doi: https://doi.org/10.33763/finukr2021.07.031

УДК 336.7

Т. Л. Дмитренко
кандидат економічних наук, завідувач відділу міжнародних фінансів та фінансової безпеки відділення глобальної економіки і міжнародних фінансів НДФІ ДННУ "Академія фінансового управління", Київ, Україна, AML-консультант ОБСЄ, Відень, Австрія, Tetiana.Dmytrenko@aml.digital
ORCID ID: https://orcid.org/0000-0002-2632-2986

О. О. Любіч
доктор економічних наук, професор, віце-президент ДННУ "Академія фінансового управління", Київ, Україна, alyubich@ukr.net
ORCID ID: https://orcid.org/0000-0002-9339-4242

Ю. В. Пархоменко
керівник експертної групи з розвитку ринку віртуальних активів Міністерства цифрової трансформації України, Київ, Україна, parkhomenko@thedigital.gov.ua

РЕГУЛЮВАННЯ РИНКУ ВІРТУАЛЬНИХ АКТИВІВ: ГЛОБАЛЬНИЙ ТА НАЦІОНАЛЬНИЙ РІВНІ ІМПЛЕМЕНТАЦІЇ МІЖНАРОДНИХ СТАНДАРТІВ ПВК/ФТ[1]

Анотація. Статтю присвячено розробленню 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 побудови "правила подорожей" 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). Розглянуто методичні підходи до таксономії віртуальних активів, класифікації учасників ринку й визначення ризику їхньої участі в операціях з відмивання злочинних доходів і фінансування тероризму, закладено базові принципи секторальної оцінки ризику щодо операцій із віртуальними активами. Особливу увагу приділено заходам, що вживаються Міністерством цифрової трансформації України, зі зниження загроз використання віртуальних активів у тіньовій економіці. Надано рекомендації стосовно розвитку прозорого, цивілізованого крипторинку.

Ключові слова: віртуальні активи, постачальник послуг з віртуальними активами, протидія відмиванню доходів, одержаних злочинним шляхом, ризик-орієнтований підхід, правило подорожей, криптовалютна біржа, крипторинок, секторальна оцінка ризиків.

Рис. 1. **Табл.** 2. **Літ.** 34.

Tetiana Dmytrenko
Ph. D. (Economics), SESE "The Academy of Financial Management", Kyiv, Ukraine, OSCE AML Consultant, Vienna, Austria, Tetiana.Dmytrenko@aml.digital
ORCID ID: https://orcid.org/0000-0002-2632-2986

[1] ПВК/ФТ – протидія відмиванню коштів, одержаних злочинним шляхом, та фінансуванню тероризму.

© Дмитренко Т. Л., Любіч О. О., Пархоменко Ю. В., 2021

Oleksandr Lyubich
Dr. Sc. (Economics), Professor, SESE "The Academy of Financial Management", Kyiv, Ukraine, alyubich@ukr.net
ORCID ID: https://orcid.org/0000-0002-9339-4242

Yuliya Parkhomenko
Ministry of Digital Transformation of Ukraine, Kyiv, Ukraine, parkhomenko@thedigital.gov.ua

VIRTUAL ASSETS MARKET REGULATION: GLOBAL AND NATIONAL LEVEL OF IMPLEMENTATION OF AML/CFT INTERNATIONAL STANDARDS

Abstract. The article is devoted to the implementation of international standards of the Financial Action Task Force (FATF) in the field of new technologies (Recommendation 15) and related risks of money laundering, terrorist financing (AML/CFT). The issues of risk assessment and management are considered from the perspective of the development of the virtual assets (VA) market, its infrastructure, new instruments, and from the perspective of interaction with the banking and payment systems. The article also discusses the current problems of the development and functioning of the global cryptomarket and strategic planning of international cooperation in solving these issues, as well as an action plan at the national level. In addition, virtual asset service providers (VASPs) are trying to determine a cost-effective way to comply with this rule due to the lack of any standardized protocol in the VASP for exchanging such information. The authors disclose methodological approaches to assessing AML/CFT risks (1 Recommendation), mechanisms for conducting a sectoral risk assessment, and specifics of AML procedures, such as identification and verification of customers, determination of beneficial ownership, transfer of such information when performing transactions with virtual assets. The directions of the development of interaction between the central government authorities, the law enforcement system, and participants in the virtual asset market at the national and global level, the need to implement the "Travel Rule" (16 FATF Recommendations), using the latest fintech and blockchain (DLT) technologies to increase the speed and security of transmitted information are also analyzed. In addition, the rule requires VASP beneficiaries to obtain and retain the necessary information about the initiator and beneficiary. Particular attention is paid to the measures of the Ministry of Digital Transformation of Ukraine regarding the reduction of threats to the use of virtual assets in the shadow economy, the development of fraud in cyberspace, cybercrime in order to develop a transparent civilized crypto market and digital technologies in general.

Keywords: virtual assets, virtual asset service provider, counteraction to money laundering, risk-oriented approach, travel rule, cryptocurrency exchange, crypto market, sectoral risk assessment.

JEL classification: F65, G14, G18.

Т. Л. Дмитренко
кандидат экономических наук, заведующая отделом международных финансов и финансовой безопасности отделения глобальной экономики и международных финансов НИФИ ГУНУ "Академия финансового управления", Киев, Украина, AML-консультант ОБСЕ, Вена, Австрия

А. А. Любич
доктор экономических наук, профессор, вице-президент ГУНУ "Академия финансового управления", Киев, Украина

Ю. В. Пархоменко
руководитель экспертной группы по развитию рынка виртуальных активов Министерства цифровой трансформации Украины, Киев, Украина

РЕГУЛИРОВАНИЕ РЫНКА ВИРТУАЛЬНЫХ АКТИВОВ: ГЛОБАЛЬНЫЙ И НАЦИОНАЛЬНЫЙ УРОВНИ ИМПЛЕМЕНТАЦИИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ПОД/ФТ

Аннотация. Статья посвящена разработке подходов к внедрению обновленных Рекомендаций Международной группы по противодействию отмыванию грязных денег (FATF), а именно риск-ориентированного подхода к обращению виртуальных активов и деятельности провайдеров услуг с виртуальными активами, взаимодействия путем построения "правила путешествий" финансового сектора и рынка таких активов относительно уменьшения риска использования их в преступных операциях (в частности, идентификации и верификации клиентов, определения информации об открытых ключах инициаторов трансакций с виртуальными активами и их бенефициарных владельцев), в законодательство Украины и практику Национальной системы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ). Рассмотрены методические подходы к таксономии виртуальных активов, классификации участников рынка и определению риска их участия в операциях по отмыванию преступных доходов и финансированию терроризма, заложены базовые принципы секторальной оценки риска относительно операций с виртуальными активами. Особое внимание уделено мерам, которые принимаются Министерством цифровой трансформации Украины, по снижению угрозы использования виртуальных активов в теневой экономике. Представлены рекомендации относительно развития прозрачного, цивилизованного крипторынка.

Ключевые слова: виртуальные активы, поставщик услуг с виртуальными активами, противодействие отмыванию доходов, полученных преступным путем, риск-ориентированный подход, правило путешествий, криптовалютная биржа, крипторынок, секторальная оценка рисков.

