УДК 342.951

ЛУК'ЯНЧУК Р.В., *кандидат наук з державного управління.*
ORCID https:// orcid.org/ 0000-0003-1080-2878.

ПРОТИДІЯ ФІНАНСУВАННЮ ТЕРОРИЗМУ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТ

DOI...

Анотація. *Визначено роль та значення феномену криптовалют. Окреслено напрями злочинного використання криптовалют. Розкрито алгоритми використання російськими злочинцями криптовалют та нелегальних крипторинків. Розкрито передумови та особливості використання криптовалютних міксерів та тумблерів з метою приховування злочинних криптовалютних операцій. Охарактеризовано децентралізований сервіс "Tornado Cash" та напрями його злочинного використання. Визначено сучасні шляхи обходу санкцій та уникнення санкційного тиску під час придбання криптовалют російськими військовими злочинцями та хакерами. Деталізовано особливості функціонування централізованих та децентралізованих криптовалютних бірж у контексті наявних та вірогідних обмежень здійснення росіянами транскордонних платежів у криптовалютах та p2p-переказів. Розглянуто положення закону ЄС про AML з метою запровадження обмежень щодо здійснення анонімних криптовалютних операцій. Висвітлено позитивний досвід Ізраїлю щодо боротьби з фінансуванням тероризму за допомогою криптовалют. Визначено подальші шляхи удосконалення механізмів щодо запобігання використанню криптовалют з метою підтримки військових злочинців та фінансування тероризму, у тому числі й у рамках нормативного врегулювання.*

Ключові слова: *віртуальні активи, криптовалюта, злочинність, фінансування тероризму, держава-агресор, міжнародні терористичні угрупування, хакери, криптобіржі, пожертвування, KYC, санкційний тиск.*

Summary. *The role and significance of the cryptocurrency phenomenon is defined. The directions of criminal use of cryptocurrencies are outlined. Algorithms for the use of cryptocurrencies and illegal crypto markets by Russian criminals have been revealed. The prerequisites and features of the use of cryptocurrency mixers and tumblers for the purpose of concealing criminal cryptocurrency operations are disclosed. The decentralized service "Tornado Cash" and the directions of its criminal use are characterized. Modern ways of circumventing sanctions and avoiding sanctions pressure during the purchase of cryptocurrencies by Russian war criminals and hackers have been identified. The features of the functioning of centralized and decentralized cryptocurrency exchanges in the context of existing and probable restrictions on cross-border cryptocurrency payments and p2p transfers by Russians are detailed. The basic provisions of the EU law on AML were considered in order to introduce restrictions on the implementation of anonymous cryptocurrency transactions. The positive experience of Israel in combating the financing of terrorism with the help of cryptocurrencies is highlighted. The further directions of improvement of the mechanisms to prevent the use of cryptocurrencies for the purpose of supporting war criminals and financing terrorism have been identified, including within the framework of regulatory settlement.*

Keywords: *virtual assets, cryptocurrency, crime, terrorist financing, aggressor state, international terrorist groups, hackers, crypto exchanges, donations, KYC, sanctions pressure.*

Постановка проблеми. Одним із факторів, які значно впливають на традиційну фінансову систему, стало глобальне поширення феномену криптовалют. З кожним роком обсяг угод та сервісів, які здійснюються з використанням криптовалют, значно та динамічно зростає. Віртуальні активи та криптовалюти викликають значний інтерес у

країнах світу завдяки своїм унікальним властивостям. Це призводить до того, що в сучасних умовах потреба законодавчого врегулювання криптовалют постає актуальним питанням, яке має темпорально вирішуватися як на рівні кожної держави окремо, так і на міжнародному рівні. Ринок платіжних послуг швидко розвивається в умовах цифровізації економіки, у зв'язку з чим розробляються нові інструменти, способи та рішення проведення розрахунків. Загально відомо, що

Віртуальні валюти відносяться до переліку ризикованих активів, у зв'язку із відсутністю належної законодавчої бази та офіційних обмінних процедур. Серед інших негативних факторів ризику виділяють: 1) неможливість анулювання трансакцій та повернення фінансових ресурсів у випадку шахрайства; 2) відсутність гарантій виконання біржових смарт-контрактів; 3) уразливість щодо взлому складових платіжних систем, у тому числі й клієнтських програм, що встановлені на комп'ютерах кінцевих користувачів. Курси криптовалют визначаються виключно балансом між попитом та пропозицією, чим обумовлено високу їхню волатильність.

Вказані загрозливі фактори та ризикований характер абсолютно жодним чином не впливають на зменшення попиту на криптовалюти, а навпаки, засвідчують постійне динамічне збільшення кількості бажаючих придбати віртуальні активи, що є більш аніж переконливим засвідченням розвитку та масштабування світової криптоіндустрії.

