційних посередників, котрі виступають у ролі головних захисників у глобальному режимі протидії відмиванню коштів. Передбачувана анонімність контрагентів із криптовалютами може перешкодити процедурам ідентифікації клієнтів "знай свого клієнта" (*know your customer* – KYC), які є складовою різних політик протидії відмиванню коштів. Інтернет-екосистема, що забезпечує обіг цифрової валюти, несе нові загрози кіберзахищеності та інсайдерської інформації, тимчасом як ітеративний характер DLT-системи запобігає обігу, коли відбулася шахрайська або неправомірна трансакція. Нарешті, відсутність вбудованих географічних обмежень ускладнює вибір юрисдикції, котра потенційно зможе регулювати певну послугу чи трансакцію.

У такому середовищі фінансові установи й наглядові органи стикаються зі складними технічними проблемами. Після порівняної лояльності на початковому етапі наразі фінансові регулятори більш агресивно реагують на загрози, які виникають, і потенційні вигоди, пов'язані з цифровою валютою – ICO (*initial coin offering* – первинна пропозиція токенів) та DLT. Неоднозначний правовий статус багатьох підприємств, котрі займаються випуском та/або обігом віртуальних активів, посилює виклики для їхніх партнерів – фінансових установ, чия толерантність до регуляторного ризику може скоріше відображати культуру "дикого заходу" технологічних стартапів, ніж традиційних постачальників фінансових послуг.

Незважаючи на заклики до прийняття глобальних норм AML[1] для торгівлі криптовалютами [13], таких єдиних правил до минулого року не було. Протягом 2018–2019 рр. FATF розроблено міжнародні стандарти AML-політик і процедур щодо обігу віртуальних активів, термінологічний словник та визначено, що постачальники платіжних послуг із цифровими валютами повинні мати ті самі зобов'язання, що і їхні "некриптові" контрагенти [14]. Більшість юрисдикцій, котрі видали правила чи вказівки з цього питання, дійшли висновку, що на комерційний обмін криптовалют на фіатні валюти, в т. ч. через криптобіржі, повинні поширюватися зобов'язання AML (або, у випадку Китаю, встановлена заборона на обіг).

[1] Боротьба з відмиванням грошей (*anti-money laundering,* AML) – цілий комплекс заходів, законів і нормативно-правових актів, спрямованих на припинення прибутку від вчинюваних протиправних дій.

Водночас національні нормативно-правові акти містять різний рівень специфікації норм і правил:

– спеціальні ліцензійні вимоги до криптобірж;

– охопленість правилами щодо протидії відмиванню коштів адміністраторів і послуг віртуального гаманця;

– критерії, за якими ICO підпадає під дію законів про цінні папери чи рівнозначних нормативно-правових актів із регуляторними наслідками;

– різницю в трактуванні операційної діяльності з обігу криптовалют і фіатних грошей.

У багатьох випадках особливості руху віртуальних цінностей або взагалі не встановлені, або мають неоднозначне тлумачення. Зауважимо: хоча закони про санкції стосовно національної безпеки в цій статті не розглядаються, зрозуміло, що обсяг вимог до застосування санкцій, як правило, буде значним і більшим за стандартні вимоги щодо дотримання AML-політик і процедур.

Ринки віртуальних активів потенційно вразливі до шахрайських дій та можуть бути пов'язані з фінансовими злочинами. Велика частина цих ризиків матеріалізуються не в самій технології блокчейн, а в навколишній екосистемі емітентів, діяльності криптобірж і електронних гаманців, які підтримують доступ споживачів до DLT. Швидкість розвитку технологій та простота створення нових цифрових активів, імовірно, й надалі ускладнюватимуть роботу правоохоронних органів і фінансових установ, тому потрібно постійно оцінювати виклики з боку представників тіньового сектору. Далі наведено фактори підвищених ризиків у цьому контексті.

• Торгівля незаконними товарами. Цифрові валюти є ідеальним засобом оплати за нелегальні товари та послуги (постачання наркотиків, торгівля людьми й органами, дитяча порнографія та інші пропозиції "темного павутиння").

