УДК 342.951

БІЛАН І.А., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1237-1565.

ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ КРИПТОВАЛЮТ З МЕТОЮ ФІНАНСУВАННЯ ТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВІЙНИ

DOI...

Анотація. *Визначено світові тенденції сучасності у контексті розвитку міжнародної криптоіндустрії. Деталізовано загрози фінансування тероризму та легалізації доходів, здобутих злочинним шляхом з використанням криптовалюти та віртуальних активів. Розкрито роль та місце механізмів AML/CFT. Узагальнено напрямки діяльності FATF з метою запобігання використанню віртуальних активів для фінансування тероризму. За рекомендаціями FATF окреслено основні ризики та виклики для держав, пов'язані із операціями із віртуальними активами. Деталізовано зусилля світової спільноти щодо попередження глобальних ризиків та недопущення масштабування відмивання коштів й фінансування тероризму за допомогою криптовалют. Обгрунтовано доцільність подальшого санкційного тиску та повного виключення рф із держав-членів FATF, внесення її до чорного списку. Визначено здобутки вітчизняної спецслужби у напрямку протидії використанню криптовалют з метою фінансування тероризму. Підсумовано подальші шляхи посилення спроможностей щодо запобігання фінансуванню тероризму з боку держави-агресора.*

Ключові слова: *фінансова система, віртуальні активи, криптовалюта, криптосектор, злочинність, фінансування тероризму, міжнародні терористичні угрупування, легалізація доходів, здобутих злочинним шляхом, технологія блокчейн, криптобіржі.*

Summary*. The modern world trends in the context of the development of the international crypto industry are defined. The threats of terrorist financing and the legalization of criminally obtained income with the use of cryptocurrency and virtual assets are detailed. The role and place of AML/CFT mechanisms are revealed. The directions of FATF activities to prevent the use of virtual assets for criminal purposes and to finance terrorism are summarized. The FATF recommendations outline the main risks and challenges for states related to transactions with virtual assets. The efforts of the world community to prevent global risks and the scaling of money laundering and terrorist financing using cryptocurrencies are detailed. The expediency of further sanctions pressure and the complete exclusion of the Russian Federation from the FATF member states, including its inclusion in the black list, are substantiated. The achievements of the domestic special service in the direction of countering the use of cryptocurrencies for the purpose of financing terrorism have been identified. The further directions to strengthen capabilities to prevent the scale of terrorism financing by the aggressor state are summarized.*

Keywords: *financial system, virtual assets, cryptocurrency, crypto sector, crime, terrorist financing, international terrorist groups, legalization criminal proceeds, blockchain technology, crypto exchanges.*

Постановка проблеми. Світова тенденція сучасності – глобальний та стрімкий розвиток міжнародної криптоіндустрії. Криптовалюти дедалі більше стають звичайною складовою світу фінансів та входять у повсякденне життя, конкуруючи з атрибутами традиційної економіки. На цьому фоні все частіше населення світу використовує саме криптогаманці у якості альтернативи банківським рахункам та фіантним грошам. Поява криптоіндустрії та альтернативних платіжних систем є відповіддю на масштабні виклики цифровізації та зміну моделей поведінки споживачів таких платіжних сервісів.

Адже наявність проблем з дерегуляцією криптовалютних платежів може завдати істотного удару по економічній безпеці держав [11, с. 105]. У зв'язку із зростанням популярності криптовалют, провідні держави у всьому світі переймаються цією проблематикою та намагаються розробити відповідні нормативні акти. У цьому контексті наша держава нещодавно легалізувала ринок віртуальних активів, що у свою чергу, має стати потужним стимулом для розвитку вітчизняної цифрової економіки. 16 березня 2023 року – саме у цей день Президент України підписав довгоочікуваний Закон України "Про віртуальні активи" [1], що дає змогу нарешті запустити криптовалютний ринок в Україні. Очікувано такий стан справ має допомогти залучити додаткові інвестиції, збільшити податкові надходження до державного бюджету, сприяти розвитку національного криптосектору. Врегульований обіг віртуальних активів, вірогідно, зможе як повернути увагу та довіру іноземних інвесторів, так і значно покращити загальний імідж України на світовій арені.

Як засвідчує вітчизняний досвід, відповідно до анонсованого щорічного Послання Президента України до Верховної Ради України про внутрішнє та зовнішнє становище [2], наша країна поступово стає світовим лідером у цифровій трансформації держави та суспільства в цілому. Динамічний розвиток криптоіндустрії одночасно провокує сучасні загрозливі тенденції та виклики, які мають бути вирішеними на системній основі саме завдяки законодавчому врегулюванню обігу криптовалют. Україна в цьому контексті не відстає від загальносвітових тенденцій та робить важливі кроки щодо законодавчого забезпечення розбудови власної моделі криптосектору.