Розвиток фінансової діяльності за участю віртуальних активів (*далі* – VA) і постачальників послуг із віртуальними активами (*далі* – VASP) привертає дедалі більшу увагу світових регуляторних органів. У червні 2019 р. FATF представила Керівництво щодо підходу на основі оцінки ризику – віртуальні активи та постачальники послуг з віртуальними активами (*далі* – Керівництво) [1]. Прийнявши зміни до своїх сорока рекомендацій (*далі* – Рекомендації) [2], FATF проголосила, що всі її вимоги стосовно протидії відмиванню коштів, одержаних злочинним шляхом, та фінансуванню тероризму (*далі* – ПВК/ФТ) застосовуються до операцій із VA та VASP, включаючи (але не обмежуючись цим) використання підходу на основі оцінки й управління ризиком, нагляд або моніторинг VASP із метою протидії відмиванню коштів та фінансуванню тероризму, запобіжні заходи належної перевірки клієнтів, ведення записів і звітування про підозрілі трансакції тощо.

Серед усіх Рекомендацій щодо ПВК/ФТ, висвітлених у Керівництві, Рекомендація 16 [3] (зазначена для VASP у Пояснювальній записці до Рекомендації 15, п. 7(b) [4]), аналогічна "правилу подорожей", що, згідно із Законом США про таємницю банківської діяльності [5, sec. 6308], є однією з найскладніших вимог дотримання VASP. Відповідно до цього правила, VASP, які беруть участь у переданні VA, повинні отримувати і зберігати необхідну інформацію про клієнта та його бенефіціара (ім'я, номер рахунку,

адресу та ін.), а також надійно й оперативно передавати її бенефіціару. Крім того, VASP-бенефіціари мусять отримувати і зберігати основні відомості про джерела походження активів. "Правило подорожей" має на меті простежити операції з VA та визначити відповідного ініціатора й бенефіціара у випадку потенційного відмивання коштів та фінансування тероризму (*далі* – ВК/ФТ), пов'язаного з переданням VA. У Керівництві також підкреслюється, що обмін інформацією про джерела походження та бенефіціарних власників VA не обов'язково повинен бути приєднаний до самої трансакції з VA (тобто дані можуть бути надані як безпосередньо, так і опосередковано). Однак псевдоанонімність віртуальних трансакцій є справжнім викликом для VASP у досягненні відповідності Рекомендації 16.

Додавання особистої інформації до блокчейну чи іншої розподіленої книги може спричиняти занепокоєння щодо конфіденційності. Втім, відстеження адреси гаманця VA можливо уникнути, оскільки вона або пов'язана із фактичним джерелом чи бенефіціарним власником, або ні. Більше того, VASP намагаються визначити економічний і ефективний спосіб дотримання правил через відсутність будь-якого стандартизованого протоколу між постачальниками цих активів для обміну такою інформацією, що створює загрозу з боку злочинної діяльності.

На проблематику пом'якшення ризиків, пов'язаних із використанням VA у злочинній діяльності на глобальному й національному рівнях націлені секторальна, національна та супранаціональна оцінка ризиків як інструмент оцінювання ризику й комплекс пропозицій активних дій щодо пом'якшення виявлених ризиків і загроз та гармонізації систем ПВК/ФТ різних країн. Для інтеграції результатів оцінок ризиків необхідно застосовувати сумісні підходи проведення таких оцінок. Саме ці виклики наразі долаються на всіх рівнях міжнародними організаціями за допомогою співпраці з представниками ринку VA, фінансового ринку та наукової спільноти.

Питанням віртуальних активів присвячено спеціальні дослідження фахівців центральних банків Євросоюзу, Федеральної резервної системи США та країн Східної Азії, Австралії, таких як А. Грінберг, А. Мойсеєнко, К. Ізенман, Л. Моєн [6–8] та ін.

Уже зазначалося, що особлива увага приділяється ризикам, пов'язаним із використанням VA як засобу платежу та об'єкта інвестування, а також управлінню такими ризиками. Постає питання реагування наглядових органів центральної влади і правоохоронної системи на подібні загрози. Вітчизняні дослідники поки що приділяють недостатню увагу потенційному й реальному використанню VA, тим більше у сфері ПВК/ФТ. В Україні віртуальні валюти в аспекті розкриття їхньої сутності та довіри до них досліджують Т. Л. Дмитренко, О. О. Любіч, В. І. Міщенко, С. В. Міщенко, С. В. Науменкова, В. Г. Швець, Т. В. Яцик [9–11] та ін., однак питання протидії використанню VA для відмивання грошей розглядається в загальних рисах.

Метою статті є вивчення міжнародних стандартів ПВК/ФТ, визначення шляхів їх упровадження в національне законодавство та ефективного регулювання ринку VA, оцінювання ризиків часткової імплементації міжнародних стандартів ПВК/ФТ, роботи Комітету експертів Ради Європи з оцінки заходів боротьби з відмиванням грошей і фінансуванням тероризму (MONEYVAL) щодо імплементації оновленої редакції Рекомендації 15 FATF про новітні технології та пов'язаних із нею Рекомендацій 1 і 16. А також надання пропозиції стосовно побудови ефективної взаємодії VASP із учасниками банківського й небанківського секторів фінансового ринку та інших секторів економіки, державними наглядовими і правоохоронними органами на національному й глобальному рівнях.

Рекомендація 16, аналогічна "правилу подорожі" згідно із Законом про банківську таємницю США [5], розроблена з метою запобігання неконтрольованому доступу терористів та інших злочинців до електронних переказів коштів. Країни повинні:

– забезпечити отримання фінансовими установами необхідних та чітких відомостей про відправника й вигодоодержувача (бенефіціара) грошових переказів і пов'язаних повідомлень, а також відповідний інформаційний супровід грошових переказів або пов'язаних повідомлень на всіх етапах здійснення платежу;

– забезпечити моніторинг фінансовими установами грошових переказів для відстеження таких переказів коштів, які не супроводжуються повною необхідною інформацією про відправника коштів та/або вигодоодержувача (бенефіціара), та за потреби вжиття відповідних заходів;

– у контексті обробки грошових переказів забезпечити реалізацію фінансовими установами заходів щодо замороження, а також заборонити проведення операцій із включеними до списку фізичними та юридичними особами відповідно до зобов'язань, визначених у відповідних резолюціях Ради безпеки ООН, таких як № 1267 (1999 р.) [12] і наступних, пов'язаних із нею резолюціях, а також № 1373 (2001 р.) [13], котрі стосуються запобігання й протидії тероризму та його фінансуванню.

З цією метою встановлено такі вимоги до фінансових установ:

– включати необхідні й точні відомості про джерела походження коштів клієнта, відповідні повідомлення про банківські перекази та інформацію, що їх супроводжує на всіх етапах здійснення платежу;

– відстежувати ланцюгові перекази, щоб виявити тих, кому бракує необхідної інформації про ініціатора та/або отримувача, і вжити відповідних заходів;

– заморожувати чи забороняти проведення операцій із зазначеними фізичними і юридичними особами в контексті обробки банківських переказів [12].

Керівництво радить застосовувати Рекомендацію 16 до всіх VASP, щоб гарантувати, що VA не використовуються терористами та іншими злочинцями для переміщення незаконно отриманих коштів [2].

У Пояснювальній записці до Рекомендації 15, п. 7(b), зазначено, що VASP повинні отримувати від ініціатора операції та зберігати необхідну й точну інформацію про джерела та про вигодоотримувача (бенефіціара) ініціатора щодо передання VA, подати її до бенефіціара VASP чи фінансової установи, якщо така є, та негайно й у надійний спосіб передати запитувану інформацію на запит відповідних органів влади. Подібним чином, бенефіціари VASP повинні отримувати та зберігати необхідну інформацію про ініціатора операції з VA, а також надавати її за запитом відповідних органів влади негайно й у надійний спосіб.