В умовах активної глобальної цифровізації та зростання попиту на криптовалюти кримінальні ризики поступово переходять у нову площину. З появою нових фінансових інструментів у легальному обігу на випадок можливості їхнього конфіденційного використання, вони відразу потрапляють до сектору тіньової економіки. Це відбувається також і відносно криптовалют, які з кожним роком набувають все більшої популярності як засіб скоєння злочину або у вигляді предмету, відносно якого він здійснюється. Криптографічні трансакції не вимагають від зловмисників та терористів використання реальних імен, персоналізованого банківського рахунку, будь-якої ідентифікації, що сприятиме уникненню ними кримінального переслідування з боку правоохоронних органів. 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 не можливо уявити без залучення та використання можливостей віртуальних валют та зокрема криптовалют.

Міжнародні терористичні угрупування та російські військові терористи не залишаються осторонь ци процесів, зберігаючи значний фінансовий вплив та потенціал, вони все частіше шукають нові джерела фінансування своєї злочинної діяльності, враховуючи високі темпи глобальної технологічної інформатизації. Це пов'язано з тим, що система блокчейн являє собою певну "чорну скриню", яка приховує більшу частину операцій від державних та правоохоронних органів, які ведуть боротьбу з тероризмом та відмиванням "брудних" коштів.

Таким чином, системна боротьба щодо використання криптовалют у злочинних цілях стає все складнішою, що потребує розробки та впровадження нової моделі захисту глобального криптовалютного ринку від протиправних операцій, пов`язаних із легалізацією доходів, здобутих злочинним шляхом та фінансування тероризму тощо. Пошук оптимальних шляхів удосконалення організаційно-правових засад обігу криптовалют та недопущення масштабів їхнього злочинного використання, у першу чергу, державою-агресором, є доцільним та своєчасним, як з позиції наукового підходу, так і практичної складової.

Результати аналізу наукових публікацій. Кримінальні правопорушення у сфері обігу криптовалют та можливості блокчейн-технологій у розслідуванні злочинів, вчинених у кіберпросторі певним чином вивчали: Д. Казначеєва, А. Дорош [5], Ю. Калайда [6] та інші фахівці. Деякі аспекти використання криптовалют з метою фінансування тероризму висвітлювали у своїх наукових працях: О. Грабчук та І. Супрунова [1], Д. Гресь [2], Т. Гринчук та Л. Гусак [3], А. Демчук [4], А. Крит'єв [7].

У зарубіжній науковій літературі проблематику використання криптовалют з метою фінансування злочинної діяльності, зокрема тероризму, досліджували: А. Трозі [8], Ф. Теіхман і М. Фолкер [9], А. Нахіда [10].

Проте жоден із вказаних авторів предметно не досліджував проблематику використання криптовалют у злочинних цілях та з метою фінансування тероризму, особливо в умовах агресивної війни рф проти України, що засвідчує актуальність обраного наукового дослідження.

Метою статті є визначення перспективних шляхів удосконалення організаційно-правових засад обігу криптовалют і недопущення масштабування їхнього злочинного використання, у першу чергу державою-агресором.

Виклад основного матеріалу. Криптовалюти та механізми їхнього функціонування з використанням інструментарію розподілу реєстрів є "трампліном" для майбутнього розвитку та удосконалення платіжних систем. З іншого боку – в руках злочинців та терористів криптовалюти стають новим, зручним у застосуванні інструментом для безпечного переміщення та зберігання коштів, які потім вірогідно можуть використовуватися з метою фінансування тероризму. Шалена популярність криптовалют у злочинному середовищі визначено тим, що в сучасних умовах чітко не окреслено юридичні параметри обігу криптовалюти, не встановлено межі їх використання.

Існують такі криміногенні властивості, притаманні технічним характеристикам децентралізованих криптовалют, зокрема: високий ступінь анонімності власників криптовалют та здійснених ними трансакцій; низькі комісійні або повна їхня відсутність; можливість здійснення миттєвих транснаціональних грошових переказів; відсутність будь-яких обмежень щодо сум таких переказів; транснаціональний характер криптовалют (неможливість встановлення державних та митних кордонів при проведенні трансакцій); незворотність таких трансакцій; відсутність єдиної керівної особи, яка може виступати у якості "центральної точки контролю" у процесі випуску та обігу криптовалют та яка може поінформувати уповноважені державні або правоохоронні органи про факти скоєння підозрілих операцій тощо. Саме тому криптовалюти досить активно використовуються злочинцями у якості специфічного еквіваленту грошових засобів під час торгівлі наркотичними засобами, психотропними речовинами, порнографічними матеріалами, іншими забороненими товарами та послугами, а також під час фінансування тероризму, з метою ухилення від сплати податків тощо.

Свого часу у глобальних вимірах допомагали злочинному використанню криптовалют нелегальні крипторинки, таких як: "Silk Road", "Silk Road 2.0", "Evolution", "Hydra". Так, на анонімній торгівельній Інтернет-платформі "Silk Road", яка функціонувала у період з 2011 по 2013 роки на базі комп'ютерної мережі "Tor", за допомогою криптовалюти біткоїн, реалізовувалося понад 10 тис. заборонених товарів та послуг, а її загальний річний обіг складав понад $17 млн. США. Закриття цього сайту за результатами успішної операції ФБР США лише на певний час пригальмувало розвиток нового сегменту кримінального бізнесу, оскільки незабаром з'явилися нові Інтернет-платформи "Road 2.0" та "Evolution", які за короткий період часу збільшили свої

прибутки у десятки разів. У 2014 році внаслідок проведення спецоперації під назвою “Onymous” були заблоковані, а згодом закриті потужні Інтернет-платформи, які використовувалися з кримінальною метою, у тому числі й “Silk Road 2.0” та “Hydra”. Була припинена діяльність 619 нелегальних доменів, загальна вартість яких складала 1,18 млн. Євро.