• Зломи й крадіжки особистих даних. Віртуальні гаманці та електронні сервіси обміну цифрових валют дають хакерам можливості для фінансового шахрайства і крадіжок. Якщо обліковий запис зламано через одну з цих служб, віртуальні активи можуть бути переказані на анонімні рахунки та замінені на фіатні чи інші активи, причому скасувати такі трансакції після їх виявлення практично неможливо.

• Маніпулювання ринком і шахрайство. Хоча блокчейн-технологія, в принципі, дає змогу переглядати й контролювати біржові операції всім учасникам, можливість виявляти та стримувати інсайдерські торги, маніпуляції активами, інші форми ринкових зловживань за участі незареєстрованих ICO й неліцензованих (незареєстрованих) торгових майданчиків із віртуальними активами істотно обмежена. Відсутність регуляторного нагляду за незареєстрованими пропозиціями та легкість створення нових рахунків для реалізації злочинних схем роблять ці ринки вразливими.

• Сприяння неліцензованому бізнесу. Різноманіття законодавчих і регуляторних вимог до послуг із віртуальними активами в різних юрисдикціях

створює додаткові проблеми при визначенні відповідності діяльності підприємств, що використовують такі активи, місцевим правилам. Надання фінансових послуг суб'єктам господарювання, чия діяльність суперечить цим правилам, може за певних обставин потягти за собою надходження, незаконні з точки зору національного законодавства з протидії відмиванню коштів.

Окрім активізації описаної протиправної діяльності, анонімність, ліквідність і глобальна природа криптовалют роблять їх привабливими для потенційних "відмивачів" грошей.

Наведена на рисунку трифазна модель відмивання кримінальних фондів, рекомендована для використання FATF, передбачає виокремлення в єдиному процесі легалізації таких стадій: розміщення (*placement*), розшарування (*layering*) та інтеграцію (*integration*). Зазначені стадії можуть реалізуватись одночасно або частково накладатися одна на одну. Це залежить від наявного механізму легалізації та вимог, що висуваються злочинною організацією.

На стадії розміщення можливість швидко відкривати анонімні рахунки в криптовалюті забезпечує злочинним групам низький ризик при переказі й консолідації незаконних грошових коштів. На стадії розшарування віртуальні активи є ідеальним засобом для транзиту нелегальних надходжень через кордон. Незареєстровані ICO також надають можливості для багаторівневого розшарування. Якщо "відмивачі" грошей контролюють також ICO, вони можуть використовувати шахрайське залучення капіталу для конвертації своїх незаконних криптовалютних надходжень у фіатну валюту.

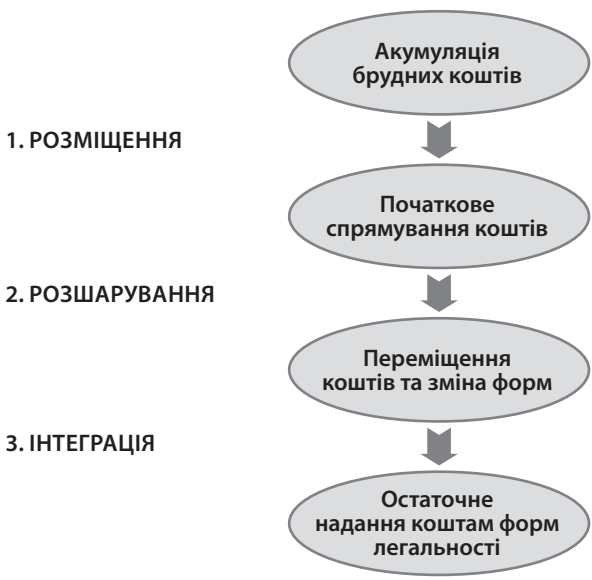

Рисунок. **Трифазна модель відмивання кримінальних фондів**

Джерело: Барановський О. І. "Відмивання" грошей: сутність та шляхи запобігання. Харків : Форт, 2003. 472 с.