На фоні позитивних аспектів, криптовалюти мають і зворотню сторону. Фінансування тероризму, наркоторгівля, незаконний обіг зброї, вибухівки, засобів ураження, легалізація та відмивання доходів, здобутих злочинним шляхом, дистанційні крадіжки та вимагання грошових коштів з використанням сучасних інформаційних технологій вже важко уявити без залучення та використання можливостей криптовалют. В умовах війни висвітлення загрозливих тенденцій використання віртуальних активів та криптовалют з метою фінансування тероризму є особливо актуальним й своєчасним.

Результати аналізу наукових публікацій. Проблемні питання оподаткування криптовалютних операцій висвітлювали у своїх наукових працях: Д. Кобильник та А. Бурчак [9], Н. Данко [6], І. Спільник та О. Ярощук [12], О. Чаплинська [13] та інші. Кримінальні правопорушення у сфері обігу криптовалюти та можливості блокчейн-технологій у розслідуванні злочинів, вчинених у кіберпросторі, досліджували Д. Казначеєва, А. Дорош [7], Ю. Калайда [8] та ін. Деякі аспекти використання криптовалют з метою легалізації доходів, здобутих злочинним шляхом та фінансування терроризму висвітлювали у своїх наукових роботах: О. Грабчук та І. Супрунова [3], Д. Гресь [4], Т. Гринчук та Л. Гусак [5], А. Демчук [6], А. Крит'єв [11]. Проте не достатньо дослідженими залишаються питання протидії використанню криптовалют з метою фінансування тероризму, особливо в умовах повномасштабної війни рф проти України.

Метою статті є визначення на основі аналізу загрозливих тенденцій використання віртуальних активів та криптовалют для фінансування тероризму, подальших шляхів запобігання злочинному використанню криптовалют як засобу фінансування тероризму та відмивання "брудних" коштів в умовах війни.

Виклад основного матеріалу. Світова популярність криптовалют тримається на таких базових факторах, як: анонімність користувачів, децентралізація, низька або нульова комісія за операціями. При дотриманні цих вимог, зацікавленість криптовалютою постійно зростає, навіть через великі фінансові ризики, які вона становить. Останнім часом криптовалюта, завдяки своїм сприятливим характеристикам та привабливості, все

частіше використовується у злочинних цілях та з метою фінансування тероризму. У світових масштабах фінансування терористичної діяльності за допомогою криптовалюти за останній рік збільшилося вчетверо, за підрахунками міжнародних експертів близько 20 % усіх терактів спонсорувалося саме за допомогою криптовалют. Згідно звіту Chainalysis, у 2022 році терористичні організації та хакерські угруповання отримали тіньових майже $10 млрд. США саме завдяки криптовалютам.

Починаючи з 24 лютого 2022 року для багатьох криптовалютних бірж актуальним стало виявлення та розслідування незаконних операцій щодо фінансування терористичної діяльності російських окупантів в Україні за допомогою криптовалюти. Фахівці з'ясували, що з початку 2022-го нелегальні проросійські групи у різних країнах, багато представників яких є у санкційних списках, зібрали для військових угруповань окупантів понад $4 млн. США. За результатами моніторингу трансакцій були ідентифіковані військові російські злочинці, які використовували криптовалюту саме для фінансування збройної агресії рф проти України. За наслідками виявлення злочинної активності, тисячі трансакцій, пов'язаних із підозрілою нелегальною активністю було заблоковано. Це пояснюється тим, що після виходу міжнародних платіжних систем з рф різко зріс попит на послуги саме криптобірж. Адже криптовалюти не зможуть повноформатно допомогти рф здійснювати торгівлю та бізнес в обхід західних санкцій через обмежений ринок та застосування на криптобіржах механізмів з відстеження платежів. Ліцензовані криптобіржі повинні відповідати вимогам та стандартам міжнародного законодавства щодо протидії відмиванню коштів та фінансуванню тероризму, що має значно ускладнити використання криптовалют для обходу санкцій.