Наймасштабнішою міжнародною операцією по боротьбі з використанням криптовалют у сфері кримінальної діяльності беззаперечно є успішно завершена у липні 2015 року операція під назвою “Shrouded Horizon”, яка об’єднала 20 держав світу та призвела до арешту майже 300 виявлених кіберзлочинців. За результатами цієї операції було ліквідовано хакерський форум “Darkode”, через який укладалися багаточисельні угоди, пов’язані з купівлею-продажем та обміном шкідливим програмним забезпеченням, викраденими персональними данними, інформацією зі взломаних серверів та іншим програмним забезпеченням для кіберзлочинів. Окрім торгівлі забороненими товарами, контентом та послугами, одним з найбільш затребуваних сегментів кримінального використання криптовалют є відмивання доходів, здобутих злочинним шляхом та фінансування тероризму. Можна констатувати, що незаконний обіг грошових коштів (відмивання, вивід за кордон, переведення у готівку тощо) активно здійснюються через механізми конвертації фіантних коштів у віртуальні валюти, у тому числі й у криптовалюти, обіг яких позбавлений фінансового контролю як з боку кредитних організацій так і уповноважених державних органів.

Виходячи із кращих практик міжнародного досвіду, для України, в сучасних умовах правового режиму воєнного стану, важливим напрямком залишається удосконалення нормативно-правового та організаційно-технічного забезпечення функціонування вітчизняного криптовалютного ринку, створення дієвих важелів та передумов задля його зростання, динамічного перспективного розвитку.

Проте, на фоні отриманих позитивних здобутків та поступальних кроків нашої держави у напрямку розбудови та подальшого розвитку вітчизняної та світової криптоіндустрії, існують наявні проблемні питання, які виникають паралельно із динамічним розвитком криптосектору та мають поширювану загрозливу тенденцію, особливо щодо злочинного використання криптовалют з метою фінансування тероризму. Все ще, на жаль, у світі не існує єдиних вироблених та встановлених міжнародних стандартів щодо уніфікованого унормування здійснення регулювання глобального обігу криптовалют, чим і користуються злочинці та терористи. Також все ще відсутні на глобальному рівні ефективних механізмів пошуку та ідентифікації осіб, причетних до злочинної діяльності з використанням криптовалюти. На цьому фоні міжнародні експерти неодноразово фіксували факти використання децентралізованих криптовалют у злочинних цілях, серед яких набули популярності “Bitcoin”, “Ethereum”, “Monero”.

Якщо раніше організовані злочинні угруповання та військові злочинці рф намагалися уникати відкритого можливого використання цифрових валют, то назараз у відкритій формі агітують “донорів” застосовувати, наприклад, “Bitcoin” у якості анонімного та безпечного платежу. Поступово “Bitcoin” втрачає свої позиції та замість нього терористи активно використовують інші блокчейни, зокрема “Ethereum”, “Monero”, “TRON”. Особливо користується попитом серед злочинців блокчейн “TRON” – децентралізована платформа метою якої є пряма взаємодія розробників контенту зі своєю аудиторією без посередників.

Основною віртуальною валютою “TRON” є “TRX”, яка використовується для оплати праці розробників вказаної платформи, враховуючи її стабільність та низький коєфіцієнт комісії за проведені трансакції. Також ця криптовалюта активно

використовується з метою отримання пожертвувань для фінансування російської військової агресії та терористичної діяльності. Проте у найближчій перспективі вказані пріоритети та тенденції перестануть бути такими.

Основні інституціональні компанії, які не мають реального відношення до криптовалюти, однак активно її скуповують у якості інвестицій, пропонуючи кастодіальні послуги або приймають криптовалютні компанії у якості банківських клієнтів. Таким чином, фінансові установи зобов'язані забезпечувати відповідні вимоги більш ретельно, аніж це роблять навіть самі криптовалютні компанії. В умовах використання розподілених реєстрів, де кожна трансакція записується у публічну "бухгалтерську книгу", фінансова установа, по суті, може проаналізувати цю інформацію аби бути впевненою, що вони мають справу з максимально безпечними установами. Посилення контролю за дотриманням вимог з боку криптовалютних бірж має призвести до значного зниження рівня криптозлочинності, у тому числі й в силу того, що правоохоронні органи зможуть, на упередження, призупинити діяльність підозрілих суб'єктів.