Розширення переліку товарів із подальшим розрахунком криптовалютами збільшує можливості інтеграції. Готовність ICO приймати криптовалюти в процесі андеррайтингу віртуальних активів, подібних до корпоративних цінних паперів, також може призвести до незаконного підприємництва, за якого до продажу пропонуються великі пакети віртуальних активів (технічні віртуальні активи) з неповною інформацією про емітента або взагалі без неї. Така практика можлива через відсутність процедур регулювання розміщення віртуальних активів ICO.

Особливої уваги потребують трансакції з фінансування тероризму та ухилення від санкцій. Анонімність і легкість створення і в цьому випадку роблять цифрові валюти ідеальними для отримання платежів особами, котрі включені в міжнародні й національні списки терористів або до яких застосовуються санкції з червоними прапорцями. Використання цифрових валют наразі не набуло поширення для фінансування тероризму, проте терористичні групи експериментують із віртуальними активами з 2014 р. і вже послуговувалися біткойнами при проведенні кампаній зі збору коштів у соціальних мережах [4]. У країнах, що перебувають під дією санкцій, здійснюються спроби створення власних віртуальних валют, зокрема у Венесуелі [15].

Усі ці ризики посилюються серед нерегульованих секторів ринків віртуальних активів. Враховуючи регуляторний тиск, спрямований на подолання анонімності й запровадження нагляду за відмиванням коштів, отриманих злочинним шляхом, у сегментах, де ринки віртуальних активів взаємодіють із традиційним сектором фінансових послуг, спостерігаються ознаки того, що ринок віртуальних активів стає прозорішим і деякі нові віртуальні гроші є більш сумісними з чинними правилами на фінансових ринках. Водночас окремі з них віддають перевагу саме конфіденційності трансакцій та ідентифікації особи з метою полегшення позаринкових операцій [6].

Стосовно управління ризиком AML для користувачів віртуальних активів, а також їхніх контрагентів фінансові установи повинні звертатися до операторів ринку таких активів та їхніх клієнтів, повністю усвідомлюючи роль останніх у операціях із віртуальними активами й усі потенційні ризики. Як і у випадку з кожним новим напрямом діяльності, головним питанням дотримання AML для фінансових установ та викликом щодо прозорості власної діяльності буде їхня здатність розумно управляти цими ризиками. Фінансові установи, що прийняли рішення обслуговувати нові напрями діяльності або таких клієнтів, повинні оцінювати ризик та адаптувати власні AML-політики і процедури з урахуванням цієї співпраці, щоб забезпечити виконання зобов'язань щодо протидії відмиванню коштів.

Можливість підтвердити особу, юрисдикцію та оцінити ступінь ризику потенційних операцій має велике значення для виконання програм AML. Незважаючи на суперечливі виклики, котрі постають перед діяльністю ринку віртуальних активів щодо впровадження міжнародних вимог до обігу віртуальних активів, фінансові установи повинні забезпечити, щоб AML-політики та процедури провайдера послуг із віртуальними активами давали

змогу виконувати діяльність із такою само довірою, як традиційні послуги. Хоча необхідні заходи на практиці залежатимуть від конкретного замовника й послуги, при ідентифікації клієнта та контрагента необхідно виходити з певних загальних міркувань. Фінансові інститути не можуть мати відносини з клієнтами, котрі не підтвердили власну справжність як особи. Якщо припустити, що процедури KYC вже проведено стосовно інших фінансових послуг клієнту, у фінансових установ, імовірно, виникнуть питання на предмет доказів власності на віртуальні активи клієнта, електронного гаманця, де вони зберігаються, і джерел походження цих активів [5].

Наразі деякі національні, наприклад американські, норми протидії відмиванню коштів не зобов'язують фінансові установи виконувати процедури KYC щодо контрагентів за трансакціями (незалежно від того, чи проводились операції з криптоактивами раніше). Надання базової інформації про контрагента зазвичай необхідне для дотримання вимог AML-політик, а також для підтримки протидії шахрайству та послаблення моніторингу таких операцій. Оскільки процедури нагляду стосовно ідентифікації і скринінгу списків клієнтів базуються на ризик-орієнтованому підході, фінансовим установам доцільно використовувати такий підхід і до заходів щодо перевірки джерел походження віртуальних активів у клієнта, з огляду на основні ризики, створювані цими активами.