Фінансування тероризму – це його матеріальна підтримка, основна причина загибелі багатьох людей внаслідок скоєння терористичних актів, диверсійно-підривної діяльності або військової агресії. На цьому фоні терористи та інші злочинці активно використовують новітні механізми відмивання коштів для того, щоб приховати справжнє джерело походження своїх фінансових активів та здобутих злочинних доходів. Практично існують різні методи відмивання грошей, а їхня кількість регулярно та прогресивно збільшується, у тому числі, завдяки шаленому глобальному розвитку цифрових технологій та популярності віртуальних активів. Такий стан справ провокує діяльність світової спільноти у напрямку активізації зусиль з метою запобігання та протидії будь-яким спробам використання криптовалют для фінансування тероризму.

Реагуючи на виклики та загрози, пов'язані із відмиванням коштів, здобутих злочинним шляхом та з метою системної протидії фінансуванню тероризму, світовою спільнотою розроблено механізми під назвою Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) – протидія відмиванню грошей та фінансуванню тероризму. Квінтесенцією цієї моделі є стримування надходження незаконних грошей у міжнародну фінансову систему та протидія фінансуванню тероризму. Закони AML/CFT з'явилися на світовій арені незабаром після утворення міжнародної структури Financial Action Task Force on Money Laundering (FATF) – Міжнародної групи з протидії відмиванню брудних грошей. Положення AML/CFT відрізняються в залежності від країни, але є глобальні спроби узгодити відповідні міжнародні стандарти [14]. В сучасних умовах механізми AML/CFT – це, у тому числі, й процедури ідентифікації осіб, що користуються та здійснюють операції з криптовалютами. Після отримання такої інформації її перевіряють та зберігають. Інформація користувача містить дані про доходи та витрати. Таку процедуру проводять постійно, щоб протидіяти відмиванню грошей, прямому фінансуванню терористичних організацій, створенню зброї масового знищення, спонсоруванню злочинних організацій тощо. На виконання нормативних вимог

збирається інформація не стільки про користувача, скільки про його матеріальний статок, отримані доходи та витрати.

Багато років FATF спостерігає за розвитком ринку віртуальних активів та працює над заходами, які повинні вживатися країнами для запобігання використання віртуальних активів у злочинних цілях та з метою фінансування тероризму. Найважчим у цьому напрямку діяльності є стрімкий розвиток сфери діджиталізації, поява різних видів платіжних електронних методів та типів віртуальних валют. Основними ризиками для держав є те, що операції з віртуальними активами важко відслідкувати, так як вони забезпечують високий рівень анонімності. У більшості країн взагалі немає законів та чітко визначеного державного органу, який би здійснював регулювання та контроль за обігом віртуальних активів, суб'єктами надання послуг, пов'язаних з віртуальними активами. Для мотивування країн запроваджувати регулювання у сфері віртуальних активів, FATF включила відповідні вимоги до Стандартів, які є обов'язковими до виконання цивілізованими країнами. Згідно зі Стандартом 14, країни повинні вжити заходів для забезпечення того, щоб фізичні чи юридичні особи, які надають послуги, пов'язані з віртуальними активами, мали ліцензію, були зареєстровані та підпадали під ефективні системи моніторингу та забезпечення виконання відповідних вимог, вказаних у Стандартах FATF. Група розробки фінансових заходів боротьби з відмиванням грошей в особі FATF розпочала щорічні перевірки постачальників криптовалют. Країни, які не дотримуються правил, будуть додані до "особливого списку", що посилить контроль за ними з боку організації. Крім того, FATF планує додавати до "чорного списку" країни, які не зможуть врегулювати проблеми нагляду за криптовалютами. Такі країни зазнають економічних санкцій та інших суттєвих фінансових обмежень.

За правилами, встановленими FATF, необхідно визначати особу, яка займається введенням віртуальної валюти в обіг і має повноваження викуповувати віртуальну валюту, у статусі "адміністратора" віртуальної валюти. Чимало криптовалют – включно з Bitcoin, Litecoin та Etherium – не мають адміністратора. Такі криптовалюти працюють на програмному забезпеченні з відкритим вихідним кодом, який регулює видачу та погашення, і жодна сторона не має права змінювати програмне забезпечення або правила обміну. Існують також інші віртуальні валюти, які використовують "розподілену книгу" для перевірки переказів, зберігаючи при цьому центральний контроль над видачею та погашенням. В результаті, є широкий діапазон віртуальних валют, монет та токенів, які мають різні характеристики і підлягають різним ступеням контролю з боку їхніх операторів. Децентралізованість криптовалют є основним фактором, що приваблює зловмисників та відмивачів грошових коштів. При цьому, створення та обіг криптовалюти вимагають розробки відповідного програмного забезпечення, яке встановлює правила її використання, регулює емісію та погашення криптовалюти.