У контексті діяльності VA під необхідною інформацією розуміються:

– ім'я автора, тобто клієнта-відправника;

– номер рахунку ініціатора, коли цей рахунок використовується для обробки трансакції (наприклад, гаманець VA);

– фізична (географічна) адреса ініціатора – національний ідентифікаційний номер чи ідентифікаційний номер клієнта (тобто не номер трансакції), який однозначно ідентифікує особу, котра розпочала процедуру замовлення, або дата й місце народження;

– ім'я бенефіціара;

– номер рахунку бенефіціара, коли такий рахунок використовується для обробки трансакції (наприклад, гаманець VA) [4].

Керівництво детально описує механізм, що полегшує надання необхідної для переказу інформації:

1. Не обов'язково, щоб інформація додавалася безпосередньо до переказу VA. Вона може бути подана як безпосередньо, так і опосередковано. Передбачено, що необхідна інформація не повинна передаватися як частина або включення в переказ на блокчейні чи іншій платформі DLT. Її надання бенефіціару VASP може бути абсолютно окремим від операції з VA [1]. Будь-яке технологічне або програмне рішення є прийнятним за умови, що воно дає змогу установам-бенефіціарам дотримуватися вимог Рекомендації 16.

2. FATF підкреслює, що механізм передання інформації може бути написаним кодом в основному протоколі трансакції DLT переказу VA чи таким, що працює поверх платформи DLT (наприклад, за допомогою смарт-контракту, цифрового підпису або іншої технології – незалежної (тобто не DLT) платформи обміну повідомленнями чи програми, інтерфейсу програми (API)); допускається й будь-який інший ефективний (негайний і надійний) засіб для дотримання Рекомендації 16.

3. Керівництво вимагає необхідної (негайної й надійної) процедури передання інформації, пов'язаної з VA, для обміну між VASP-джерелом і VASP-бенефіціаром. Враховуючи транскордонний характер, глобальне охоплення та швидкість трансакції переказу VA, "негайно" означає, що VASP повинні подати необхідну інформацію разом або одночасно із самим переказом, "надійно" – що VASP мають гарантувати цілісність і доступність до необхідної інформації, отриманої від VASP чи інших зобов'язаних осіб, для полегшення ведення діловодства (серед інших вимог) та захистити її від несанкціонованого розголошення.

Керівництво також містить перелік даних щодо оцінки VASP із метою впровадження ризик-орієнтованого підходу для ідентифікації бенефіціарів переказів VA, а також передання джерела походження активів бенефіціара для подальшого переказу VA на платформі DLT. Цей перелік включає відкриті й приватні ключі; транспортний рівень безпеки / рівень захищених сокетів (TLS/SSL) з'єднання; сертифікати X.509; сертифікати атрибутів X.509; технологію API чи іншу комерційну технологію або програмне забезпечення чи рішення для обміну даними [14].

"Правило подорожей", офіційно прийняте FATF 21 червня 2019 р., – це зобов'язання щодо дотримання міжнародних стандартів про боротьбу з відмиванням коштів та фінансуванням тероризму, що їх повинні застосовувати фінансові установи в 37 країнах – членах FATF. Його ще називають "правилом криптоподорожей", оскільки воно імітує "правило подорожі" Закону США про конфіденційність банківської діяльності. Крім того, вважається, що це правило замінює зусилля, спрямовані на боротьбу з відмиванням коштів та реалізацію політики "Знай свого клієнта" (KYC) [15].

Відповідно до Рекомендації 16, ініціатори й бенефіціари переказів цифрових фондів повинні обмінюватись описовою інформацією. "Правило подорожей" застосовуватиметься до всіх VASP, фінансових установ та залучених до операцій організацій. До цього криптоіндустрія намагалася боротися з відмиванням грошей і фінансуванням тероризму шляхом здійснення політик KYC і KYT ("Знай свою трансакцію"), що дає змогу встановити ідентичність зареєстрованих облікових записів користувачів та підозрілих переказів криптоактивів.

Як складова Рекомендації 16 передання VA має супроводжуватися такою інформацією: ім'я, номер рахунку, фізична адреса, національний ідентифікаційний номер, ідентифікаційний номер клієнта, дата й місцезнаходження ініціаторів і бенефіціарів переказу, а також номери банківських рахунків, що належать ініціаторам трансакції.

Підприємства або фізичні особи, визначені в класифікації бізнесу як постачальники послуг віртуальних активів (VASP), повинні здійснювати обмін даними та VA, забезпечувати передання, випуск, захист і виконання зобов'язань з віртуальних активів, відповідно до "правила подорожей" Рекомендації 16.

VASP збирають і зберігають необхідну й достовірну інформацію про активи, про бенефіціарів та передають її до установ-бенефіціарів, якщо такі є, а останні отримують її та зберігають.

Якщо локальні VASP не відповідають стандартам FATF, вона залишає за собою право накладати санкції на країни таких VASP, додаючи їх до списку спостереження щодо високого ризику імплементації міжнародних стандартів (сірий список) або до списку несумісності з міжнародними стандартами FATF (чорний список).

Країни визначають дотримання положень FATF щодо протидії відмиванню коштів та фінансуванню тероризму пріоритетом діяльності VASP у

всіх юрисдикціях. У березні 2019 р. налічувалося до 20 країн, де володіння біткоїнами було незаконним чи обмеженим. У разі відсутності відповідного рішення щодо "правила подорожей" у 2020 р. збільшення їх кількості може стати реальним ризиком. Коли країни стикаються з відмиванням грошей і фінансуванням тероризму через криптоактиви, найпростішим рішенням є їх повна заборона.

На додаток до численних, різноманітних викликів, питання передання необхідних даних для дотримання "правила подорожей" щодо VASP і подібних норм перебуває в процесі вирішення. Наразі багато криптокомпаній виконують дві третини вимог, встановлених цим правилом та глобальними регуляторними Рекомендаціями FATF.

Експерти стверджують, що криптогалузь краще представити за допомогою простої структури й набору ресурсів, котрі всі VASP можуть використовувати для впровадження міжнародних стандартів ПВК/ФТ на основі власних потреб і вимог місцевої юрисдикції. У червні 2021 р. FATF розглянула прийняття вдосконалених галузевих настанов щодо оцінки ризику та майбутніх кроків для протидії злочинній діяльності на ринку VA. Варто зауважити: чим більш гармонізованими є правила між усіма учасниками національних систем ПВК/ФТ, тим легше їх упроваджувати в діяльність галузі й застосовувати як на національному рівні, так і на глобальному ринку.

На черговому засіданні в червні 2021 р. FATF заявила, що цього року, завдяки швидкому розвитку технології віртуальних активів, вона продовжуватиме оцінювати галузь та робити наступні заохочувальні кроки у сфері ПВК/ФТ. Ціллю "правила подорожей" і спільною метою політик та процедур ПВК (KYC, CDD) залишається очищення від злочинного та утвердження легального використання VA для забезпечення їх довгострокового обігу.

"Правило подорожей" є важливим інструментом, який допомагає фінансовим установам дотримуватися міжнародних стандартів у сфері ПВК/ФТ. VASP, котрі не встигають відповідати цим новим нормативним вимогам, загрожує вимирання. (Про це свідчать недавні події, коли нові правила, такі як CryptoBridge [16], є причиною закриття торгових майданчиків.) Тому VASP повинні ініціювати конструктивну й об'єктивну дискусію з регуляторами, щоб уникнути такої ситуації не лише у 2021 р., а й у наступному десятилітті.