Зобов'язання послуговуватися розумним підходом щодо мети й характеру ділових відносин при моніторингу рахунків на предмет виявлення підозрілої діяльності [16] доцільно застосовувати до сторін угод із віртуальними активами, так само, як і до операцій із фіатними грошима. Знову ж таки, якщо фінансові установи особливо занепокоєні діяльністю на ринку віртуальних активів, їм, мабуть, доцільно розробити спеціальні червоні прапорці (критерії ризику), котрі використовуються на торгових майданчиках із віртуальними активами (AML-боти, аналітичні програмні продукти на кшталт Chainalysis Reactor, Crystal, CipherTrace), та навчити відповідальних працівників оцінювати такі операції.

Стосовно впровадження звітності про трансакції з віртуальними активами та обліку записів слід зазначити, що залежно від характеру трансакції національні режими боротьби з відмиванням коштів, отриманих злочинним шляхом, можуть вимагати від фінансових установ і провайдерів послуг із віртуальними активами надсилання файлів-повідомлень, у різний спосіб записувати або інформувати про трансакції, котрі перевищують певні порогові значення, що застосовуються для трансакцій із віртуальними активами. Як і щодо оновлень міжнародних AML-стандартів, упроваджені політики й процедури повинні давати фінансовим установам упевненість у тому, що дані, котрі вони отримують, є точними та достатніми для незалежної оцінки. Коректна ідентифікація власників рахунків, які проводять операції з віртуальними активами, допоможе фінансовим установам належним чином контролювати моніторинг трансакцій, включаючи вимоги до агрегації [17] та виявлення структурованих платежів [18]. Тією мірою, якою фінан-

сові установи мають намір покладатися на незалежність аналізу даних для цих функцій, такі системи й повинні бути встановлені та апробовані ними в офлайн-режимі до початку обробки реальних трансакцій.

При оцінюванні й управлінні ризиками клієнтів, що займаються віртуальними активами, особливі міркування щодо відшкодування збитків виникають у разі, коли клієнт фінансової установи є провайдером послуг із віртуальними активами. Послуги криптобіржі, обмінника або зберігача електронного гаманця (його ключів) повинні мати власні зобов'язання щодо проведення AML-політик і процедур залежно від юрисдикції, в котрій вони пропонують послуги. На андеррайтера віртуальних активів, такого як емітент ICO, також можуть покладатися зобов'язання щодо протидії відмиванню коштів, і до всіх зазначених вище видів бізнесу можуть бути застосовані вимоги інших режимів ліцензування та/або реєстрації фінансових послуг і послуг із віртуальними активами інших юрисдикцій. Деякі з цих питань ми розглянемо детальніше за типами взаємодії.

• Криптобізнес – фінансові установи. Спеціалісти фінансових установ можуть вимагати надання додаткової, розширеної інформації щодо операцій із віртуальними валютами, їхніх клієнтів, котрі самі є фінансовими установами. Управління та оцінка ризику в криптобізнесі, ймовірно, охоплюватиме низку питань, пов'язаних із відповідністю цього бізнесу чинним нормативним вимогам у таких аспектах:

1) збір інформації: чи дозволяють потенційний клієнт та його модель бізнесу збирати дані, достатні для виконання належної перевірки (ідентифікації й верифікації) в процесі оцінки ризику своїх клієнтів, та чи дозволяє він отримувати інформацію про контрагентів і місця здійснення операцій;

2) моніторинг та звітність: чи є в потенційного клієнта механізми моніторингу рахунків і процедури поточної звітності;

3) географічний контроль: чи здатна служба потенційного клієнта контролювати юрисдикції, в котрих є доступ до її послуг;

4) правовий статус та відповідність ліцензії й реєстрації: чи проводила служба потенційного клієнта ліцензування та/або реєстрацію своїх послуг у всіх юрисдикціях, у яких вони працюють, та чи здійснювала вона необхідні ліцензування й реєстрацію в юрисдикції США.