Незважаючи на постійні заклики до прийняття глобальних стандартів боротьби з відмиванням коштів для торгівлі криптовалютами, таких єдиних правил, на жаль, поки що не існує. Однак постачальники платіжних послуг у криптовалюті повинні підпадати під ті ж зобов'язання, що і платники звичайними коштами, і більшість юрисдикцій дійшли логічного висновку, що комерційний обмін криптовалютами повинен підлягати зобов'язанням щодо процедур AML/CFT. Фінансування тероризму за допомогою криптовалют має величезний обсяг та забезпечує анонімність відправників цих коштів, проте механізми AML/CFT-ідентифікації здатні запобігти таким злочинним випадкам. Тобто механізми AML/CFT створено для того, щоб протидіяти легалізації доходів, які є незаконними та запобігти фінансуванню тероризму. Цей фінансовий інструмент надає змогу проаналізувати і зрозуміти, які кошти є незаконними.

Починаючи з 2019 року, міжнародна структура FATF регулярно оновлює своє "Керівництво щодо менеджменту ризиків для віртуальних активів і постачальників послуг віртуальних активів". Це основний документ, яким керуються більшість країн світу при впровадженні стандартів AML у криптосфері. На його вимоги також орієнтуються криптобіржі, відповідні сервіси та індивідуальні власники криптовалют. У рекомендаціях FATF зазначається, що країни та суб'єкти, які беруть участь у діяльності, пов'язаній з віртуальними активами, повинні усвідомлювати відповідні ризики та вживати преветентивних заходів з метою зниження таких ризиків. Керівництво щодо менеджменту ризиків для віртуальних активів і постачальників послуг віртуальних активів, яке розроблене FATF у 2019 році, орієнтовано на 180 країн світу. Відповідно до документу постачальники послуг віртуальних активів (VASP), а також криптовалютні біржі й постачальники цифрових гаманців зобов'язані збирати інформацію про відправників та отримувачів за криптовалютними трансакціями на загальну суму від $1000 США. На виконання розроблених нормативів, держави повинні карати постачальників послуг віртуальних активів у випадку недотримання ними вимог на законодавчому рівні, використовуючи штрафи та санкції. Від країн-членів FATF вимагалося запровадити усі встановлені превентивні заходи цієї міжнародної структури, включаючи комплексну перевірку клієнтів, ведення обліку та звітності щодо підозрілих трансакцій та їхню подальшу перевірку.

У жовтні 2021 року міжнародна організація FATF оновила вказані нормативні вимоги, які є частиною постійного моніторингу діяльності постачальників послуг віртуальних активів (VASP). Керівництво FATF 2021 року містить оновлення, які зосереджені на таких ключових сферах: уточнення визначення віртуальних активів; загальні вказівки щодо застосування стандартів FATF до стейблкойнів; додаткові вказівки щодо інструментів, доступних країнам для боротьби із вірогідними ризиками відмивання грошей і фінансування тероризму для однорангових операцій; оновлені інструкції щодо ліцензування та реєстрації VASP; додаткові вказівки для державного та приватного секторів щодо впровадження "правила подорожей"; Принципи обміну інформацією та співпраці між керівниками VASP [15]. За результатами діяльності з моніторингу FATF формує чорний список країн, до якого потрапляють країни з дуже складною економіко-правовою ситуацією та такі, що мають високий ризик відмивання грошей, або спонсорують тероризм. Це, зокрема, Куба, Іран, Північна Корея та Сирія. Щодо Ірану, Північної Кореї FATF закликає застосовувати жорсткі санкції для того, щоб змусити ці країни дотримуватися рекомендацій та встановлених міжнародних нормативних вимог. Вірогідно, що ці країни мають дуже слабку фінансову систему відносно міжнародних стандартів, запроваджених FATF. Чорним списком FATF прийнятно називати перелік держав світу, які порушують міжнародні вимоги щодо боротьби з відмиванням коштів, та які фінансують тероризм. У разі віднесення тієї чи іншої країни до "чорного списку" FATF здійснює суттєвий вплив на її економічну та фінансову стабільність, що призводить до відмови інших держав мати будь-які справи із державою-порушником міжнародної фінансової дисципліни та як наслідок – повна економічна ізоляція.