Цілком можливо припустити, що світові криптобіржі у подальшому будуть більш ретельно та відповідально ставитися до наданих ними сервісів, оскільки дотримання вимог, заснованих на оцінці операційних ризиків вже стає нормою. Традиційно більшість криптобірж полагалися на публічно заявлену та розроблену політику стандарту KYC (Know Your Customer – "знай свого клієнта") та AML CFT CWMDF (Antimoney laundering and counter-terrorist financing and counter-weapons of mass destruction financing) – протидія відмиванню "брудних" коштів, здобутих злочинним шляхом, протидія фінансуванню тероризму, інших криптовалютних сервісів. Адже злочинці навчилися обходити встановлену процедуру KYC. Для цього вони використовують більш конфіденційну валюту, яка не вимагає авторизації, або під час процедури KYC надають фальсифіковані дані, які знаходять у мережі Інтернет. Одним із сучасних та простих способів розміщення коштів у криптовалюті є багаточисельні незначні нарахування на різні рахунки, тобто користувач створює декілька активних аккаунтів та нараховує на них максимально допустиму суму за якої відсутня вимога проведення ідентифікації.

У системі блокчейну існує також власна криптогральна індустрія, в якій зловмисники переводять криптовалюту на гральну платформу, роблять незначні ставки та потім швидко зворотньо виводять гроші. Цей спосіб надає змогу замаскувати схему відмивання коштів та фінансування тероризму. Більш того, існує можливість виконання трансакцій через мережу TOR, які неможливо відслідкувати, у зв'язку з тим, що досить складно визначити реальну IP-адресу. Оскільки будь-які протизаконні операції у валютно-фінансовій сфері негативно впливають на економічну безпеку будь-яких держав, то виникає нагальна потреба створення та оновленої методики та напрацювань щодо запобігання відмиванню коштів та фінансуванню тероризму з використанням криптовалют.

Також з метою уникнення ідентифікації спеціальними службами, злочинці використовують такі сервери, як тумблери та міксери, які змішують у випадковому порядку операції з криптовалютою, що у свою чергу, значно знижує можливості розкриття скоєних кримінальних правопорушень. Існує чимало міксерів, які використовуються для здійснення анонімних переказів криптовалют. Проте більша частина з них є централізованими сервісами, які можуть зловживати довірою користувачів, викрадати їхні заощадження або особисті дані. Засновники криптовалютних міксерів неодноразово анонсували, що вони відіграють важливу родь з метою захисту користувачів та інвесторів. Проте правоохоронні органи повідомляють, що такі сервіси часто використовуються для відмивання коштів, здобутих злочинним шляхом або з метою фінансування тероризму. Так, у січні 2022 року з сінгапурського сервісу Crypto.com було викрадено 4600 ETH, вартістю $15 млн. США, а

потім “прокручені” через міксер “Tornado Cash”. У червні 2022 року було зламано кросчейн Horizom з екосистеми Harmony. Зловмисники викрали активи на загальну суму $100 млн. США, більш частина яких надійшла на сервіс “Tornado Cash”. На відміну від них сервіс “Tornado Cash” побудований на принципі децентралізації, тобто являв собою набір смарт-контрактів з якими користувачі взаємодіяли завдяки web-3 гаманцям. Контракти приймали депозити та змішували їх в одному пулі, для чого застосовувалася технологія zk-SNARK (Zero-Knowledge Succinct Non-Interactive). Тобто транскації відбувалися без розкриття інформації про платежі, а усі активи були анонімізовані та не пов’язані з певною особою.

Децентралізований сервіс “Tornado Cash” був запущений у серпні 2019 року на базі блокчейну Ethereum, який надає змогу анонімізувати трансакції. На першому етапі розробники зберегли контроль за протоколом через гаманець з мультипідписом. Але у травні 2020 року після запуску другої версії протоколу з метою підвищення рівня децентралізації були знищені ключі доступу до смарт-контрактів. Протягом 2021 року смарт-контракти “Tornado Cash” були розгорнуті в інших популярних блокчейнах: BNB Chain, Polygon, Avalanche, Gnosis тощо. За даними американських аналітичних досліджень протокол “Tornado Cash” є найбільш популярним способом незаконного відмивання криптовалют, пов`язаних з кіберзлочинністю, у зв’язку з чим в серпні 2022 року криптовалютний міксер “Tornado Cash” потрапив під санкції США, а у Нідерландах 12 серпня 2022 року заарештували засновника та розробника цього сервісу росіянина Олексія Перцева. Одночасно було заблоковано $436 млн. США з репозиторію “Tornado Cash”. За усю свою історію протокол “Tornado Cash” обробив понад $3,5 млрд. США та зібрав понад 17,7 млн. комісій. При цьому, 1,2 млрд. напряму пов’язані з крадіжками, взломами та іншими незаконними операціями, а послугами сервісу “Tornado Cash” скористалися понад 57 тис. унікальних користувачів. Досить активно цей міксер використовували хакери північнокорейського угрупування “Lazarus”.

В умовах військової збройної агресії рф проти України, фактичної війни, потужного санкційного тиску на державу-агресора, на жаль, саме криптовалюти можуть допомогти рф вести торгівлю в обхід міжнародних та європейських санкцій через обмежений ринок та відсутності на криптобіржах дієвих механізмів щодо відстеження платежів російських військових злочинців та зловмисних операцій. Російські окупаційні війська, навіть попри санкції, отримують мільйони доларів у вигляді донатів та пожертв у криптовалютах. Криптовалюти залишаються єдиним каналом пожертв для прихильників рф з-за кордону.