Наприклад, у США керівництво FinCEN[1] застосувало вимоги щодо обслуговування рахунків платіжних систем, відкритих до взаємодії з цифровими валютами, до рахунків торгових систем із віртуальними активами та зберігачів електронних гаманців, котрі є головними центрами моніторингу (шлюзами) обігу віртуальних активів [19], а саме вимоги до статусу діяльності платіжної системи, відповідності державним і місцевим ліцензійним вимогам, якщо це застосовується; спроможності проводити базову оцінку ра-

[1] FinCEN (*Financial Crimes Enforcement Network*) – Мережа по боротьбі з фінансовими злочинами, являє собою бюро Міністерства фінансів Сполучених Штатів, яке збирає та аналізує інформацію про фінансові операції з метою боротьби з внутрішнім і міжнародним відмиванням грошей, фінансуванням тероризму та іншими фінансовими злочинами.

хунків щодо AML-ризику та, за потреби, здійснити подальшу ретельну перевірку [20]. Хоча фінансова установа не несе самостійної відповідальності за ефективність програм AML своїх клієнтів, недоліки в будь-якій із них – це червоні прапорці, які слід враховувати при оцінюванні поточного рівня ризику клієнта [21]. Відповідно, FinCEN рекомендує, щоб належна ретельність платіжної системи була порівнянною зі ступенем ризику, виявленим шляхом його оцінки. Таким чином, якщо платіжні системи пов'язані з підвищеним ризиком щодо відмивання грошей або фінансування тероризму, здійснюється подальша, ретельніша перевірка, котра відповідатиме ступеню ризику [7].

В окремих випадках, з юридичних чи технічних причин, послуги підприємств, що проводять операції з віртуальними активами, не підпадають під чинні режими реєстрації. Подібні аргументи можуть надавати переваги в окремих випадках, але з огляду на вимоги щодо протидії відмиванню злочинних коштів, імовірно, доведеться вжити певні заходи для з'ясування достовірності цих аргументів (особливо у випадках, коли постає питання законності діяльності підприємства). Крім того, доцільно врахувати вказаний ризик, вирішуючи, чи надавати послуги таким клієнтам та яким чином це робити[1].

• Інші криптовалютні ризики. Навіть коли фінансові установи впевнені в тому, що віртуальні активи клієнта не підпадають під регуляторні вимоги щодо протидії відмиванню коштів, отриманих злочинним шляхом, вони повинні оновити інформацію про клієнта, щоб мати змогу враховувати конкретні ризики відмивання грошей через використання віртуальних активів, котрими володіє клієнт і які використовуються в його діяльності.

Питання географічного контролю заслуговує на особливу увагу в контексті обслуговування операцій із віртуальними активами. Крім ризику встановлення бізнес-відносин із підсанкційними особами і юрисдикціями, відсутність спільної політики регулювання ринку віртуальних активів, зокрема наявність різних вимог до реєстрації та заборона емісії й обігу віртуальних активів у Китаї, створює юридичні ризики, аналогічні іншим послугам із різними типами регулювання по юрисдикціях, діяльність яких провадиться на глобальних ринках (наприклад, азартні ігри в інтернеті). Неможливість контролю цих послуг зумовлює потребу в докладному розгляді діяльності таких підприємств щодо використання їх у незаконних операціях. При цьому необхідно звернути окрему увагу на трансакції у фіатній валюті та операції переведення віртуальних активів у фіатні валюти, матеріальні та/чи нематеріальні активи реального сектору.

Впровадження AML-політик і процедур має включати розумні заходи щодо виявлення нелегальної діяльності підприємств, запобігання їй або використанню таких підприємств у подібних операціях. Навіть коли немає ризику кримінального порушення, фінансові установи, що обслуговують

[1] Моделі FATF, засновані на AML, передбачають заборону на прийняття доходів, одержаних злочинним шляхом ("незаконних доходів"). *Див.,* наприклад, параграфи 1956 і 1957 Кодексу США.

операції з віртуальними активами, повинні вирішити, чи надавати послуги підприємствам, чий статус реєстрації викликає сумніви.