Слід звернути увагу на те, що у 2020 р. розроблено нові криптографічні норми, а також проведено масштабні заходи правозастосування щодо діяльності VASP та їхніх керівників через відсутність відповідності нормативним актам. Прогалини в цих правилах є тими можливостями, котрими користуються відмивачі грошей і терористичні організації. Зокрема, потенціал відмивання грошей криптовалютних бірж, наявність міксерів, що змішують великі обсяги трансакцій із метою неможливості відстеження ланцюга операцій, та анонімних віртуальних валют (Monero) розглядаються законодавцями як спроба уникнути регулювання, враховуючи їхню природу.

Застосування рекомендацій і положень про боротьбу з відмиванням коштів та фінансуванням тероризму до VA й VASP згідно з Керівництвом стикається з різними проблемами, зокрема такими:

• Анонімність. Використання псевдоніма й посилення анонімності характеру діяльності з VA ускладнює ідентифікацію кожної особи, котра стоїть за трансакцією з VA, та передання інформації про таку особу з метою дотримання "правила подорожей". Навіть якщо VASP пов'язує рахунок VA кожного клієнта з його реальною ідентифікацією, ця дія буде ефективною лише в разі, коли клієнт зберігає свої VA з обліковим записом VASP. Тільки-но клієнт вилучає свої VA від одного VASP і надсилає їх іншому VASP, належний контроль для відстеження трансакції через обов'язкове виконання політик KYC (без використання аналітичних програм таких компаній, як "Chainanalysis" [17], "Crystal" [18], "Elliptic" [19], "CipherTrace" [20] і подібних) стає неможливим. Саме цю проблему покликане розв'язати "правило подорожей".

• Порушення конфіденційності. Одним із можливих рішень для дотримання "правила подорожей" є прикріплення необхідних для ідентифікації даних безпосередньо до інформації про трансакції на блокчейні або іншому розподіленому реєстрі. Проте це порушуватиме конфіденційність. Зокрема, VASP мав би необхідну інформацію про ініціатора (тобто замовника, котрий відправляє), а також про бенефіціара (тобто одержувача). Відомості для ідентифікації як ініціатора, так і бенефіціара розкриваються й записуються в реєстрі. Хоча таким чином забезпечується дотримання "правила подорожей", це означає також, що кожен вузол у блокчейні чи відповідному розподіленому реєстрі доступний усім і кожний має доступ до такої особистої інформації без можливості її зміни.

• Відсутність ефективного за часом і витратами способу дотримання "правила подорожей". VASP намагаються визначити економічний та доступний спосіб дотримання правила через відсутність стандартизованого протоколу між VASP для обміну такою інформацією. Оскільки кожний VASP приймає різні процедури ідентифікації й верифікації клієнтів, а отже, й вимоги ризиковості до операцій із VA, це змушує одного постачальника послуг із віртуальними активами узгоджувати з іншим постачальником вимоги щодо взаємодії та відповідність стандартам по кожній трансакції. Крім того, зазначене може перешкодити дотриманню правила, а також здатності VASP масштабувати свої бізнес-моделі.

Визначений добровільною самооцінкою державний сектор демонструє чітке спрямування на прийняття та впровадження переглянутих стандартів FATF. 32 із 54 юрисдикцій, котрі відповідають FATF-стилю регіонального органу (FSRM), повідомили, що мають чинні норми протидії відмиванню коштів і фінансуванню тероризму для VASP, 13 – що в них є правила, які розробляються, а ще 5 юрисдикцій – про чинну або потенційну заборону VASP (рисунок).

Рисунок. **Державний сектор: упровадження урядами крипторегулятивних норм протидії відмиванню коштів та фінансуванню тероризму**

Джерело: Cryptocurrency Crime and Anti-Money Laundering Report / CipherTrace Cryptocurrency Intelligence. 2021. February.

У Звіті про кримінальні злочини та боротьбу з відмиванням грошей аналітичної криптовалютної розвідки компанії "CipherTrace" (лютий 2021 р.) [20] також зазначається, що з 32 юрисдикцій із встановленими режимами надання послуг VA ПВК/ФТ 30 ввели режими ліцензування або реєстрації, при цьому 18 юрисдикцій рекомендують поширити свої норми на VASP, зареєстровані за кордоном, які пропонують товари чи послуги клієнтам у їхніх юрисдикціях. Більшість юрисдикцій, котрі розпочали процедури ліцензування й реєстрації VASP, повідомили про наявність менш ніж 10 зареєстрованих VASP, у решті число VASP перевищує 100. Понад 1000 зареєстрованих чи ліцензованих VASP функціонують тільки у 20 юрисдикціях.

Побоювання, пов'язані з децентралізованими обмінами та регуляторною відповідальністю, спричинили потребу в подальших вказівках для визначення обсягу вимог щодо протидії відмиванню коштів і фінансуванню тероризму для VASP у конкретних юрисдикціях. Режими нагляду запроваджені в 31-й із 32 юрисдикцій зі встановленими нормативно-правовими рамками у формі центральних банків, податкових органів або спеціалізованих організацій. 15 юрисдикцій повідомили, що їхні відповідні наглядові органи почали проводити перевірки на місцях та поза ними, причому 8 юрисдикцій уже накладають покарання за порушення ПВК/ФТ.

Прийняття й застосування "правила подорожей" у межах юрисдикцій FATF були обмеженими, причому останні посилаються на відсутність масштабних технологічних рішень, які охоплювали б усі вимоги з дотримання VASP. Незважаючи на те, що FATF обстоює технологічно нейтральну позицію, орган, котрий розробляє політику, визнав наявність безлічі пер-

спективних рішень, звернувши увагу на спробу реалізації галузевої ініціативи щодо стандартизації систем обміну повідомленнями в рамках спільноти VASP.

Хоча FATF налаштована загалом оптимістично, вона визнає існування серйозних бар'єрів на шляху впровадження правила, такі як виявлення контрагентів VASP, ширше використання "холодних" (приватних) і нехостинг-гаманців, що здійснюють трансакції з клієнтами VASP, пакетна обробка даних, проблеми сумісності та ін. Запропонувавши декілька негайних рішень, Контактна група віртуальних активів FATF (робоча група, призначена для моніторингу й залучення сектору VA) підтвердила прихильність до партнерства з галуззю із метою виявлення та просування рішень щодо поточних і майбутніх перешкод, оскільки як VASP, так і регулятори наближаються до впровадження "правила подорожей", закликаючи спільноту до подальшої роботи та подвоєння зусиль із залученням неохочих VASP до введення міжнародних стандартів і розв'язання решти проблем. FATF очікує істотного прогресу в напрямі подолання проблем із дотриманням "правила подорожей" протягом наступних 12 місяців.

У змаганні за пошук механізму його дотримання ключовим фактором є галузева співпраця: ініціативи з відкритим кодом виявилися головними чинниками, націленими на інтеграцію та зручність використання в протоколах VASP, захищаючи цінності безпеки й конфіденційності. Серед перспективних рішень – створення Альянсу обміну інформацією про правила подорожей (TRISA), який уже впровадив стандарт повідомлень interVASP IVMS101 і співпрацює з PayID, OpenVASP, Shyft та BIP75 [21]. Постійний відкритий діалог, тісна співпраця між VASP та регуляторний нагляд украй необхідні, оскільки і приватний, і державний сектори просуваються до більш безпечної, захищеної й доступної системи цифрових платежів у всьому світі.