Загальновідомо, що російське військово-політичне керівництво не лише відмиває "брудні" гроші, а й сприяє фінансуванню збройної агресії та актів тероризму проти України. У річницю повномасштабного вторгнення в Україну, а саме у лютому 2023 року, рф отримала чергову "догану" від авторитетних світових інститутцій: FATF своїм рішенням безстроково припинила членство рф у Міжнародній групі з протидії відмиванню коштів. Підставами для цього стали такі чинники та передумови, як: величезні фінансові ризики, пов'язані із державою-агресором, військові дії проти України, численні порушення

законів війни та прав людини, безліч військових злочинів, чисельні акти тероризму та його спонсорування. Тобто світова спільнота дійшла висновку, що злочинні дії рф протирічать основним принципам діяльності FATF, які спрямовані на сприяння та забезпечення глобальної безпеки й цілісності світової фінансової системи.

За таких умов, Україна активно наполягає на повному виключенні рф з усіх міжнародних організацій, у тому числі й FATF та Інтерполу, для того, щоб згодом внести державу-агресора до так званого "чорного списку", що допоможе позбавити російську військову машину потужного фінансування. Проте, на жаль, такі заклики не отримали одностайного схвалення з боку міжнародної спільноти та деякі світові регулятори не солідарні з українськими пропозиціями у вказаному контексті. Так, зокрема, Інтерпол зберіг за рф право міжнародного розшуку та повернення злочинців, їхніх активів протягом всього 2023 року. Станом на червень 2023 року рф, навіть в умовах безстрокового припинення членства у FATF, не віднесено ані до "чорного", ані до "сірого" списків, які налічують понад 20 країн світу – визнаних спонсорів тероризму. По факту, дійсно відбулося призупинення членства рф у FATF, що не є ідентичним включення держави-агресора до чорного списку, а видається лише проміжним етапом. Тобто таке рішення FATF не можна вважати повною перемогою над ворогом.

Зрозуміло, що навіть без внесення до т.зв. "чорного списку" безстрокове призупинення членства рф у FATF матиме для цієї країни значні негативні та критичні наслідки на світовій арені. Це, у свою чергу, призведе до ще більшого зниження довіри іноземних інвесторів, значно ускладнить приток інвестиційного капіталу до московії. Призупинення членства рф у FATF означатиме, що усі суб'єкти, здійснюючи будь-які трансакції з російською банківською системою мають проявляти обережність, посилити перевірку та оцінку ризиків, а глобальні юрисдикції повинні закріпити своє регулювання та оновити рекомендації за фінансовими ризиками. У зв'язку із призупиненням членства рф у FATF ймовірно буде ускладнення зовнішньої торгівлі та з проведенням міжнародних платежів. Такий важливий крок має послабити економіку держави-агресора та ускладнити фінансування війни. Найбільш уразливою має стати російська банківська система, яка й без того страждає від потужніх санкцій. Російські банки очікує зменшення присутності у світовій фінансові системі та скорочення обсягів внутрішнього ринку, у зв'язку з чим робота банківської системи стає нерентабельною. З метою фінансування своєї злочинної діяльності, російські терористи активно використовують саме віртуальні валюти та криптовалюти. Цей спосіб набув актуальності саме завдяки таким особливостям: анонімність, децентралізація, швидкість проведення операцій, неможливість скасування трансакції, безлімітне переміщення фінансових активів за кордон, відсутність належного правового регулювання тощо.

Тому, в сучасних умовах, велика та значна роль відводиться саме діяльності міжнародній інституції FATF щодо протидії фінансуванню тероризму та відмивання "брудних" коштів. На цьому фоні FATF мають інформувати світові фінансові регулятори та спостерігати за тим, щоб у подальшому рф та її сателіти лімітували фінансування тероризму. Якщо рф буде продовжувати свої терористичні дії на території України, вона має опинитися у повній економічній ізоляції та під потужним санкційним тиском. Повне виключення рф із держав членів FATF та внесення її до "чорного списку" – принциповий, адекватний та важливий крок. На переконання світових експертів, це утворює універсальний контроль за фінансовою системою рф, який має ускладнити для агресора пошук альтернативних інструментів щодо обходу санкцій, обмежити міжнародну торгівлю, можливості отримання експортних платежів та має прискорити відтік капіталу із країни.