Приміром, для ICO, які не мають серед своїх контрагентів зобов'язаних суб'єктів щодо вимог протидії відмиванню коштів, фінансові установи повинні ретельно оцінити їхню структуру на існування відповідного ризику. При цьому слід особливо пильно проконтролювати ICO на наявність:

– продажу токенів одному покупцеві з метою отримання необмеженої суми грошових коштів від однієї особи;

– наміру ICO за якнайкоротший час перетворити частину залучених коштів на фіатну валюту.

Фінансові установи повинні вивчити умови випуску віртуальних активів, щоб визначити, чи здійснює емітент заходи моніторингу обігу для запобігання порушенню прав учасників останнього й вимог законодавства.

На підставі викладеного доходимо таких висновків. Сучасний світ вимагає прогресивних підходів до регулювання підприємницької діяльності та розвитку новітніх технологій. Ризик-орієнтований підхід набуває дедалі більшого визнання й поширення для створення сприятливих умов розвитку нових ринків і запобігання використанню нових інструментів зі злочинними намірами.

Саме з такого погляду міжнародними AML-стандартами рекомендований ризик-орієнтований підхід до регулювання ринку віртуальних активів. Треба наголосити, що при оцінюванні ризику використання віртуальних активів головною ознакою для інструментів є вартість, а для учасників ринку – ведення бізнесу з віртуальними активами, тобто в інтересах третіх осіб. Щодо діяльності з майнінгу варто зазначити, що вона не має ознаки вартості для операцій на крипторинку та ризиків щодо відмивання коштів, а шахрайства в ній пов'язані з незаконними діями на ринку електроенергії.

Для врегулювання й визначення ризиків криптобізнесу особливої уваги потребує взаємодія із секторами реальної економіки, так звані шлюзи обміну віртуальних активів на фінансові інструменти, цінні папери, нерухомість, майнові права тощо. Тобто важливо налагодити гармонійну співпрацю наглядового органу реального сектору економіки та ринку віртуальних активів, що рекомендовано міжнародними стандартами. Згідно з прийнятим у грудні 2019 р. національним AML-законодавством, в Україні наглядовим органом для ринку віртуальних активів призначено Міністерство з цифрової трансформації, головним завданням котрого наразі є розроблення базового законодавства з регулювання діяльності ринку віртуальних активів, реєстрація інструментів і учасників цього ринку та оцінка ризиків щодо їх обігу й діяльності.

Зважаючи не лише на різну природу віртуальних активів, а й на ймовірну її зміну в різні проміжки часу, а також беручи до уваги намагання наглядових органів інших секторів економіки виявити подібність віртуальних активів до усталених інструментів у цих секторах, доцільно створити для регулювання єдину національну інформаційну систему віртуального обігу

активів із різними ступенями відкритості для реєстрації інструментів цього ринку, його учасників – торгових майданчиків, зберігачів електронних гаманців і ключів, ICO й поточної інформації про них (реєстрації, зміни форми, ліквідації тощо). Варто покласти функції з регулювання подібних до використовуваних у реальному секторі цінностей віртуальних активів на наглядові органи на засадах солідарної відповідальності й погодження прийняття рішень з іншими регуляторами, наприклад наглядовою радою при основному державному наглядовому органі. Такий підхід сприятиме побудові прозорого ринку віртуальних активів та результативній координації функцій спостереження органів державної влади і приватного сектору.

Список використаних джерел

1. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: the FATF Recommendations / FATF-GAFI. URL: http://000.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html.

2. 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.

3. *Sloane B., Bhargav P.* Blockchain basics: Introduction to distributed ledgers. 2018. March 18. URL: https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-basics-intro-bluemix-trs/.

4. Terrorist Use of Virtual Currencies, Center for a New American Security / Z. K. Goldman, E. Maruyama, E. Rosenberg et al. 2017. May. URL: https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

5. *Paesano F.* Regulating cryptocurrencies: challenges & considerations. *Basel Institute on Governance (BIG) Working Paper.* 2018. No. 28. April. URL: https://www.baselgovernance.org/sites/default/files/2019-06/190425%20Working%20Paper%20Cryptocurrency%20Regulations_v2.pdf.