З травня 2022 року проросійські активісти поступово нарощували обсяги залучення криптовалютних інвестицій Через п’ять місяців після вторгнення рф в Україну було виявлено 54 волонтерські групи які займалися краудфінансуванням російських військових закупівель, поширенням дезінформації та пропагандою на підтримку війни. Ці організації отримали майже $2,2 млн. США у вигляді пожертв. Станом на 24 лютого 2023 року кількість таких проросійських структур збільшилося до 100, а розмір сум донатів – до $5,4 млн., а ще $0,7 млн. США залучили за рахунок пожертв з боку волонтерських організацій Білорусі. На цьому фоні 10 % проросійських пожертв надходять саме з незаконних джерел, включаючи Даркнет-ринки та продавців викрадених кредитних карт. У 2022 році активними та відомими отримувачами закордонних криптодонатів виступили “Координаційний центр допомоги Новоросії”, який зібрав у криптовалюті понад $40 тис. США, і спрямовував їх на закупівлю зброї, безпілотників, оптичних приладів, транспортних засобів. У переліку отримувачів є також російська кіноактриса Анастасія Михайловська, яка отримала на свій гаманець

понад $34 тис. США на фінансування російської армії та пов'язаного з ПВК "Вагнер" воєнізованого угрупування "Русич", яке залучило понад 2,7 BTC, 30 ETH та $88 тис. США у різних стейблкоїнах (у сукупності понад $212 тис. США) тощо. Репортер державного телебачення та пропагандист рф Євген Піддубний зібрав понад $215 тис. США у криптовалюті, а Організація сприяння збереженню вітчизняних традицій та культурної спадщини "Віче" – приблизно $82 тис. США. Вказані віртуальні валюти спрямовувалися на покриття військових потреб рф, а саме: придбання безпілотників, амуніції, форменого одягу, зброї та боєприпасів, транспорту.

З метою обходу блокувань на ліцензованих криптобіржах терористи рф розпочали скуповувати сторонні облікові дані та акаунти для прихованої роботи та злочинної діяльності на криптовалютних біржах. Таким чином, зросла кількість нових оголошень щодо купівлі номінальних акаунтів для роботи на криптовалютних біржах. У середньому ціна логіну та паролю від акаунта складає $50 США. За облікові дані з QR-кодом для здійснення двуфакторної аутентіфикації, повним пакетом документів, на який зареєстрований акаунт, електронною поштою та файлами-cookie покупець має заплатити до $300 США. Ціна напряму залежить від країни реєстрації, дати реєстрації та історії активності. Як правило, стартовий пакет містить дані для входу в акаунт, резервні засоби отримання доступу, реквізити онлайн телефонії для отримання верифікації за допомогою СМС, паспорт номіналу. Активними покупцями таких послуг є представники російського кримінального сегменту та росіяни із заблокованими біржовими акаунтами. Сам факт придбання чужого акаунта не формує складу кримінального правопорушення, оскільки він не є майном на відміну від криптовалют. Проте нарівні з цим механізм продажу номінальних акаунтів має низку ризиків. У цьому сегменті чимало шахраїв, які потенційно можуть звернутися на біржу із заявою про викрадення даних з облікованих записів. Також, на переконання експертів, у даркнеті зросла кількість пропозицій з дублювання документів для проходження KYC-процедури у фінансових організаціях. Після введення центробанком рф заборони на валютні операції у березні 2022 року, різко зросла кількість підпільних обмінників, які пропонували росіянам купівлю продаж доларів та євро через криптовалюти.

Моніторинг трансакцій залишається одним із найскладніших завдань у сучасній криптоіндустрії, оскільки кластери операцій стають доступними тільки через деякий час. У звязку з цим проведені операції можливо досліджувати лише постфактум. Крім того, криптовалютну трансакцію неможливо заблокувати просто так. Необхідно бути впевненим у правомірності дій клієнта, що він діє у відповідності з правилами використання платформи. На жаль, санкції не розвалили російський крипторинок, проте на фоні санкційного тиску рф намагається розвивати транскордонні платежі у криптовалютах та p2p-перекази (прямі перекази між користувачами без участі посередників). В цьому контексті санкції поділили світові криптобіржі для росіян на дві групи. Перша група – криптобіржі, які мають обов'язкові процедури щодо протидії відмиванню "брудних" коштів та фінансуванню тероризму, відмовляються співпрацювати з сумнівними альткоїнами та дотримуються усіх санкційних обмежень. Такий стан справ значно ускладнює росіянам можливості користування такими криптобіржами. Другий тип криптобірж робить ставку на лояльність та низький рівень протидії відмиванню коштів та фінансуванню терористичної діяльності, у зв'язку з чим включають у свій лістинг підозрілі альткоїни та працюють за рахунок великих обертів та загальної доступності. Цей тип криптобірж активно використовується для придбання, переважно за рахунок криптовалюти та стейблкоїнів, товарів та послуг переважно з КНР та країн Південно-Східної Азії, Ірану, у тому числі й військового призначення. Криптовалютний тренд

сучасності, яким можуть скористатися російські військові злочинці – розвиток направлення (Play-to-Earn – "грай, щоб заробити"), які за рахунок впровадження в існуючі топові ігри дозволяють геймерам заробляти. Також ці вірогідно криптобіржі використовуються для здійснення міжнародних розрахунків з метою обходу санкцій.

Ще існує інший дієвий спосіб уникнення санкцій за допомогою саме криптовалют. Наприклад, дубайська криптоплатформа "Coinsfera" набирає популярності серед росіян, оскільки ця площадка надає змогу укладати угоди непомітно від крипторинків. Слід вказати, що "Coinsfera" не класична криптобіржа, а являє собою OTC-платформу, яка надає послуги позабіржової торгівлі, тобто продавці та покупці можуть укладати угоди купівлі/продажу криптовалют напряму за готівкові кошти. Головна перевага таких трансакцій полягає у тому, що вони не фіксуються у книзі ордерів та не відображаються публічно, що у свою чергу, забезпечує учасникам угоди повну конфіденційність. Криптообмінник "Coinsfera" було запущено ще у 2015 році, а його офіси відкриті у Дубаях, Стамбулі, Лондоні та Косово. Увагу підсанкційних осіб вона привабила ще до повномасштабного вторгнення рф в Україну, оскільки він працює без будь яких торгівельних обмежень. У свою чергу, Інтернет-Даркнет-платформа "Hydra Market" та криптовалютна біржа "Garantex Europe OU", зареєстрована в Естонії, за версією Мінфіна США, працювали переважно з росіянами, сприяючи їм у проведенні біржових трансакцій.

На фоні санкційного тиску щодо рф, збільшився попит на апаратні криптогаманці. Інтерес росіян до апаратних гаманців збільшився на 89 % тільки у період з 11 до 16 квітня 2023 року. Окрім того, попит на апаратні криптогаманці зростає у зв'язку з обмеженнями, запровадженими ліцензованими криптобіржами відносно росіян, які запровадили ліміти на зберігання коштів на рахунках, а також заборонили придбання валюти через систему p2p. Також попит на "холодні" криптогаманці формується за рахунок запровадження у державі-агресорі обмежень на придбання та обіг іноземної валюти: центробанк рф заборонив росіянам знімати з рахунків понад $10 тис. США, що стало поштовхом для активізації використання апаратних гаманців, які зберігають анонімність користувача та надають змогу уникнути обмеження та замороження коштів, оскільки будь який інший сценарій загрожує блокуванням фінансів. Причиною зростання попиту на апаратні криптогаманці є той факт, що з ними можна працювати без мережі Інтернет, що додатково захищає користувачів від несанкціонованого витоку даних.

У жовтні 2022 року Євросоюз запровадив заборону на обслуговування криптовалютних гаманців росіян у рамках санкційного тиску. Після цього, чимало криптобірж розпочали вводити заборони для росіян. Так, криптобіржа "Binance" запровадила валютні обмеження для росіян, заборонивши їм купувати долари та євро. Також ця платформа ввела обмеження на зберігання криптовалюти – до €10 тис., хоча згодом зняла ці ліміти. У березні 2023 року аналітики компанії "HAPI Labs" повідомили, що майже 96 % донатів на російську армію пройшли саме через криптобіржу "Binance", що є переконливим свідченням недотримання цією торгівельною платформою AML процедур. Окрім криптобіржі "Binance", трансакційні надходження з біржових акаунтів, які спонсорують війну здійснювали такі біржі, як: "FTX", "Kucoin", "WhiteBIT". Тільки за перші 8 місяців війни на підтримку російських військових угрупувань було зібрано понад $4 млн. США у криптовалютах.

Таким чином, санкційний тиск не можна недооцінювати, проте росіяни шукають сервіси, які допоможуть їм безпечно придбати та зберігати криптовалюту, у тому числі, й з метою фінансування тероризму. На жаль, існує низка сервісів, які за рахунок своїх технічних особливостей не можуть блокувати криптовалютні операції, незалежно від

громадянства користувачів та їхнього місцезнаходження – це децентралізовані біржі та некастодіальні гаманці. Децентралізовані біржі – це площадки для торгівлі та використання фінансових інструментів на основі технології блокчейн. На відмінну від централізованих бірж у них відсутня адміністрація, яка керує платформою та може впливати на рішення про блокування того чи іншого користувача. Також вони не вимагають проходження процедури KYC та створення гаманця, який би перебував під контролем біржі. Для підключення вимагається лише некастодіальний гаманець, який має ключі, які знаходяться тільки у власника, тобто біржа не може його заблокувати та будь-яким чином впливати на біржові операції за його участю.

Розуміючи ризики та загрози у цій площині, провідні держави світу переймаються проблематикою розробки дієвих механізмів запобігання використанню криптовалют із злочинною метою. Так, опікуючись питаннями забезпечення безпечного використання криптовалют, у ЄС підготували окремий AML-закон для криптоіндустрії [11]. Очікується, що з набуттям чинності цим нормативним актом для обігу криптовалют настають певні наслідки. По-перше, децентралізовані автономні організації, платформи "NFT" і платформи "DeFi" підпадають під дію правил AML. Згідно із вказаним законопроектом, вони будуть зобов'язані виконувати вимоги, доки "контролюються прямо чи опосередковано, у тому числі через смарт-контракти або протоколи голосування, фізичними та юридичними особами, які можна ідентифікувати". На відміну від Регламенту ЄС про ринки криптоактивів, який незабаром буде введено в дію, законопроект про боротьбу з відмиванням грошей включає децентралізовані платформи як зобов'язані суб'єкти. Метою закону ЄС про AML є усунення наявних нормативних прогалин та деяких розбіжностей. Так, нормативно передбачається, що відповідальні суб'єкти криптоіндустрії, зокрема криптобіржі, зобов'язані проводити належну перевірку всіх своїх клієнтів і повідомляти владу про підозрілі транзакції так само, як це зараз роблять, наприклад, банки, фінансові установи. Якщо закон буде прийнято, то кредитні та фінансові установи повинні застосовувати заходи належної обачності, дозволяючи криптовалютні транзакції на суму понад €1000 ($1080 США). Крім того, запроваджуються посилені заходи належної перевірки кореспондентських відносин із постачальниками крипто-послуг з-за меж ЄС і платежів із використанням гаманців, розміщених на власному хості. Ділові контакти з неліцензійними організаціями категорично забороняються. Для комерційних криптоплатежів існуватимуть обмеження на транзакції на суму понад 1 тис. Євро, що випливають із гаманців, розміщених на власному хості, якщо власника гаманця не ідентифіковано. Зокрема, правила зобов'яжуть кредитні та фінансові установи проводити процедуру "дью-діліджене" у разі проведення транзакцій на суму від €1000. Згідно з нововведенням, перекази для криптогаманців, власник яких не ідентифікований повністю, матимуть обмеження виключно у сумі €1000. Користування анонімними криптоакаунтами планують заборонити. Крім того, Європейська Комісія має оцінити необхідність перегляду положень законопроєкту через три роки, щоб AML-правила чітко відповідали правовій базі із цифрової ідентифікації. Розроблені європейською спільнотою заходи мають на меті посилити безпеку криптовалютних операцій, запобігти ризикам використання криптовалют з метою фінансування тероризму та легалізації доходів, здобутих злочинним шляхом.

Актуалізація проблематики використання криптовалют із злочинною метою також знайшла своє підтвердження у звіті Європолу щодо загроз організованої злочинності в Інтернеті (IOCTA), де зазначається, що криптовалюти, останнім часом, активно та поширено застосовуються для полегшення здійснення платежів за різноманітні форми незаконної діяльності [12].

У контексті змістовного розкриття тематики цієї наукової статті цікавим видається висвітлення позитивного досвіду Ізраїлю щодо боротьби з фінансуванням тероризму за допомогою криптовалют. За результатами спеціальної операції, проведеної Національним бюро по боротьбі з фінансуванням тероризму, Ізраіль успішно перехопив мільйони доларів США криптовалютних засобів, спрямованих на проведення терористичної діяльності. Цей успіх став результатом спільних зусиль розвідувальної служби, відповідальних урядових структур з використанням передових технологічних рішень. Було конфісковано криптовалюти, які йшли транзитом на адресу ліванського воєнізованого угрупування "Хезболла" та іранських "Сил Кудс", що спричинило потужний удар по їхнім фінансовим ресурсам. Ці терористичні угрупування використовували саме криптовалюту з метою отримання та подальшого фінансування своєї злочинної діяльності. Аналітична компанія "Chainalysis" підтвердила, що Ізраіль конфіскував майже $1,7 млн. США у криптовалюті. Компания "Chainalysis" визнала, що завдяки її напрацюванням був гарантований успіх цієї операції. З 2021 року Ізраіль здійснив конфіскацію 189 облікових записів на криптовалютній біржі "Binance", які попередньо пов'язані з терористичними організаціями ІДІЛ та ХАМАС. У квітні 2023 року Національне бюро по боротьбі з фінансуванням тероризму прозвітувало про арешт понад 500000 шекелів ($137870 США) з 80 рахунків криптобіржі "Binance", які належать трьом компаніям: "Al Mutahadun For Exchange", "Dubai Company for Exchange" и "Al Wefaq Co. For Exchange" [13]. Такі дії уряду Ізраілю були обґрунтовані тим, що криптобіржа "Binance" неодноразово приховувала інформацію від регуляторів, нехтувала процедурами погодження KYC та діяла з порушеннями рекомендацій власного відділу комплаєнсу.

Висновки.

1. Віртуальні валюти є високотехнологічним сегментом грошового обігу, який являє собою об'єктивний новий етап розвитку системи розрахунків, що має чимало ризиків та загроз для усієї національної економіки як окремо узятої держави, так і глобальному вимірі. Поступово криптовалюти піддаються жорсткому регуляторному впливу. Цілком логічно, що у 2023 році санкції та обмеження стосовно криптовалют стануть ще жорсткішими і масштабнішими, і можуть стати сильним потрясінням для глобального крипторинку. Можна виокремити такі ризики використання криптовалют з метою "прихованого" фінансування тероризму: висока волатильність віртуальних валют, простий спосіб незаконного виводу коштів за кордон, анонімність та швидкість трансакцій та операцій, відсутність контролю та нормативно-правового регулювання криптовалют на міжнародному рівні, мінімізація ризиків, пов'язаних з відмиванням злочинних доходів та фінансуванням тероризму.

2. На жаль, навіть на централізованих криптобіржах виявлені гаманці, які використовуються з метою фінансування військової агресії рф та своєчасно не блокуються біржами, навіть за запитами правоохоронних органів. Росіяни продовжують шукати лазівки з метою використання криптовалют для підтримки військових злочинців та фінансування тероризму через систему криптодонатів та пожертвування. Також попри наявні санкції та санкційний тиск, актуальними напрямками придбання криптовалют залишаються: використання криптовалютних тумблерів та міксерів, які змішують у випадковому порядку операції з криптовалютою, що у свою чергу, значно знижує можливості розкриття скоєних кримінальних правопорушень та з метою приховування своєї злочинної діяльності; придбання сторонніх, тобто "чужих" облікових записів та акаунтів для прихованої роботи та злочинної діяльності на криптовалютних біржах під "прикриттям"; масове використання росіянами апаратних

криптогаманців; сприяння придбанню криптовалют лояльними до росіян криптовалютними біржами та платформами, які ігнорують санкції та встановлені обмеження, на кшталт “Binance”, “FTX”, “Kucoin”, “WhiteBIT”, “Coinsfera” тощо.

3. Враховуючи специфіку криптовалют та наявні рекомендації профільних міжнародних організацій, можливо визначити такі заходи вирішення актуальних проблем використання криптовалют з метою фінансування тероризму.

По-перше, зокрема це створення кластерів, тобто груп адрес, які вірогідно контролюються одним і тиж самим суб’єктом та їхня подальша деанонімізація. Саме таким чином можна провести аналіз блокчейн-операцій та дізнатися важливу інформацію про геолокацію або про обмін криптовалют, який здійснювався з метою придбання монет.

По-друге, це проведення криміналістичного аналізу переферійних пристроїв злочинців, спрямований на з`ясування криптовалютних адрес, які він контролює.

По-третє, створення єдиного глобального реєстру трансакцій криптовалют.

По-четверте, це залучення експертів – свідків, які можуть перевіряти, уточнювати та підтверджувати здобуті слідчими докази.

По-п’яте, це впровадження сучасних нових технологій під час проведення фінансових розслідувань протиправного використання віртуальних активів, що включає використання інноваційних інструментів у цьому контексті.

4. Для нашої країни, в умовах набуття чинності закону України “Про віртуальні активи” доцільним є прискорення імплементації у національне законодавство кращих практик європейських нормативних вимог, які висуваються до криптоіндустрії та якими передбачені, зокрема, встановлені заборони використання анонімних криптоакаунтів та інших обмежень.

Використана література

1. 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.

2. Гресь Д.О. Щодо використання криптовалюти у фінансуванні тероризму: materiały z Międzynarodowej naukowo-praktycznej konferencji *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. Pp. 58-61.

3. 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.

4. 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.

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

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

7. Крит’єв АГ. Використання криптовалют для відмивання коштів та фінансування тероризму: зб. матеріалів II Міжнар. наук.-практ. Інтернет-конф. *Майбутнє банкінгу: сучасні виклики та перспективи розвитку*, м. Київ, 15 черв. 2017 р. – (М-во освіти і науки України, ДВНЗ “Київ. нац. екон. ун-т ім. Вадима Гетьмана” та ін.). Київ: КНЕУ, 2017. С. 105-106.

8. Arianna Trozze, Josh Kamps, Eray Arda Akartuna, Florian J Hetzel, Bennett Kleinberg, Toby Davies, Shane D Johnson. Cryptocurrencies and future fnancial crime. *Crime Science*. (2022). Vol. № 11. Pp. 1-35. URL: https://doi.org /10.1186/s40163-021-00163-8

9. Teichmann, F.M.J. and Falker, M.-C. Cryptocurrencies and financial crime: solutions from Liechtenstein. *Journal of Money Laundering Contro*l. (2021), Vol. № 24. Pp. 775-788. URL: https://doi.org/10.1108/JMLC-05-2020-0060

10. Naheeda Ali. Crimes Related to Cryptocurrency and Regulations to Combat Crypto Crimes. *Journal of Policy Research*. (2022). № 8 (Sep. 2022). Pp. 289-302. URL: https://doi.org/10.5281/ zenodo.7288155

11. У Європі підготували AML закон для криптоіндустрії. URL: https://finap.com.ua/u-yevropi-pidgotuvaly-aml-zakon-dlya-kryptoindustriyi

12. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report

13. Anti-Terrorism Law 5776-2016. URL: https://nbctf.mod.gov.il/he/Announcements/ Documents/ 9102%צת-23.pdf

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