Слід зазначити, що санкційний тиск з боку світової спільноти проти рф приносить свої реальні й позитивні результати. Восьмий пакет санкцій вплинув навіть на криптосферу: усі криптокомпанії, які отримали ліцензію у країнах ЄС мали завершити усі відносини з рашистами до 22 жовтня 2022 року включно на виконання вимог Ради ЄС. Канада і США також підтримали рішення ЄС. Отже, російські трейдери можуть співпрацювати лише з криптобіржами з Азії, Африки, Латинської Америки, Австралії та Океанії, де ринок криптовалюти значно менший та менш релевантний. На цьому фоні держава Іран розглядає можливість посісти пріоритетне місце серед країн, що активно використовують криптовалюту з метою фінансової підтримки рф. Ще у серпні 2022 року Іран заявив, що планує масштабно використовувати смарт-контракти, а його майнери та валідатори будуть торгувати з державою-агресором. Підставами для цього став той факт, що через санкції рф втратила доступ до ринку криптовалют у ЄС, проте криптовалюта все одно може бути залучена для фінансування тероризму в обхід санкцій за допомогою російських сателітів [16]. Доцільно вказати, що наразі сформований та запущений 11-й пакет санкцій ЄС проти рф, спрямований на усунення будь-яких можливих лазівок з боку держави-агресора. Також члени ЄС шукають нові та дієві способи для того, щоб посилити обмеження на ключові сектори російської економіки і боротися з ухиленням від санкцій через треті країни, особливо Латинської Америки, Африки та Південно-Східної Азії.

Проте, на жаль, рф змогла накопичити за кордоном близько третини ймовірних доходів, отриманих минулого року від експорту товарів. За даними “Bloomberg”, близько $80 млрд. США накопичено у вигляді готівки, криптовалют, нерухомості та інвестиціях у філії за кордоном. Ці ресурси є тіньовими резервами, побічним продуктом рекордного позитивного сальдо рахунку поточних операцій (приблизно різниця між експортом та імпортом), який допоміг підтримати фінанси рф після нападу на Україну в лютому 2022 року. Доля російських коштів та криптовалют за кордоном перебуває у центрі дедалі більшої уваги, оскільки союзники України, такі як Канада та Німеччина, висувають ідею використання мільярдів заморожених російських активів для компенсації країні та допомоги в її відновленні.

Члени Європейського Парламенту у березні 2023 року схвалили жорсткіші правила задля усунення існуючих прогалин у боротьбі з відмиванням грошей, фінансуванням тероризму та ухиленням від санкцій в ЄС. Відповідно до схвалених документів, банки, менеджери активів і криптоактивів, агенти з нерухомості та віртуальної нерухомості зобов’язані перевіряти своїх клієнтів (чим вони володіють і хто контролює компанію). Зазначені організації також повинні будуть встановити детальні типи ризиків відмивання грошей та фінансування тероризму у своїй сфері діяльності та передавати відповідну інформацію до центрального реєстру. Щоб обмежити операції із готівкою та криптоактивами, депутати Європарламенту хочуть обмежити платежі, які можуть приймати особи, які надають товари чи послуги. Будуть встановлені ліміти до 7 тис. Євро для готівкових платежів та 1 тис. Євро для переказів криптоактивів у разі, коли неможливо ідентифікувати особу клієнта. Також будуть заборонені будь-які схеми отримання громадянства за інвестиції (“золоті паспорти”) і буде здійснюватися контроль за так званими “золотими візами”. Крім того, кожна держава-член ЄС повинна буде створити підрозділ фінансової розвідки (ПФР) для запобігання, звітування та боротьби з відмиванням грошей і фінансуванням тероризму [17].

Заслуговує на увагу позиція О. Грабчука та І. Супрунової, що фінансування тероризму через мережі DarkNet із використанням в якості платіжного засобу криптовалюти на сьогоднішній день становить реальну загрозу світовій спільноті, що зумовлено відсутністю емісійного центру, анонімністю технологій блокчейн. Переконливою

вбачається аргументація цих авторів щодо необхідності удосконалення законодавства в сфері протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом та фінансуванню тероризму, в напрямі врахування використання цифрових валют для здійснення злочинів, необхідності розробки нових методів та заходів для відстеження, аналізу використання терористами DarkNet. При цьому, частина заходів повинна бути пов'язана із пошуком програмного забезпечення, яке дозволить покращити каталогізацію глибоких веб-сайтів [3, с. 241].

Слушно вказує Д. Гресь, що з урахуванням поточної ситуації в нашій країні, використання криптовалюти задля фінансування незаконних збройних формувань стає загрозою для національної безпеки, а протидія фінансуванню тероризму з використанням криптовалюти повинна бути одним із пріоритетних напрямків діяльності держави та правоохоронних органів [4, с. 60].

За даними Служби безпеки України, саме переказ криптовалют на електронні гаманці невідомих фізичних осіб є одним із відомих каналів фінансування тероризму. Для того, щоб створити електронний гаманець для купівлі криптовалюти, наприклад, "Monero" (яка вважається однією із найбільш анонімних), потрібно лише скачати програму на комп'ютер або смартфон. Під час реєстрації не потрібно вводити своє справжнє ім'я, номер телефону або адресу електронної пошти. Надіслати будь-яку грошову суму іншому користувачеві можливо за лічені секунди. Для цього потрібно лише знати його "адресу" – багатозначний код, який програма створює автоматично для кожного користувача індивідуально. Час від часу вітчизняна спецслужба затримує власників криптообмінників, оскільки останні, зазвичай, беруть участь у схемах часткового фінансування тероризму на користь рф. Наприклад, свого часу правоохоронці звинуватили в незаконній діяльності власників обмінних пунктів, наприклад, "casherbox.com" та "minertech.org", які займалися конвертацією електронних валют в інтересах терористичної організації "ДНР". Фінансування тероризму за допомогою криптовалюти може мати величезний обсяг та забезпечувати анонімність відправників цих коштів.

У квітні 2023 року Служба безпеки України розкрила шахрайську фінансову піраміду "Life is good", якою керували представники рф. Згідно із даними СБ України, спочатку проект працював виключно на території рф, втім після 2017 року організатори націлилися на український ринок. За весь час існування шахрайського проекту зловмисники увели в оману майже тисячу жертв на загальну суму $40 млн. США. Представники "Life is good" обіцяли користувачам прибуток від інвестицій у перспективні підприємства світового рівня. Залучені кошти шахраї акумулювали на банківських рахунках та криптогаманцях. Організатори піраміди налагодили схему із залучення віртуальних активів через мережу обмінників в Україні. За даними слідства, до організації цієї оборудки причетні 10 громадян держави-агресора [18]. Виходячи із викладеного, заслуговує на увагу позиція А. Демчук, яка вважає, що важливим напрямом у сфері протидії та розслідуванні кримінальних правопорушень, вчинених із використанням криптовалюти, є заходи з підвищення ефективності міжнародного співробітництва у сфері боротьби з кіберзлочинністю, особливо зважаючи на те, що злочинність через використання такого інструменту, як криптовалюта набуває транснаціонального характеру. Тому заходи протидії потребують постійного удосконалення, а боротьба лише на національному рівні в рамках окремої країни не буде максимально ефективною [7, с. 75].

Висновки.

Проведений аналіз свідчить про наявність загрозливих тенденцій використання криптовалют для фінансування тероризму в умовах війни. По-перше, криптовалюта відіграє безпрецедентну роль у війні через пожертвування – як на підтримку України, так і на

підтримку рф. По-друге, рф та Іран можуть використовувати криптовалюту для ухилення від міжнародних санкцій. По-третє, криптовалюта все частіше виступає інновацією економіки тероризму у світових масштабах. Це означає, що інновація криптовалюти може повністю вийти за межі усталених економічних відносин. У зв`язку з цим можна констатувати, що економіка тероризму незалежна від легальних економічних структур в рамках процесів виробництва та споживання товарів та послуг.

Росія залишається активним спонсором тероризму. Важливою подією 2023 року стало призупинення її членства у FATF, а подальшим перспективним кроком вбачається повне виключення рф з цієї міжнародної інституції, внесення держави-агресора до т.зв. "чорного списку", що має значно послабити російську економіку під потужним санкційним тиском. Актуальною проблемою залишається використання світових криптобірж спецслужбами та військово-політичним керівництвом рф для фінансування тероризму та відмиванню "брудних" коштів.

На фоні прозорості та відкритості операцій із криптовалютами, на жаль, вони все ще можуть потенційно використовуватися російською військовою машиною в обхід санкцій для легалізації доходів, здобутих злочинним шляхом, фінансування протизаконної діяльності, особливо терористичної. Також злочинці постійно шукають нові схеми використання криптовалют з метою фінансування тероризму, виходячи із того, що криптовалютні біржі не так суворо регулюються законом, а також використовують у своїх інтересах ситуації, коли смарт-контракти на біржі не регулюються жодним законодавством.

Запобігти цьому негативному явищу можливо шляхом посилення санкційного тиску на державу-агресора. Цьому також сприятиме прийнятий Верховною Радою України Закон України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом" від 21.03.23 р. № 2997 [19]. Цей Закон дає змогу імплементувати в національне законодавство України положення Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, посилити спроможності загальнодержавної системи боротьби з тероризмом з урахуванням європейських та загальносвітових практик у сфері протидії терористичній діяльності. Це, у свою чергу, сприятиме удосконаленню механізмів запобігання, виявлення, протидії терористичній діяльності, посиленню міжнародного співробітництва з питань протидії тероризму.

Адекватною мірою протидії фінансуванню тероризму з використанням криптовалют має стати: розробка та запровадження дієвого механізму блокування та недопущення фінансування терористичної діяльності російськими військовими, який унеможливлить вірогідний обхід санкцій; міжнародно-правове регулювання вимог щодо ліцензування операцій на світових криптовалютних біржах; посилення покарання за фінансування тероризму.

Використана література

1. Про віртуальні активи: Закон України від 17.02.22 р. № 2074. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text

2. Виступ Президента зі щорічним Посланням до Верховної Ради про внутрішнє і зовнішнє становище України 28 грудня 2022 року. URL: https://www.president.gov.ua/news/ vistup-prezidenta-zi-shorichnim-poslannyam-do-verhovnoyi-rad-80113

3. Грабчук О.В., Супрунова І.В. Фінансування тероризму: нові виклики та загрози державній безпеці, напрями удосконалення державного управління. *Вчені записки Університету "КРОК".* 2020. № 3 (59). С. 236-242.

4. Гресь Д.О. Щодо використання криптовалюти у фінансуванні тероризму: materiały z Międzynarodowej konferencji naukowo-praktycznej *Integracja szkolnictwa wyższego prawniczego Ukrainy z europejską przestrzenią edukacyjną – wyzwania bezpieczeństwa wewnętrznego w czasie stanu wojennego,* Łomża, Kharków, 15.02.2023 r. Łomża: MANS w Łomży, 2023. P. 58-61.

5. Гринчук Т.П., Гусак Л.П. Використання криптовалют у злочинних цілях та пріоритетні напрями її правового регулювання. *Фінансовий простір.* 2022. № 2 (46). С. 6-14.

6. Данко Н.С. Перспективи оподаткування криптовалюти в Україні кріз призму міжнародного досвіду. *Інтернаука.* – (Міжнародний науковий журнал). 2018. № 9. (49). С. 27-30.

7. Демчук А.І. Щодо деяких аспектів використання криптовалюти у легалізації (відмиванні) доходів, одержаних злочинним шляхом та фінансуванні тероризму. *Журнал східноєвропейського права.* 2020. № 72. С. 71-78.

8. Казначеєва Д.В., Дорош А.О. Кримінальні правопорушення у сфері обігу криптовалюти. *Вісник кримінологічної асоціації України.* 2021. № 2 (25). С. 149-157.

9. Калайда Ю.П. Можливості блокчейн-технологій у розслідуванні кримінальних правопорушень, вчинених у кіберпросторі. *Інформація і право.* № 4(39)/2021. С. 170-178.

10. Кобильник Д.А., Бурчак А.Ю. Криптовалюта як об'єкт податкового права: практичне застосування та правове регулювання. *Право та інновації.* 2020. № 2 (30). С. 24-30.

11. Крит'єв А.Г. Використання криптовалют для відмивання коштів та фінансування тероризму: зб. матеріалів ІІ Міжнар. наук.-практ. Інтернет-конф. *Майбутнє банкінгу: сучасні виклики та перспективи розвитку*, м. Київ, 15 черв. 2017 р. – (МЩН України, ДВНЗ "Київ. нац. екон. ун-т ім. Вадима Гетьмана"). Київ: КНЕУ, 2017. С. 105-106.

12. Спільник І., Ярощук О. Інституалізація криптовалюти: регулювання, правовий статус, облік і оподаткування. *Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації.* 2020. Вип. 2. С. 81-92.

13. Чаплинська О.В. Оподаткування криптовалюти в Україні: реалії та перспективи. *Порівняльно-аналітичне право*. 2019. № 1. С. 252-254.

14. Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT). URL: https://www.imf.org/external/np/leg/amlcft/eng

15. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. URL: https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

16. Як криптовалюта допомагає фінансувати терроризм та як цього уникнути. URL: https://speka.media/yak-kriptovalyuta-dopomagaje-finansuvati-terorizm-ta-yak-cyogo-uniknuti-p1dg5p

17. New EU measures against money laundering and terrorist financing. URL: https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing

18. СБУ викрила в Україні російську фінансову піраміду на майже 40 млн. доларів. URL: https://ssu.gov.ua/novyny/sbu-vykryla-v-ukraini-rosiisku-finansovu-piramidu-na-maizhe-40-mln-dolariv

19. Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом: Закон України від 21.03.23 р. № 2997. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40699

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~