6. *Van Saberhagen N.* Crypto-Note v. 2.0. *Monero White Paper.* 2013. October 17. URL: https://www.github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf.

7. *Scott Sh.* Cryptocurrency Compliance: An AML Perspective. 2017. URL: http://files.acams.org/pdfs/2017/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott.pdf.

8. *Дзюблюк О.* Соціально-економічні засади суспільної довіри до банківського сектору. *Вісник Тернопільського національного економічного університету.* 2016. № 2. С. 54–69.

9. Ефективність та конкурентоспроможність банківської системи України : монографія / за заг. ред. Г. Т. Карчевої ; ДВНЗ "Ун-т банк. справи". Київ, 2016. 278 с.

10. *Науменкова С. В., Міщенко В. І., Міщенко С. В.* Макроекономічні аспекти оцінювання достатності капіталу банків в Україні. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2017. № 2 (23). С. 4–16. URL: https://doi.org/10.18371/fcaptp.v2i23.121032.

11. *Науменкова С. В., Міщенко В. І., Міщенко С. В.* Цифрові валюти у контексті суспільної довіри до грошей. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2018. № 2 (25). С. 305–316. URL: https://doi.org/10.18371/fcaptp.v2i25.136837.

12. 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.

13. *Mnuchin S.* Panel Discussion at the World Economic Forum: The Remaking of Global Finance. *World Economic Forum*. 2018. January 25. URL: https://www.weforum.org/people/steven-mnuchin.

14. Guidance for a risk-based approach to virtual currencies / FATF-GAFI. 2015. URL: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

15. *Pons C., Gupta G.* Venezuela Says Launch of "Petro" Cryptocurrency Raised USD 735 Million. *Reuters*. 2018. February 20. URL: https://www.reuters.com/article/us-crypto-currencies-venezuela/venezuela-says-launch-of-petro-cryptocurrency-raised-735-million-idUSKCN1G506F.

16. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation the FATF Recommendations (The FATF Recommendations), Recommendation 10 / FATF-GAFI. URL: https://www.cfatf-gafic.org/index.php/documents/fatf-40r/376-fatf-recommendation-10-customer-due-diligence.

17. Electronic Code of Federal Regulations (e-CFR) Title 31. Money and Finance: Treasury Subtitle B. Regulations Relating to Money and Finance Chapter X. Financial Crimes Enforcement Network, Department of the Treasury Part 1010. General provisions Subpart C. Reports required to be made section 1010.313. Aggregation. / Cornell Law School, Legal Information Institute. URL: https://www.law.cornell.edu/cfr/text/31/1010.313.

18. U.S. Code Title 31. Money and finance Subtitle IV. Money Chapter 53. Monetary transactions Subchapter II. Records and reports on monetary instruments transactions Section 5324. Structuring transactions to evade reporting requirement prohibited / Cornell Law School, Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/31/5324.

19. Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States / The Financial Crimes Enforcement Network (FinCEN). 2005. April 26. URL: https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf.

20. Bank Secrecy Act Guide Policies Needed: BSA, OFAC, Anti-Money Laundering, and CIP / The Federal Deposit Insurance Corporation (FDIC). URL: https://www.fdic.gov/regulations/examinations/bsa/.

21. Bank Secrecy Act Anti-Money Laundering Examination Manual / The Federal Financial Institutions Examination Council (FFIEC). 2014. URL: https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf.

References

1. FATF-GAFI. (2012). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: the FATF Recommendations*. Retrieved from http://000.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html.

2. European Parliament, & Council. (2018, May 30). *Directive (EU) 2018/843 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).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843.

3. Sloane, B., & Bhargav, P. (2018, March 18). *Blockchain basics: Introduction to distributed ledgers*. Retrieved from https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-basics-intro-bluemix-trs/.