За підсумками 2020 р. у річних звітах аналітичних компаній "Chainanalysis", "Crystal", "Elliptic", "CipherTrace" [17–20] висловлюється занепокоєння через число користувачів і трансакцій, пов'язаних із приватними стейблкоїнами, а також відсутність ПВК/ФТ-регулювання з боку приватного й державного секторів для подолання розширення такої діяльності.

Крім того, FATF запропонувала такі стратегії зниження ризику, як відсутність контролю протидії відмиванню коштів, що здійснюється за межами переказів VASP-VASP; обмеження трансакцій чи обсягу однорангових трансакцій; проведення операцій із VA з використанням посередницького VASP або фінансової установи та, у крайньому разі, заборона переказів із допомогою нехостинг-гаманців [22].

Протягом наступного 12-місячного періоду триватиме дослідження мінливого ландшафту ризику та даватимуться подальші вказівки щодо обмеження можливостей ВК/ФТ, котрі відкриває застосування нехостинг-гаманців. FATF закликає галузь проявляти ініціативу в упровадженні AML-процедур при прийнятті нових продуктів, послуг і технологій, аби забезпе-

чити постійне дотримання зобов'язань із ПВК/ФТ та підготовку до майбутніх регуляторних обмежень.

Наступні кроки FATF із метою дотримання вимог криптопротидії ВК/ФТ очікуються під час головування представника Німеччини М. Плеєра [17]. Він обіцяє домагатися більш жорсткого режиму протидії відмиванню грошей та визначив п'ять основних напрямів діяльності:

– AML/CFT процедури при цифровому перетворенні;
– протидія фінансуванню тероризму з етнічною чи расовою мотивацією;
– протидія відмиванню грошей за участі контрабанди мігрантів;
– протидія екологічній злочинності;
– протидія незаконній торгівлі зброєю.

Під час головування Німеччини FATF і далі розвиватиме введені стандарти VA. Частиною її плану щодо цифрової трансформації ПВК/ФТ є започаткування ініціативи з моніторингу ризиків VA. На відміну від попереднього президентства, це триватиме не один, а два роки. Зазначена ініціатива включатиме два дослідження можливостей і викликів для VASP/VA для ефективнішого впровадження ПВК/ФТ, а також збір та аналіз поточної інформації VASP/VA стосовно ПВК/ФТ.

FATF не розглядає цифрові валюти центрального банку (CBDC) як віртуальні активи, натомість вона використовує стандарти, подібні до будь-якої іншої форми фіатної валюти, випущеної центробанком [10]. Децентралізовані біржі, платформи чи програми вважаються VASP. Децентралізований, або розподілений, додаток (DApp) не є VASP за стандартами FATF (останні не застосовуються до базового програмного забезпечення чи технології), але суб'єкти, що беруть участь у DApp, такі як власники або оператори, можуть бути VASP згідно з визначенням FATF. Послуги депозитного обслуговування VA, в т. ч. ті, котрі включають технологію смарт-контрактів, брокерські послуги, послуги обміну замовлень (торгові майданчики), розширені торгові послуги та провайдери зберігання – всі вони є VASP [6].

Деякі незамінювані токени (NFT), котрі спочатку не є VA, насправді можуть бути ними на вторинних ринках, що дозволяють передання чи обмін вартості або сприяють відмиванню грошей, фінансуванню тероризму та розповсюдження зброї масового знищення.

Активи не повинні вважатися неохопленими Рекомендаціями FATF через формат, у котрому вони пропонуються, й жодний актив не має тлумачитись як такий, що повністю виходить за межі стандартів FATF [11]. Окрім ризиків ВК/ФТ VASP повинні почати оцінювати та пом'якшувати ризики фінансування розповсюдження зброї масового знищення. Наразі FATF розробляє окремі вказівки для роз'яснення цих вимог. Стандарти FATF застосовуються до так званих приватних стабільних монет.

FATF рекомендує країнам аналізувати й пом'якшувати ризики ВК/ФТ перед упровадженням VA, особливо якщо приватний стейблкоїн буде використовуватися для трансакцій P2P. Зменшення ризику може включати обмеження сфери можливості клієнтів здійснювати анонімні трансакції та/

або шляхом забезпечення виконання зобов'язань не зобов'язаних до реєстрації/ліцензування осіб щодо ПВК/ФТ у рамках угоди, наприклад за допомогою програмного забезпечення для моніторингу трансакцій і виявлення підозрілої діяльності [22]. Трансакції до/від не зобов'язаних до реєстрації/ліцензування юридичних осіб (наприклад, нехостинг-гаманців) і такі, на більш ранньому етапі котрих відбувалися трансакції P2P, варто вважати ризикованішими.

FATF рекомендує такі можливі тактики зменшення ризику операцій P2P у юрисдикціях із високим ризиком:

- реалізація VA – еквівалента STR (звіт про підозрілі операції);
- відмова в ліцензуванні VASP, якщо вони дозволяють здійснювати трансакції до/від не зобов'язаних до реєстрації/ліцензування юридичних осіб (тобто приватних чи нехостинг-гаманців);
- посилення вимог до ведення діловодства й до належної перевірки (CDD);
- постійний пильний нагляд за VASP;
- видання публічних рекомендацій і рекомендацій для підвищення обізнаності щодо ризиків, пов'язаних із трансакціями P2P.

VASP, котрі не застосовували "правило подорожей", слід вважати ризикованішими. VASP повинен здійснити перевірку контрагента VASP перед тим, як передати далі необхідну інформацію. Незалежно від наявності регулювання в юрисдикції бенефіціара, VASP можуть вимагати від бенефіціарів дотримання "правила подорожей" згідно з контрактом чи діловою практикою. Загалом такі ділові рішення приймаються кожним окремим VASP на основі оцінки ризиків. Організатори й бенефіціари VASP повинні перевіряти трансакції з метою підтвердження, що контрагент не є санкційною особою [7].

Надання інформації про організаторів і бенефіціарів допускається в разі, якщо це відбувається негайно та надійно, відповідно до стандартів FATF. Представлення необхідної інформації за фактом не можна дозволяти (тобто це має робитися до або під час передання VA). У випадку відсутності організації-ініціатора чи організації-бенефіціара (трансакції до та із нехостинг-гаманців) VASP все одно повинен збирати необхідну інформацію про свого клієнта. Країни також мають розглянути вимогу VASP щодо розгляду таких передач VA як операцій із підвищеним ризиком, котрі потребують посиленого контролю й обмежень.

При впровадженні "правила подорожей" потрібно належним чином перевірити контрагента VASP. Для того щоб така перевірка була своєчасною й безпечною, FATF рекомендує застосовувати трифазний підхід:

Етап 1: з'ясування, чи здійснюється передання VA контрагентом VASP, чи вони спрямовуються в нехостинг- гаманець чи іншу службу.

Етап 2: визначення контрагента VASP.

Етап 3: 1) встановлення, чи є контрагент VASP придатним для надсилання даних про клієнтів і ділових відносин із ним; 2) використання блокчейн-аналітики для оцінювання VASP та виявлення розбіжностей; 3) виконання

повної перевірки контрагента VASP перед першою операцією з VASP; 4) періодичні перевірки надійності контрагента VASP; 5) упровадження оновлених вказівок щодо ліцензування й реєстрації VASP [8].

Стандарти FATF дають можливість юрисдикціям гнучко застосовувати процедури ліцензування/реєстрації VASP. Щодо VASP регіональні наглядові органи повинні вимагати як мінімум ліцензування чи реєстрації в юрисдикції (країнах), де вони створені. Юрисдикції також мають право примушувати VASP, котрі пропонують товари та/або послуги клієнтам, що перебувають у їхній юрисдикції, отримати ліцензію чи зареєструватися в ній. Національні органи влади повинні мати механізми для моніторингу сектору VASP і виявлення фізичних або юридичних осіб, які здійснюють діяльність чи операції з VA без необхідної ліцензії/реєстрації.

Обмін інформацією між органами влади й приватним сектором та їхніми міжнародними колегами є вкрай важливим у секторі VASP через транскордонний характер і багатовідомчий діапазон VA та VASP. FATF розробила принципи обміну інформацією та співпраці між наглядачами VASP під новим керівництвом. Повний їх перелік охоплює визначення органів нагляду й VASP, а також найкращі практики обміну інформацією та співпраці юрисдикцій.

Кожна країна має призначити принаймні один компетентний орган як свого керівника VASP для цілей ПВК/ФТ, і він не може бути органом саморегулювання. Для цілей ПВК/ФТ країни повинні чітко ідентифікувати своїх керівників VASP. Якщо VASP працює в декількох юрисдикціях, первинний наглядач може бути визначений, коли VASP проводить істотну частку своїх господарських операцій у цій юрисдикції [7].

Протягом останніх п'яти років віртуальні активи дедалі частіше використовуються для різних законних видів діяльності, включаючи інвестиції чи трансакції. Незважаючи на це, VA мають певні особливості у сфері ВК/ФТ, котрі роблять їх вразливими до зловживань із боку злочинців. Широке застосування злочинцями VA створює серйозні виклики для VASP, фінансових установ, наглядових і правоохоронних органів.

У зв'язку з необхідністю вертикальної оцінки ризиків щодо VASP [23] розробляється комплексна класифікація й систематизація різних типів VA та VASP, описуються основні загрози у сфері ВК/ФТ, які виникають через використання віртуальних активів (включаючи торгівлю наркотиками, шахрайство, підробки та крадіжки).

Оцінка визначає невід'ємний ризик восьми типів і підтипів VA (табл. 1). Псевдоанонімні VA (біткоїн) та анонімні (Monero) вважаються такими, що мають дуже високий рівень вказаного ризику через свою анонімність, зручність у використанні й особливості безпеки.

Оцінка ризику також включає визначення рівня невід'ємного ризику у 12 підтипів VASP (табл. 2). Загальний рейтинг ризику VASP оцінюється як середній. Слід зауважити, що українські VASP повинні зареєструватися в Міністерстві цифрової трансформації України з моменту набрання чиннос-

Таблиця 1. **Оцінка ризику віртуальних активів**

Типи активів	Підтипи активів	Невід'ємний ризик
Платіжні VA (криптовалюти)	Псевдоанонімні	Дуже високий
	Анонімні	Дуже високий
	Платформи	Високий
	Стейблкоїни (монети)	Середній
Утілітні (службові) VA		Низький
Інвестиційні VA	Забезпечені VA	Низький
	Платформа VA із функціями забезпечення	Середній
VA закритих екосистем		Дуже низький

Складено за: CipherTrace випускає свої дружні AML інструменти для криптобірж / Hebergementwebs. URL: https://www.hebergementwebs.com/%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD/ciphertrace-publishes-its-aml-fatfriendly-tools-for-crypto-exchange; Дмитренко Т. Л., Любіч О. О. Упровадження міжнародних стандартів регулювання ринку віртуальних активів в Україні. *Фінанси України*. 2020. № 9. С. 65–79.

Таблиця 2. **Оцінка ризику постачальників послуг із віртуальними активами**

Типи постачальників	Підтипи постачальників	Невід'ємний ризик
Емісії та їх розміщення (андеррайтинг)	ICO/IEO	Середній
Зберігання (кастодіальна діяльність)	Постачальники зберігачів гаманців	Середній
	Спеціалізоване зберігання	Середній
Обмінники й біржі	Централізовані біржі	Високий
	Однорангові (P2P) біржі	Середній
	Брокери	Середній
	VA ATMs	Низький
Програмні послуги та інструменти	Централізовані застосунки	Середній
	Децентралізовані застосунки	Середній
Інші	Аноніматори	Середній
	Керівники фондів	Середній
	Майнери або валідатори	Низький

Складено за: Cryptocurrency Anti-Money Laundering Report. 2019 Q3. November 34 / CipherTrace. URL: https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/; Дмитренко Т. Л., Любіч О. О. Упровадження міжнародних стандартів регулювання ринку віртуальних активів в Україні. *Фінанси України*. 2020. № 9. С. 65–79.

ті Законом України "Про віртуальні активи" (проєкт закону від 11.06.2020 № 3637) [24]. Отже, цей документ є попередньою оцінкою вказаного сектору щодо ризиків у сфері ВК/ФТ.

Оцінка ризику також описує пом'якшувальні фактори, які VASP зобов'язані застосовувати для зменшення ризику у сфері ВК/ФТ відповідно до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" від 16.08.2020 № 361-IX [25], а також інших нормативних актів, що стосуються оцінки й управління ризиками у сфері ПВК/ФТ. Державна служба фінансового моніторингу

України опублікувала два загальних попередження щодо VA і VASP та продовжує отримувати звіти про підозрілі операції (STR), пов'язані з VA або VASP, на добровільних засадах від різних організацій. Прокуратура й правоохоронні органи також впровадили необхідні аналітичні програми для аналізу справ, пов'язаних із VA.

FATF опублікувала 14 вересня 2020 р. перелік так званих індикаторів червоного прапорця [26], котрі суб'єкти господарювання повинні враховувати. Цей перелік має підтримувати приватні організації в моніторингу транзакцій та сприяти вдосконаленню їхньої звітності, що подається до підрозділу фінансової розвідки. Оцінку ризику планується оновити найближчим часом, коли уявлення про ринок стане повнішим.

Протягом останніх п'яти років VA дедалі частіше застосовують у різних законних видах діяльності, наприклад у інвестиціях чи торгових операціях. Водночас VA мають певні особливості, які роблять їх вразливими до зловживань у сфері ВК/ФТ, де у 2019 р. здійснено оборудок на суму понад 10 млрд дол. США [20]. Широке використання злочинцями VA створює серйозні виклики для VASP, наглядових і правоохоронних органів.

Міжнародні організації також визнали ризик щодо VA та VASP. У 2018 р. ЄС прийняв П'яту директиву щодо боротьби з відмиванням грошей (5 AMLD) [27], згідно з якою провайдери, що надають послуги з обміну між віртуальними й фіатними валютами, та провайдери зберігачів гаманців підлягають регулюванню у сфері ПВК/ФТ. У 2019 р. FATF видала Керівництво щодо застосування підходу, який ґрунтується на оцінці ризику щодо VA та VASP [28]. Воно вимагало від країн виявити, зрозуміти й оцінити свої ризики у сфері ВК/ФТ, пов'язані з VA і VASP, та діяти з метою їх ефективного пом'якшення. В липні 2020 р. FATF оприлюднила огляд упровадження її стандартів щодо VA та VASP [29]. Раніше, у 2015 р., вона опублікувала Керівництво щодо підходу на основі ризику до віртуальних валют [30]. У 2019 р. Орган з оцінки наднаціонального ризику ЄС (SNRA) [31] також оголосив про вищий ризик використання VA і VASP. Окрім того, у 2019 р. Європейський банківський орган (EBA) проаналізував застосування та придатність законодавства ЄС до криптоактивів [32].

Віртуальні активи мають унікальні технологічні властивості, котрі забезпечують псевдоанонімні й анонімні трансакції, швидке транскордонне передання вартості та неособисті ділові відносини. Ці властивості можуть поліпшити різноманітні фінансові продукти й послуги, такі як фінансування торгівлі, транскордонні платежі та врегулювання фінансових інструментів. Традиційні фінансові установи визнали ці переваги. Наприклад, опитування Банку міжнародних розрахунків, здійснене серед 63 центральних банків, показало, що більшість із них розглядали можливість емісії за підтримки центробанків щодо VA у 2018 р. [33].

Рівень прийняття VA на ринку в усьому світі зростає. Кількість VA з ринковою капіталізацією щонайменше на 1 млн дол. США збільшилася з 30 до приблизно 1000 між 2015 і 2020 рр., а загальна капіталізація всіх VA наближається до 300 млрд дол. [34]. Підвищення рівня прийняття користува-

чами VA та властивих їм технологічних особливостей призвело до широкого використання таких активів для діяльності у сфері ВК/ФТ. VA продають нелегальні ринки продуктів і схеми шахрайства з інвестиціями, чий сукупний дохід того ж року сягнув понад 1 млрд дол. США. Також віртуальні активи дедалі частіше застосовуються групами фінансування тероризму, кіберзлочинцями та спекулянтами із сексуальною експлуатацією.

Останні досягнення у сфері цифрових технологій дають можливість фінансовим установам ефективніше аналізувати великі обсяги структурованих і неструктурованих даних та ефективніше визначати закономірності й тенденції. Збір даних і спільна аналітика допомагають фінансовим установам у розумінні, оцінюванні та пом'якшенні ризиків ВК/ФТ, що сприяє простішому, динамічнішому й ефективнішому визначенню таких видів діяльності, зменшенню кількості помилкових спрацьовувань, завдяки чому приватний сектор виконуватиме вимоги вчасно й менш обтяжливо. Це також може перешкодити злочинцям скористатися інформаційними прогалинами, оскільки вони взаємодіють із безліччю вітчизняних і міжнародних фінансових служб, кожна з яких має обмежений та частковий огляд операцій. Разом із тим це може негативно позначитися на захисті особистих і основних прав. Тому надзвичайно важливо, щоб будь-який обмін інформацією відбувався з дотриманням національних та міжнародних правових засад захисту даних і конфіденційності.

Результати проведеного дослідження дають можливість сформулювати пропозиції щодо розвитку ринку віртуальних активів в Україні, впровадження міжнародних стандартів FATF та Європейського Союзу в діяльність провайдерів послуг із віртуальними активами, налагодження взаємодії представників бізнесу, органів законодавчої й виконавчої влади, правоохоронних органів, громадянського суспільства як на національному, так і на глобальному рівні.

Для виконання вимог Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" від 06.12.2019 № 361-IX [25], що передбачено Рекомендаціями FATF шляхом вжиття заходів із ПВК/ФТ на ринку віртуальних активів, необхідно розробити Секторальну оцінку ризиків для цього сектору економіки. Але без прийняття Закону України "Про віртуальні активи" (законопроєкт від 11.06.2020 № 3637) [24] та реєстрації суб'єктів ринку як суб'єктів первинного фінансового моніторингу перейти до такої оцінки ризиків на державному рівні неможливо. Тому першою й головною пропозицією наразі є прийняття державного законодавчого акта для розроблення наступних кроків цивілізованого розвитку віртуальних активів.

Список використаних джерел

1. 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.

2. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation / FATF. 2012. URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

3. Recommendation 16: Wire transfers / FATF. URL: https://www.cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers.

4. Recommendation 15: New technologies / FATF. URL: https://cfatf-gafic.org/index.php/documents/fatf-40r/381-fatf-recommendation-15-new-technologies.

5. National Defense Authorization Act for Fiscal Year 2021 : H.R. 6395 (116th) / USA Congress. URL: https://www.govtrack.us/congress/bills/116/hr6395/text.

6. 2nd Global Cryptoasset Benchmarking Study / M. Rauchs, A. Blandin, K. Klein et al. Cambridge Centre for Alternative Finance, 2018. URL: https://doi.org/10.2139/ssrn.3306125.

7. *Greenberg A.* Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire. 2017. URL: https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

8. *Moiseienko A., Izenman K.* Gaming the System: Money Laundering Through Online Games. *RUSI Newsbrief*. 2019. Vol. 39, No. 9. URL: https://static.rusi.org/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf.

9. *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.

10. *Міщенко В. І., Науменкова С. В., Міщенко С. В.* Цифрові гроші центральних банків: майбутнє інституційних змін у банківському секторі. *Фінанси України*. 2021. № 2. С. 26–48. URL: https://doi.org/10.33763/finukr2021.02.026.

11. *Yatsyk T., Shvets V.* Cryptoassets as an emerging class of digital assets in the financial accounting. *Economic Annals-XXI*. 2020. No. 183 (5-6). P. 106–115. URL: https://doi.org/10.21003/ea.V183-10.

12. Резолюция 1267 (1999), принятая Советом Безопасности ООН на его 4051-м заседании, от 15.10.1999 № 1267(1999). URL: https://zakon.rada.gov.ua/laws/show/995_452#Text.

13. Резолюция 1373 (2001), принятая Советом Безопасности ООН на его 4385-м заседании, от 28.09.2001 № 1373(2001). URL: https://zakon.rada.gov.ua/laws/show/995_854#Text.

14. Рекомендації FATF. Міжнародні стандарти боротьби з відмиванням коштів, фінансуванням тероризму і розповсюдженням зброї масового знищення. Методологія з оцінки 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. Лютий. URL: https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf.

15. Директива 2005/60/ЄС Європейського Парламенту та Ради про запобігання використанню фінансової системи з метою відмивання коштів та фінансування тероризму від 26.10.2005. URL: http://zakon3.rada.gov.ua/laws/show/994_774.

16. Today's Cryptocurrency Prices by Market Cap / CoinMarketCap. URL: https://coinmarketcap.com/.

17. The 2020 State of Crypto Crime / Chainanalysis. 2020. January. URL: https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/257%20-%20001%20Appendix%20A%20-%202020-Crypto-Crime-Report%20Chainanalysis.pdf.

18. *Khaustova M.* Crystal Blockchain End of Year Report 2020. 2020. December 21. URL: https://crystalblockchain.com/articles/crystal-blockchain-end-of-year-report-2020.

19. Financial Crime Typologies 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?utm_campaign=Typologies%20Campaign%20%7C%20Q4%202020%20-%20Q1%202021&utm_medium=email&_hsmi=102370644&_hsenc=p2ANqtz--bpoJScViE4WFHyea40NrVG40XpoNFQFRd-cpluYgKT3uveLvgZSzN1HdyNmP0OzZbdjCVUfApDF7bwr8Kv9DaNcsxDA&utm_content=102370644&utm_source=hs_automation.

20. Cryptocurrency Anti-Money Laundering Report, 2019 Q3 / CipherTrace Cryptocurrency Intelligence. 2019. November. URL: https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/.

21. CipherTrace випускає свої дружні AML інструменти для криптобірж / Hebergementwebs. 2021. 12 берез. URL: https://www.hebergementwebs.com/%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD/ciphertrace-publishes-its-aml-fatfriendly-tools-for-crypto-exchange.

22. Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers / FATF. 2021. March. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html.

23. ML/TF vertical risk assessment: virtual asset service providers / SCCF. 2020. December. URL: https://www.cssf.lu/en/Document/ml-tf-vertical-risk-assessment-virtual-asset-service-providers/.

24. Проєкт Закону про віртуальні активи від 11.06.2020 № 3637 / Верховна Рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=69110.

25. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : закон України від 16.08.2020 № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text.

26. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets / FATF. 2020. URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

27. 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. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843.

28. Guidance for a risk-based approach to virtual assets and virtual asset service providers. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

29. 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.

30. Guidance for a risk-based approach to virtual currencies / FATF. 2019. URL: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

31. Supranational National Risk Assessment : Report from the Commission to the European Parliament and the Council / European Commission. Brussels, 2019. URL: https://

ec.europa.eu/info/sites/default/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

32. Report with advice for the European Commission on crypto-assets / EBA. 2019. January. URL: https://eba.europa.eu/eba-reports-on-crypto-assets.

33. Proceeding with caution – a survey on central bank digital currency / The Bank of International Settlements. 2019. January. URL: https://www.bis.org/publ/bppdf/bispap101.htm.

34. CoinMarketCap. URL: https://coinmarketcap.com.

References

1. FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Retrieved from http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

2. FATF. (2012). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

3. FATF. (n. d.). *Recommendation 16: Wire transfers*. Retrieved from https://www.cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers.

4. FATF. (n. d.). *Recommendation 15: New technologies*. Retrieved from https://cfatf-gafic.org/index.php/documents/fatf-40r/381-fatf-recommendation-15-new-technologies.

5. USA Congress. (2020). *National Defense Authorization Act for Fiscal Year 2021*. Retrieved from https://www.govtrack.us/congress/bills/116/hr6395/text.

6. Rauchs, M., Blandin, A., Klein, K., Pieters, G., Recanatini, M., & Zhang, B. (2018). *2nd Global Cryptoasset Benchmarking Study*. Cambridge Centre for Alternative Finance. DOI: 10.2139/ssrn.3306125.

7. Greenberg, A. (2017). *Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire*. Retrieved from https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

8. Moiseienko, A., & Izenman, K. (2019). Gaming the System: Money Laundering Through Online Games. *RUSI Newsbrief*, 39 (9). Retrieved from https://static.rusi.org/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf.

9. Dmytrenko, T., & Lyubich, O. (2020). Implementation of international standards of virtual assets market regulation in Ukraine. *Finance of Ukraine*, 9. 65–79. DOI: 10.33763/finukr2020.09.065 [in Ukrainian].

10. Mishchenko, V., Naumenkova, S., & Mishchenko, S. (2021). Central bank digital currency: the future of institutional changes in the banking sector. *Finance of Ukraine*, 2, 26–48. DOI: 10.33763/finukr2021.02.026 [in Ukrainian].

11. Yatsyk, T., & Shvets, V. (2020). Cryptoassets as an emerging class of digital assets in the financial accounting. *Economic Annals-XXI*, 183 (5-6), 106–115. DOI: 10.21003/ea.V183-10 [in Ukrainian].

12. United Nations Security Council. (1999). *Resolution 1267 (1999), adopted at 4051 meetings* (No. 1267(1999), October 15). Retrieved from https://zakon.rada.gov.ua/laws/show/995_452#Text [in Russian].

13. United Nations Security Council. (2001). *Resolution 1373 (2001) adopted at the 4385th meeting* (No. 1373(2001), September 28). Retrieved from https://zakon.rada.gov.ua/laws/show/995_854#Text [in Russian].

14. FATF recommendations. International standards for combating money laundering, terrorist financing and proliferation of weapons of mass destruction. Methodology for assessing compliance with FATF recommendations and the effectiveness of anti-money laundering and anti-terrorist financing systems. Rules and procedures of the 5th round of mutual evaluations by the MONEYVAL committee. (2018, February). Retrieved from https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf [in Ukrainian].

15. European Parliament, & EU Council. (2005, October 26). *Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*. Retrieved from http://zakon3.rada.gov.ua/laws/show/994_774 [in Ukrainian].

16. CoinMarketCap. (n. d.). *Today's Cryptocurrency Prices by Market Cap*. Retrieved from https://coinmarketcap.com/.

17. Chainanalysis. (2020, January). *The 2020 State of Crypto Crime*. Retrieved from https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/257%20-%20001%20Appendix%20A%20-%202020-Crypto-Crime-Report%20Chainanalysis.pdf.

18. Khaustova, M. (2020, December 21). *Crystal Blockchain End of Year Report 2020*. Retrieved from https://crystalblockchain.com/articles/crystal-blockchain-end-of-year-report-2020.

19. Elliptic. (2020). *Financial Crime Typologies in Cryptoassets. The Concise Guide for Compliance Leaders*. Retrieved from https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf?utm_campaign=Typologies%20Campaign%20%7C%20Q4%202020%20-%20Q1%202021&utm_medium=email&_hsmi=102370644&_hsenc=p2ANqtz--bpoJScViE4WFHyea40NrVG40XpoNFQFRd-cpluYgKT3uveLvgZSzN1HdyNmP0OzZbdjCVUfApDF7bwr8Kv9DaNcsxDA&utm_content=102370644&utm_source=hs_automation.

20. CipherTrace Cryptocurrency Intelligence. (2019, November). *Cryptocurrency Anti-Money Laundering Report, 2019 Q3*. Retrieved from https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/.

21. Hebergementwebs. (2021, March 12). *CipherTrace releases its friendly AML tools for cryptocurrencies*. Retrieved from https://www.hebergementwebs.com/%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD/ciphertrace-publishes-its-aml-fatfriendly-tools-for-crypto-exchange [in Ukrainian].

22. FATF. (2021, March). *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*. Retrieved from http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html.

23. SCCF. (2020, December). *ML/TF vertical risk assessment: virtual asset service providers*. Retrieved from https://www.cssf.lu/en/Document/ml-tf-vertical-risk-assessment-virtual-asset-service-providers/.

24. Verkhovna Rada of Ukraine. (2021). *Virtual Assets Act* (Draft Law No. 3637, June 11). Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=69110 [in Ukrainian].

25. Verkhovna Rada of Ukraine. (2020). *On prevention and counteraction to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction* (Act No. 361-IX, August 16). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text [in Ukrainian].

26. FATF. (2020). *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

27. European Parliament, & EU 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*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843.

28. FATF. (2019). *Guidance for a risk-based approach to virtual currencies*. Retrieved from http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

29. FATF. (2020, June). *FATF Report to G20 on So-Called Stablecoins*. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.

30. FATF. (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.

31. European Commission. (2019). *Supranational National Risk Assessment* (Report from the Commission to the European Parliament and the Council). Brussels. Retrieved from https://ec.europa.eu/info/sites/default/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

32. EBA. (2019, January). *Report with advice for the European Commission on crypto-assets*. Retrieved from https://eba.europa.eu/eba-reports-on-crypto-assets.

33. The Bank of International Settlements. (2019, January). *Proceeding with caution – a survey on central bank digital currency*. Retrieved from https://www.bis.org/publ/bppdf/bispap101.htm.

34. CoinMarketCap. (n. d.). Retrieved from https://coinmarketcap.com.