4. Goldman, Z. K., Maruyama, E., Rosenberg, E. et al. (2017, May). *Terrorist Use of Virtual Currencies, Center for a New American Security*. Retrieved from https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

5. Paesano, F. (2018, April). Regulating cryptocurrencies: challenges & considerations. *Basel Institute on Governance (BIG) Working Paper*, 28. April. Retrieved from https://www.baselgovernance.org/sites/default/files/2019-06/190425%20Working%20Paper%20Cryptocurrency%20Regulations_v2.pdf.

6. Van Saberhagen, N. (2013, October 17). Crypto-Note v. 2.0. *Monero White Paper*. Retrieved from https://www.github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf.

7. Scott, Sh. (2017). *Cryptocurrency Compliance: An AML Perspective*. 2017. Retrieved from http://files.acams.org/pdfs/2017/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott.pdf.

8. Dziubliuk, O. (2016). Socio-economic principles of public confidence in the banking sector. *Herald of Ternopil National Economic University,* 2, 54–69 [in Ukrainian].

9. Karcheva, H. T. (Ed). (2016). *Efficiency and competitiveness of the Ukrainian banking system*. Kyiv: University of Banking [in Ukrainian].

10. Naumenkova, S. V., Mischenko, V. I., & Mischenko, S. V. (2017). Realities and prospects of Ukraine banking system. *Financial and credit activity: problems of theory and practice*, 2 (23), 4–16. DOI: 10.18371/fcaptp.v2i23.121032 [in Ukrainian].

11. Naumenkova, S. V., Mischenko, V. I., & Mischenko, S. V. (2018). Conceptual transformation principles of the income regulation system in Ukraine. *Financial and credit activity: problems of theory and practice*, 2 (25), 305–316. DOI: 10.18371/fcaptp.v2i25.136837 [in Ukrainian].

12. FATF-GAFI. (2014). V*irtual Currencies Key Definitions and Potential AML/CFT Risks*. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

13. Mnuchin, S. (2018, January 25). Panel Discussion at the World Economic Forum: The Remaking of Global Finance. *World Economic Forum*. Retrieved from https://www.weforum.org/people/steven-mnuchin.

14. FATF-GAFI. (2015). *Guidance for a risk-based approach to virtual currencies*. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

15. Pons, C., & Gupta, G. (2018, February 20). Venezuela Says Launch of "Petro" Cryptocurrency Raised USD 735 Million. *Reuters*. Retrieved from https://www.reuters.com/article/us-crypto-currencies-venezuela/venezuela-says-launch-of-petro-cryptocurrency-raised-735-million-idUSKCN1G506F.

16. FATF-GAFI. (n. d.). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation the FATF Recommendations (The FATF Recommendations), Recommendation 10*. Retrieved from https://www.cfatf-gafic.org/index.php/documents/fatf-40r/376-fatf-recommendation-10-customer-due-diligence.

17. Cornell Law School, Legal Information Institute. (n. d.). *Electronic Code of Federal Regulations (e-CFR) Title 31. Money and Finance: Treasury Subtitle B. Regulations Relating to Money and Finance Chapter X. Financial Crimes Enforcement Network, Department of*

the Treasury Part 1010. General provisions Subpart C. Reports required to be made section 1010.313. Aggregation. Retrieved from https://www.law.cornell.edu/cfr/text/31/1010.313.

18. Cornell Law School, Legal Information Institute. (n. d.). *U.S. Code Title 31. Money and finance Subtitle IV. Money Chapter 53. Monetary transactions Subchapter II. Records and reports on monetary instruments transactions Section 5324. Structuring transactions to evade reporting requirement prohibited*. Retrieved from https://www.law.cornell.edu/uscode/text/31/5324.

19. The Financial Crimes Enforcement Network (FinCEN). (2005, April 26). *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States*. Retrieved from https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf.

20. The Federal Deposit Insurance Corporation (FDIC). (n. d.). *Bank Secrecy Act Guide Policies Needed: BSA, OFAC, Anti-Money Laundering, and CIP*. Retrieved from https://www.fdic.gov/regulations/examinations/bsa/.

21. The Federal Financial Institutions Examination Council (FFIEC). (2014). *Bank Secrecy Act Anti-Money Laundering Examination Manual*. Retrieved from https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf.