DOI: https://doi.org/10.32844/ibpala-2025-2.06
УДК 338.24.021.8:342.951(477)

АНАЛІЗ ОСНОВНИХ КОРУПЦІЙНИХ ПРАКТИК, ЗДІЙСНЮВАНИХ ЗА ДОПОМОГОЮ ФУНКЦІОНАЛУ ДЕЯКИХ ФОРМ ЦИФРОВИХ АКТИВІВ ТА ОЦІНКА ЇХНЬОГО ВПЛИВУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Кіяшко Юрій Михайлович,
доктор філософії у галузі права, старший науковий співробітник
відділу науково-правових експертиз та законопроектних робіт
Науково-дослідного інституту публічного права
м. Київ, Україна
ORCID ID: https://orcid.org/0000-0002-3283-8743

Войтко Тетяна Миколаївна,
науковий співробітник науково-дослідного відділу впровадження
стандартів доброчесності наукового центру проблем виховання доброчесності
та запобігання корупції у секторі безпекита оборони
Національного університету оборони України
м. Київ, Україна
ORCID ID: https://orcid.org/0000-0002-4326-0633

Репрезентоване наукове дослідження присвячене актуальному питанню – аналізу основних корупційних практик здійснюваних за допомогою функціоналу деяких форм цифрових активів та оцінці їхнього впливу на національну безпеку України. Аргументовано доведено, що стрімке впровадження багатьох цифрових технологій та інновацій, окрім переваг має певні проблемні аспекти. Підкреслено, що однією з таких позицій визнається стрімке формування та утвердження нових дієвих способів і засобів отримання неправомірної вигоди. Ураховуючи характер, кількість, можливі наслідки та популяризацію цих методик наголошено на потребі оцінки потенціалу цифрових активів як прогресуючих об'єктів, що можуть підривати національну безпеку України.

Визначено проблемні позиції формування та реалізації державної політики нульової толерантності до корупції крізь призму викликів цифрового середовища. Зауважено, що за нинішніх стратегічно закладених умов складно розраховувати на провадження дієвих управлінських заходів. Ініційовано розробку нової Антикорупційної стратегії з відповідними орієнтирами та етапізацією виконання.

Розкрито питання феномену цифрових активів саме з позиції сприяння розвитку корупційних практик в Україні. Підкреслено, що виняткові їхні властивості сприяють продукуванню багатьох унікальних механізмів отримання деяких типів неправомірної вигоди. З'ясовано спільні риси таких інструментів незалежно від форми цифрового активу.

Описано та проаналізовано поширені методи і способи скоєння самих діянь, виходячи з усвідомлення переваг об'єктів цифрового виміру. Зокрема, виокремлено та диференційовано найпоширеніші практики скоєння корупційних діянь. Наголошено на результативності цих механізмів та здійснено припущення відносно зростання кількості фактів протиправності зважаючи на переваги таких умов.

Рекомендоване посилання:
Кіяшко Ю. М., Войтко Т. М. Аналіз основних корупційних практик, здійснюваних за допомогою функціоналу деяких форм цифрових активів та оцінка їхнього впливу на національну безпеку України *International Bulletin on Public Administration and Legal Affairs*. 2025. № 2. С. 47–54. DOI:

Розкрито проблематику перспектив стійкості національної безпеки України зважаючи на зростаючий вплив таких чинників, явищ і тенденцій. Відмічено, придатність для частого й колективно використання розглянутих інструментів, у тому числі характер можливих наслідків і обсяги збитків свідчать про посягання на національні інтереси України. Підкреслюється, що у цьому сенсі виправдано вести мову про загрози й ризики для національної безпеки України з відповідними реалістичними підсумками.

Ключові слова: *делінквентна поведінка, державна політика, загрози, засоби, корупція, криптовалюти, ризики, цифрові технології та інновації.*

ANALYSIS OF THE MAIN CORRUPTION PRACTICES CARRIED OUT BY THE FUNCTIONALITY OF CERTAIN FORMS OF DIGITAL ASSETS AND ASSESSMENT OF THEIR IMPACT ON THE NATIONAL SECURITY OF UKRAINE

Kiiashko Yurii Mykhailovych,
Doctor of Philosophy in Law, Senior Research Fellow
Department of Legal Expertise and Legislative Work
Scientific Institute of Public Law
Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0002-3283-8743

Voitko Tetiana Mykolaivna,
Research Fellow, Research Department for the Implementation
of Integrity Standards,
Scientific Center for Integrity Education and Prevention
of Corruption in the Security and Defense Sector,
National Defense University of Ukraine
Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0002-4326-0633

The presented scientific research is devoted to a topical issue – analysis of the main corruption practices carried out using the functionality of some forms of digital assets and assessment of their impact on the national security of Ukraine. It is argued that the rapid introduction of many digital technologies and innovations, in addition to advantages, has certain problematic aspects. It is emphasized that one of such positions is the rapid formation and establishment of new effective methods and means of obtaining illegal benefits. Taking into account the nature, number, possible consequences and popularization of these methods, the need to assess the potential of digital assets as progressive objects that can undermine the national security of Ukraine is emphasized.

Problematic positions in the formation and implementation of the state policy of zero tolerance for corruption through the prism of the challenges of the digital environment have been identified. It has been noted that under the current strategically established conditions it is difficult to count on the implementation of effective management measures. The development of a new Anti-Corruption Strategy with appropriate guidelines and phasing of implementation has been initiated.

The issue of the phenomenon of digital assets is revealed precisely from the position of promoting the development of corruption practices in Ukraine. It is emphasized that their exceptional properties contribute to the production of many unique mechanisms for obtaining certain types of illicit benefits. The common features of such instruments, regardless of the form of the digital asset, are clarified.

The widespread methods and ways of committing the acts themselves are described and analyzed, based on the awareness of the advantages of digital objects. In particular, the most common practices of committing corrupt acts are identified and differentiated. The effectiveness of these mechanisms is emphasized and assumptions are made regarding the increase in the number of illegal acts, taking into account the advantages of such conditions.

The issues of the prospects for the sustainability of Ukraine's national security are revealed, taking into account the growing influence of such factors, phenomena and trends. It is noted that the suitability for frequent and collective use of the considered instruments, including the nature of possible consequences and

the amount of damage, indicate an encroachment on the national interests of Ukraine. It is emphasized that in this sense it is justified to talk about threats and risks to Ukraine's national security with the appropriate realistic conclusions.

Key words: *delinquent behavior, public policy, threats, means, corruption, cryptocurrencies, risks, digital technologies and innovations.*

Актуальність теми

Стійка популяризація цифрових активів, зростання кількості їх форм та нарощування функціональних можливостей останніх формують нові складні ризики і загрози перед державою (Cumming et al., 2023; Isogawa, 2023). Природна об'єктивна неможливість адекватно й своєчасно реагувати на такі подразниками групами правових, організаційних, управлінських, технічних, технологічних та комбінованих інструментів відкриває нові перспективи для різних видів зловживань (Kiiashko, 2024). Взнаки даються й тривалі процедури урядування, у тому числі прийняття управлінських рішень і, часто, неефективне публічне адміністрування основних об'єктивованих ініціатив.

Навіть при центристському підході, що виходить із поміркованості потенційного руйнівного впливу (EU Cybersecurity Strategies for the Digital Decade, 2020; MiCA, 2024) та його націленості переважно на окремі вектори суспільних відносин (Digital Assets Regulation: Insights from Jurisdictional Approaches, 2024) хибним є шлях недооцінки таких факторів. До того ж, провідні суб'єкти міжнародного права (ESMA, ЄЦБ, FATF, OECD) і деякі країни (Велика Британія, Канада, Китай, ОАЕ, Сінгапур, США, Франція, Швейцарія, Японія та ін.) також вбачають відповідний потенціал цих засобів. У вітчизняних реаліях, із-поміж іншого, наявна обстановка формує сприятливе підґрунтя для виникнення нових методів і способів скоєння корупційних правопорушень (Capelleras, 2025), а також спонукання до цих діянь усвідомлюючи змогу безкарності за відповідні делінквентні прояви. Питання набуває виняткової гостроти в період дії правового режиму воєнного стану (Cifuentes-Faura, 2024). Адже у випадку зовнішньої агресії особливо важливо дотримуватися політики нульової толерантності щодо будь-яких виявів корупцігенності.

Діаметрально протилежна поведінка може призвести до масових проявів суспільного невдоволення, зокрема й підриву духу військовослужбовців та інших представників сектора оборони. З іншої сторони, корупційна діяльність прямо і опосередковано істотно позначається на різних компонентах всієї національної безпеки України (Antonova & Abdullayev, 2021) посилюючи сукупний тиск на державу. Все це негативно відобразиться на підтримці держави з боку міжнародних й іноземних партнерів додатково послаблюючи оборонний, економічній, гуманітарний та інші стратегічні напрями.

Роль цифрових активів під наведеним кутом зору найповніше можна розкрити через усвідомлення ключових властивостей останніх. Зокрема, до таких фундаментальних позицій слід віднести наступні: 1) активна і стійка інфільтрація в різні сфери економічних відносин та суміжних процесів; 2) багатофункціональність; 3) відсутність матеріального змісту; 4) економічна цінність і вартісна визначеність; 5) значний потенціал для розвитку внаслідок зростання кількості форм прояву та розширення функціоналу існуючих активів, генеруючи нові способи їхнього застосунку та засоби реалізації; 6) конкурентоздатність; 7) подекуди радикальний вплив на характер і темпи перебігу багатьох економічних процесів; 8) схильність до непрогнозованих радикальних трансформацій багатьох форм (Kiiashko, 2025). Їхня здатність до генерування різних типів похідних об'єктів (форм цифрових активів (Butnik-Siverskyi, 2025; Derun & Mysaka, 2022; Kud, 2019)) лише розширює діапазон поведінкових можливостей для корупційних зловживань. Не виникає сумніву, йдеться про ризики доповнення існуючого численного спектра корупційних схем (Graycar, 2015) інноваційними інструментами (Campanelli, 2017). Нарощуючи варіативність поточних тіньових механізмів та забезпечуючи появу нових інструментів укорінюється тенденція щодо викривлення наявних санкціонованих підходів державного й самоврядного управлінь. Фактично поглиблюються процеси розвитку квазі самостійних шляхів досягнення значущих цілей та обмеження гарантованих національних інтересів. Така інтерпретація осягнення суті репрезентованої проблеми вкотре дає мотивовані й аргументовані підстави вести мову про посягання на національну безпеку України, що є не допустимим під час триваючої війни та ускладнення ряду геополітичних і геоекономічних заходів.

Питання корупціогенності шляхом використання різних форм цифрових активів поступово набуває дослідницької популярності та фахової уваги в світі та Україні (Transparency International, 2023). Однак, зазвичай фокус інтересу націлений на криптовалюти – найвідомішого і найчастіше використовуваного їхнього представника. Усвідомлення її переваг можливими суб'єктами правопорушення нерідко спонукає до відповідних діянь із подальшою появою причинно-наслідкового зв'язку.

Разом із тим, варто безапеляційно усвідомлювати, що їх приналежність до цифрових активів (Dmytryk, 2021) дає змогу останнім генерувати

нові типи криптовалют, які, попри обертання за допомогою технології «Блокчейн», можуть мати унікальні корупційні переваги. Тобто, технічні параметри певної цієї одиниці розробляються якраз за допомогою цифрових інструментів. В повідомленні Національного агентства з питань запобігання корупції йдеться про те, що наявний технічний та аналітичний інструментарій у співпраці з Департаментом кіберполіції Національної поліції дає змогу встановити такі значимі факти: 1) дійсність володіння задекларованої криптовалюти; 2) реальність її належності декларанту (National Agency for the Prevention of Corruption, 2024). Разом із тим, це лише не значна частина способів скоєння таких діянь сумнівність яких може підтвердити або спростувати вказаний центральний орган виконавчої влади. Так, у повній мірі не вирішеною є проблема ідентифікації користувачів відповідних платформ, що ускладнює протидію її корупційним проявам. У певних системах учасники мають змогу використовувати фальшиві дані про особу, суттєво перешкоджаючи своїй ідентифікації (Campanelli, 2017). Окрім того, деякі криптовалюти і платформи їхнього безпосереднього обертання ("Tether" (USDT), "Bitcoin" (BTC), "Monero" (XMR) (Chainalysis, 2025)) забезпечують додаткові переваги в рамках приховування реальних власників активів стимулюючи використання останніх для відповідних цілей. Перераховані й інші засоби обігу найчастіше використовувалися для різних способів маніпуляцій із утаємничення персон володільців. До того ж, такі їх типи як "Dash" (DASH), "Monero" (XMR) та "Zcash" (ZEC) взагалі передбачають застосування криптографічних кодів, що засекречують реального володільця монети (Nosov et al., 2023; Sitthipon et al., 2023). На додаток до цього, давно існує ряд сервісів і методик приховування походження криптовалют. Серед найвідоміших варто згадати такі як ресурси із «мікшування» аналізованих засобів, трансакції без посередників за допомогою технології «p2p», децентралізовані біржі, що не вимагають ідентифікації особи, офшорні структури тощо. Тобто, лише така форма цифрових активів як криптовалюти має істотний потенціал для різних проявів корупційної діяльності. Частка існуючих технічних можливостей дає змогу скоювати відповідні діяння не обмежуючись разовими випадками, а й спонукати до систематичних практик.

У контексті саме цифрових активів перспективною вбачається гіпотеза, що й інші поширені їх форми можуть бути використані для успішної реалізації корупціогенних намірів. В розумінні Закону України «Про цифровий контент та цифрові послуги» персоніфіковано таким контентом визнаються наступні об'єкти: 1) комп'ютерні програми; 2) застосунки; 3) відеофайли; 4) аудіофайли; 5) музичні файли; 6) цифрові ігри; 7) електронні книги. Попри те, що правотворець відносить представлені одиниці до групи цифрових речей виграшною бачиться позиція оперування загальною категорією «цифрові активи». Семантично ці поняття не є тотожними, однак пропонований підхід базується на міжнародній практиці класифікування (ISO 55000:2014 "Asset management", 2014) та поглядах авторитетних вчених (Adekoya & Ekpo, 2022; Kud, 2019; Harbinja, 2017; Walker, 2017). Тому авторська система координат буде формуватися і розбудовуватися саме з орієнтуванням на ці позиції та з урахуванням їхніх характеристик. До того ж, як відносно криптовалют, так і цифрового контенту сама можливість існування, технічні параметри, їхня трансформація забезпечуються виключно завдяки цифровим активам.

Стосовно корупційних переваг такого типу форм аналізованих активів, то слід зазначити, що їх доцільно розглядати в якості засобів сприяння скоєння та приховування відповідних правопорушень. Насамперед, використання деяких програм та застосунків може дозволити чи спростити певні форми делінквентної поведінки генеруючи та успішною апробуючи нові способи її реалізації.

Численна кількість діянь, у тому числі, так званих «гучних кейсів» ("Ericsson List", "Panama Papers", "Uber Files", справа «Укрспирту», ряд проваджень із систематичної підробки офіційних документів по Україні чи певним регіонам спеціальними застосунками (судові справи № 329/263/18, 755/2595/21, 755/13800/24, 766/7888/18, 676/201/21, 754/8133/19 та ін.) супроводжувалось використанням вказаних ресурсів. Інколи, вони виконували функцію із конспектування та упорядкування відомостей про корупційне правопорушення (персональні дані особи, тип і розмір неправомірної вигоди, час, місце, обстановка та інші характеристики). Часто за їхньою допомогою вдавалось сфальсифікувати певний документ для задоволення неправомірного персонального чи колективних інтересів. Мали місце випадки оперативної зміни метаданих файлу чи його втрати, а також видалення цифрових слідів (Gruber et al., 2023), що суттєво ускладнювало процес доказування органам досудового розслідування. Слід також виділити випадки маскування даних, що становлять інтерес (таємниця охоронювана законом державного, комунального та приватного походжень, персональна інформація, в тому числі для подолання системи логічного захисту та ін.) (EU Cybersecurity Strategies for the Digital Decade, 2020). Тобто, функціональні можливості вказаних засобів створюють додаткові переваги для скоєння неправомірних заходів. Більшість вказаних інструментів є придатними та попередньо націленими на підвищення ефективності стійкості й перебігу одного чи декількох процесів не обмежуючи становище інших учасників. Водночас, подекуди, має місце їхнє застосування саме з мотивів корисливості, неправомірно задовольняючи власні запити.

Ще одним перспективним вектором можна вважати свідоме завищення вартості об'єкта цифрового середовища чи послуг із його

адміністрування та (або) вчинення правочину з ним на користь конкретної особи. У цьому контексті слід вести мову про свідоме встановлення цін, що не відповідають ринковим реаліям чи суперечать іншим санкціонованим вимогам. Також слід вказати на формування умов щодо зміни юридичної долі такого предмету договірних відносин саме для певного учасника і, відповідно, дискримінаційних іншим. Національне агентство з питань запобігання корупції в одному зі звітів визнало такий ризик під час здійснення публічних закупівель (National Agency for the Prevention of Corruption, 2021). Поширена вітчизняна практика укладення договорів підряду, про надання послуг та інших в публічному секторі, де мова йде про створення чи обслуговування об'єктів цифрового виміру (судові справи № 2610/11512/2012, 461/9063/13-к, 758/12263/23, 991/9799/23 та ін.) за вартість у декілька разів вищу ринкової на релевантний календарний період.

Наявність обвинувальних вироків засвідчує факт складу кримінальних правопорушень, побічно доводячи персональну гіпотезу. Адже, скоєння цих діянь стало можливим завдяки об'єктам цифрового середовища, які хоч і були націлені на легальні заходи, однак забезпечили отримання різних типів неправомірної вигоди. Відповідно, і під цим кутом зору потенціал цифрових активів може бути реалізований для продукування корупційної діяльності. При чому мова може йти як про разове порушення, так і систематичну й масову діяльності.

Окреслена й аргументована проблема набуває особливої гостроти на фоні стрімкого розвитку цифрових активів та стійкої популяризації окремих її форм серед українського суспільства. Зокрема, за 2024 р., особами, що уповноважені реалізовувати функції держави та місцевого самоврядування було подано 2113 декларацій з криптовалютою, що також на 10 % більше порівняно з минулим звітним роком (Opendatabot, 2025). На фоні описаних проявів, публічних фактів та судових вироків така тенденція спонукає до переосмислення ролі цифрових активів із позиції загрозливості національній безпеці України.

Стан дослідження

Тематика змісту, суті, форм, способів, специфіки і наслідків корупційної діяльності, шляхом використання унікальних переваг об'єктів цифрового виміру перебуває в полі зору протягом останніх десяти років. Поява та розвиток відомих формацій цих засобів відбувалася у різні періоди і мала на меті сприяти вирішенню певних суспільно корисних проблем. Знаковим слід вважати 2008–2009 рр., коли було розроблено та реалізовано концепцію технології «Блокчейн» (хоча прообрази її архітектури було закладено ще у кінці XX ст.) та введено в обіг першу криптовалюту "Bitcoin" (BTC). Далі слід зупинитися 2016–2017 рр., коли суб'єкти міжнародного права та держави все частіше почали звертати увагу на криптовалюти та оцінювати їхні можливості. Підсумки цього аналізу стосувалися і загрозливості однойменних засобів, насамперед із позиції підриву монетарного суверенітету та обмеженості державного регуляторного впливу на ці процеси.

Разом із тим, з плином часу, поступово почала викристалізовуватися ще одна реалістична проблема – дієві способи і засоби скоєння корупційних правопорушень. Якщо аналізувати статистичні дані наукометричної бази "Scopus", то можна помітити інтенсифікацію дослідницького інтересу якраз із 2018 р., коли кількість таких робіт сягнула більше 20 і в подальшому має місце тенденція до зростання публікацій.

Світові й вітчизняні автори розкривають різні грані цього питання вкотре доводячи слушність погляду про існування як переваг, так і недоліків вказаних технологій. Розвиток криптовалютних відносин лише підживлював цікавість до такої сфери спонукаючи поглиблене вивчення цих і суміжного кола проблем.

У той же час, ролі цифрових активів як ширшої системоутворюючої категорії також присвячена неабияка увага. Одначе, полівекторність спірних питань часто призводила до порушення багатьох аспектів, що у повній мірі не розкривають ініційовану проблему, а саме демонстрації впливу таких активів на продукування нових корупційних практик. Безумовно, ряд знакових статей висвітлюють низку значимих позицій для нашої тематики. Зокрема, у роботі (Capelleras, 2025) йдеться про можливості деяких форм цифрових активів щодо здійснення корупційної діяльності. У дослідженні (Copestake et al., 2023) змістовно висвітлено тематику реакції учасників крипторинку на зміну політики регулювання обертання цифрових активів. Доробок (Lee et al., 2023) висвітлює проблему цифровізації в міжнародних бізнес-відносинах саме з позиції провадження стійких корупційних практик відповідного походження. В публікації (Malik & Froese, 2022) розкривається питання зворотного боку цифровізації якраз під кутом продукування такого типу делінквентної поведінки на різних етапах і умовах перебігу суспільних відносин. Одначе, доводи репрезентовані у вступній частині матеріалу засвідчують нагальну потребу розробки персональних знакових гіпотез.

Мета статті

Керуючись орієнтирами теми дослідницького інтересу метою роботи має стати оцінка потенціалу цифрових активів як прогресуючих об'єктів, що генерують нові способи та засоби скоєння корупційних правопорушень підриваючи національну безпеку України. Досягнення поставленої цілі бачиться можливим шляхом виконання наступного переліку завдань: 1) визначити проблемні позиції формування та реалізації державної політики нульової толерантності до корупції крізь призму викликів цифрового середовища; 2) висвітлити питання феномену цифрових

активів саме з позиції сприяння розвитку корупційних практик в Україні; 3) описати та проаналізувати поширені методи і способи скоєння самих діянь виходячи з усвідомлення переваг об'єктів цифрового виміру; 4) розкрити проблематику перспектив стійкості національної безпеки України зважаючи на зростаючий вплив таких чинників, явищ і тенденцій.

Виклад основного матеріалу

Формування та реалізація всієї державної антикорупційної політики провадиться виходячи із орієнтирів Антикорупційної стратегії на 2021–2025 роки й з обов'язковим урахуванням державної програми її здійснення. Названі два документи, базуючись на приписах вітчизняного законодавства, визначають модель роботи суб'єктів правотворчості і правозастосування на певний період. Вони об'єктивують волю суверена у частині санкціонованого реагування щодо однієї з ключових проблем вітчизняної державності. Увага в цих приписах має звертатися відносно нагальних питань, які створюють сприятливе підґрунтя для здійснення корупційної діяльності.

Проте, виклики воєнного часу, стрімкий розвиток цифрових технологій й інновацій, а також популяризація засобів віртуальної сфери мимоволі спонукають до модифікації наявної системи орієнтирів. Відповідні корупційні загрози і ризики, які здавались малозначними явищами все частіше та значніше дають про себе знати у нинішній дійсності. Невідомий, можливо не вичерпний потенціал об'єктів цифрового виміру генеруючи нові типи об'єктів цього середовища паралельно формує дієві корупційні механізми.

Декларування цінностей політики нульової толерантності до корупції у цій ситуації має сумнівні перспективи з позиції реалістичності. Відсутність рівносильних заходів правового, організаційного, управлінського, технічного, технологічного та комбіновано наповнення об'єктивно унеможливлюють дійсну підтримку управлінських кроків. Тому аналізовані виклики фактично поки не матимуть комплексного спротиву в зв'язку із відсутністю необхідної державної політики. Зазначена ситуація лише сприятиме нарощуванню функціонального потенціалу аналізованих елементів іманентно стимулюючи до корупціогенної поведінки.

Провідні іноземні та вітчизняні дослідження, а також звіти, керівництва, рекомендації й інші документи інформативного спрямування наочно доводять тезу про існування зворотного боку стрімкої інтеграції цифрових об'єктів у суспільне середовище. Одним із таких самостійних прогресуючих векторів є зростання способів і засобів скоєння корупційних правопорушень. Феномен цифрових активів, зокрема їхні виключні властивості несуть реальні ризики й загрози світовим безпековим системам, що доводиться багатьма руйнівними проявами.

Вочевидь, що в загальних рисах ці елементи налічують ряд унікальних переваг, котрі необхідно використовувати для суспільно значущих цілей. Однак, їхня недостатня дослідженність, стрімке прогресування та, як було встановлено, регуляторна обмеженість суверена можуть призвести до фактів посягання на усталений правопорядок.

До прикладу, така властивість як «… значний потенціал для розвитку внаслідок зростання кількості форм прояву та розширення функціоналу існуючих активів, генеруючи нові способи їхнього застосунку та засоби реалізації…» дає аргументовані підстави вести мову про сприятливу основу для виникнення й розвитку нових варіацій корупції. Ураховуючи об'єктивну хронічно запізнілу реакцію правотворця щодо відповідних подразників можлива поява додаткових проблем, що екстраполюються на різні сфери.

На сучасному етапі цифровий вимір забезпечує ряд можливостей для здійснення корупційних практик. Таке міркування доводиться не лише своїми міркуваннями, а й публічними фактами та судовими вироками. Численні випадки і обмежена реакція контролюючих та правоохоронних органів наочно засвідчують стійкість відповідних тенденцій.

До найпоширеніших проявів корупціогенної поведінки за сприяння цифрових технологій та інновацій слід віднести наступні: 1) відмінні технічні можливості багатьох криптовалют та платформ для їхнього обертання, насамперед із позиції унеможливлення ідентифікації особи власника цього засобу обороту; 2) існування та активна робота багатьох сервісів і методик приховування походження криптовалют (ресурси із «мікшування», трансакції без посередників за допомогою технології «p2p», децентралізовані біржі, що не вимагають ідентифікації особи, офшорні структури тощо); 3) використання окремих форм цифрових активів (програми та застосунки) в якості засобів сприяння скоєння, а також приховування відповідних правопорушень; 4) різні маніпулювання на кшталт завищення вартості об'єкта цифрового середовища чи послуг із його адміністрування та (або) вчинення правочину з ним на користь конкретної особи. Остання варіація часто має місце в рамках публічно-правових відносин підриваючи авторитет органів державної влади та самоврядних інституцій.

Досвід показує успішність таких практик і стійкість останніх до санкціонованого державного й громадського реагування. Зазначене доводить переваги цифрового виміру під кутом зору фізичної змоги скоєння окремих складів корупційних правопорушень. Відсутність такого інструментарію не надасть можливості провадити аналізовані практики у відповідні способи. Це, своєю чергою, відображається на внутрішніх переконаннях потенційного суб'єкта всиляючи впевненість у безкарності своїх діянь та стимулювавши до нових релевантних вчинків.

Загалом такі потенційні поведінкові моделі є придатними для тривалого застосування, маючи значний уразливий ефект і масштаб поширення.

Це свідчить про доцільність їхнього позиціонування в якості загроз та ризиків (залежно від форми прояву і наслідків) для національної безпеки України. Оскільки, йдеться про пряме посягання на національні інтереси, постійне забезпечення котрих – прерогатива представників відповідних секторів.

Імовірна конгломерація багатьох цих активів із різними елементами всіх безпекових систем та зміна параметрів останніх вказують на реальний і суттєвий руйнівний вплив. На рівні з іншими об'єктивованими загрозами вказані чинники, явища та тенденції також слушно відносити до відповідної групи об'єктів реагування.

Окрім того, стійкий попит до певних форм цифрових активів серед осіб уповноважених на реалізацію функцій держави та місцевого самоврядування має спонукати до прискіпливого вивчення похідного кола аспектів. Вочевидь, що пріоритетне місце у такому випадку має бути відведене потенційним корупційним правопорушенням із огляду на вже існуючі «гучні кейси». Своєчасна фахова і дослідницька увага може сприяти стійкості національної безпеки України на фоні дії інших загроз, у тому числі воєнного походження.

Висновки

1. Формування та реалізація державної політики утвердження нульової толерантності до корупції буде неефективною без прийняття нової редакції Антикорупційної стратегії. Одним із провідних проблемних питань у такому документі має стати поетапне (з урахуванням передових міжнародних та іноземних підходів) формування механізмів реагування на корупційні прояви реалізовані за допомогою технічних можливостей різних форм цифрових активів. Короткострокова стратегія надасть можливість змістовно підвищити рівень правотворчої та правозастосовної роботи за цим вектором посиливши авторитет антикорупційної політики в державі. Суттєві досягнення та належні темпи їхньої реалізації сприятимуть євроінтеграційним процесам і глобальній протидії багатьом релевантним проявам.

2. Виняткові властивості цифрових активів сприяють продукування багатьох концептуальних механізмів здатних забезпечити отримання деяких типів неправомірної вигоди. Містивши ряд унікальних переваг для досягнення суспільно значущих цілей існує висока імовірність їхнього використання для посягання на усталений правопорядок. У залежності від функціональних параметрів об'єкта цифрового виміру та запитів зацікавлених сторони(-ін), мова може йти як про приховування діяння, так і безпосереднього скоєння. Мають місце непоодинокі випадки одночасного застосування цих функцій у межах одного складу правопорушення.

3. До найпоширеніших практик скоєння самих цих діянь відносяться наступні: 1) насамперед, унеможливлення ідентифікації особи власника засобу обороту завдяки відмінним технічним можливостям багатьох криптовалют та платформ для їхнього обертання; 2) існування та активна робота багатьох сервісів і методик приховування походження криптовалют; 3) скоєння, а також приховування відповідних правопорушень, шляхом використання окремих форм цифрових активів (програми та застосунки); 4) різні маніпулювання на кшталт завищення вартості об'єкта цифрового середовища чи послуг із його адміністрування та (або) вчинення правочину з ним на користь конкретної особи. Досвід показує результативність вказаних механізмів, що засвідчує існування зворотної сторони можливостей цифрових активів. Усвідомлення ефективності таких механізмів суспільством може спонукати до провадження, в тому числі систематичного, відповідної караної діяльності.

4. Придатність для тривалого й масштабного використання розглянутих інструментів, а також характер можливих наслідків і обсяги збитків побічно вказують про посягання на національні інтереси України. Така постановка питання дає мотивовані підстави вести мову про загрози й ризики (залежно від форми прояву і наслідків) національній безпеці України. Колосальний різновекторний потенціал та здатність трансформувати алгоритми роботи всіх безпекових систем підтверджують слушність репрезентованого погляду. Зазначене має спонукати до перегляду існуючих безпекових орієнтирів на користь відповідного визнання деяких форм цифрових активів, а саме методів і способів їхнього прояву.

Список використаних джерел:

Cumming D., Glatzer Z., & Guedhami O. (2023). Institutions, digital assets, and implications for economic and financial performance. *Journal of Industrial and Business Economics*, 50 (3), 487–513. URL: https://doi.org/10.1007/s40812-023-00276-y

Isogawa M. (2023). The Top Security Risks to be Aware of When Managing Your Digital Assets. Linkedin. URL: https://www.linkedin.com/pulse/top-security-risks-aware-when-managing-your-digital-assets-isogawa

Кіяшко Ю. (2024). Цифрові інструменти у структурі актуальних загроз системі економічної безпеки України : теоретико-методологічне дослідження. I*nternational Bulletin on Public Administration and Legal Affairs.* № 2. P. 81–91. DOI: 10.32844/ibpala-2024-2

The EU's Cybersecurity Strategy for the Digital Decade (2020). European Commission. 29 p. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Regulation (EU) 2023/1114 Of The European Parliament and Of The Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 : Regulation 2023/1114. European Parliament and Council. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114&qid=1730100184935

Digital Assets Regulation: Insights from Jurisdictional Approaches (2024). *Insight report.* 41 p. URL: https://www3.weforum.org/docs/WEF_Digital_Assets_Regulation_2024.pdf

Capelleras J.-L., Martin-Sanchez V., & Zhang C. (2025). The curvilinear relationship between digitalization and export propensity: The role of home country corruption in emerging economies. Technological Forecasting and Social Change, 214, 124043. URL: https://doi.org/10.1016/j.techfore.2025.124043

Cifuentes-Faura, J. (2024). Corruption in Ukraine during the Ukrainian–Russian war: A decalogue of policies to combat it. Journal of Public Affairs, 24 (1). Portico. URL: https://doi.org/10.1002/pa.2905

Antonova L., & Abdullayev V. (2021). Corruption as a threat to national security. Public Administration and Regional Development, 12, 336–355. URL: https://doi.org/10.34132/pard2021.12.02

Кіяшко Ю. (2025). Адміністративно-правове забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами : дис. … д-р філософ (081 – Право). Київ. 253 с.

Бутнік-Сіверський О. (2024). Цифрові та віртуальні активи: методологія, правові аспекти, нематеріальні ресурси. *Теорія і практика інтелектуальної власності.* № 2. С. 94–104.

Derun I., & Mysaka H. (2022). Digital assets in accounting: the concept formation and the further development trajectory. *Economic Annals-XXI*, 195 (1–2), 59–70. URL: https://doi.org/10.21003/ea.v195-06

Кудь О. (2019). Обґрунтування поняття «цифровий актив»: економіко-правовий аспект. *International Journal of Education and Science.* Vol. 2. № 3. P. 29–41.

Graycar, A. (2015). Corruption: Classification and analysis. *Policy and Society*, 34 (2), 87–96. URL: https://doi.org/10.1016/j.polsoc.2015.04.001

Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption (2024). Transparency International. URL: https://knowledgehub.transparency.org/helpdesk/cryptocurrencies-corruption-and-organised-crime-implications-of-the-growing-use-of-cryptocurrencies-in-enabling-illicit-finance-and-corruption

Дмитрик О. (2021) Віртуальні активи і цифрові активи: до питання про співвідношення понять. *Право та інноваційне суспільство.* № 2 (17). С. 248–254.

Full declaration inspections: it will not be possible to hide assets or artificially increase them in cryptocurrency (2024). National Agency for the Prevention of Corruption. URL: https://nazk.gov.ua/uk/povni-perevirky-deklaratsiy-pryhovaty-aktyvy-v-kryptovalyuti-abo-shtuchno-ih-zbilshyty-ne-vyyde/

Cryptocrime Report (2025). Chainalysis. URL: https://www.chainalysis.com/wp-content/uploads/2025/02/the-2025-crypto-crime-report-release.pdf

Nosov V., Manzhai O. & Kovtun V. (2023). Technical, forensic and organisational aspects of work with Monero cryptocurrency. *Law and Safety*, 90 (3), 102–125. URL: https://doi.org/10.32631/pb.2023.3.09

Sitthipon T., Kaewpuang P., & Auttawechasakoon, P. (2023). A Review of Cryptocurrency in the Digital Economy. *International Journal of Computing Sciences Research*, 7, 1152–1161. URL: https://doi.org/10.25147/ijcsr.2017.001.1.124

ISO 55000:2014 (2014). Asset management – Overview, principles and terminology. URL: https://www.iso.org/obp/ui#iso:std:iso:55000:ed-1:v2:en

Adekoya O., Ekpo E. (2022). Digital Assets – an emerging trend in capital markets. *PwC Nigeria.* P. 1–9. URL: https://www.pwc.com/ng/en/assets/pdf/digital-assets.pdf

Harbinja E. (2017). Legal aspects of transmission of digital assets on death: Doctoral dissertation. University of Strathclyde. Glasgow. URL: http://digitool.lib.strath.ac.uk/R/?func=dbin-jumpfull&object_id=28644

Walker M. (2017). The new uniform digital assets law: estate planning and administration in the information age. Real Property. *Trust and Estate Law Journal.* № 52 (1). P. 52–78.

Gruber J., Hargreaves C. J., & Freiling F. C. (2023). Contamination of digital evidence: Understanding an underexposed risk. Forensic Science International : *Digital Investigation,* 44, 301501. URL: https://doi.org/10.1016/j.fsidi.2023.301501

NACP has identified 25 typical corruption risks in public procurement (2021). National Agency for the Prevention of Corruption. URL: https://nazk.gov.ua/uk/uk/nazk-vyznachylo-25-typovyh-koruptsijnyh-ryzykiv-u-publichnyh-zakupivlyah

10 % more cryptocurrencies in officials' declarations over the year (2025). *Opendatabot.* URL: https://opendatabot.ua/analytics/crypto-2025

Copestake A., Furceri D., & Gonzalez-Dominguez, P. (2023). Crypto market responses to digital asset policies. Economics Letters, 222, 110949. URL: https://doi.org/10.1016/j.econlet.2022.110949

Lee J. Y., Park B. I., Ghauri P. N., & Kumar V. (2024). Corruptive practices, digitalization, and international business. *Journal of Business Research*, 181, 114748. URL: https://doi.org/10.1016/j.jbusres.2024.114748

Malik A., & Froese F. J. (2022). Corruption as a perverse Innovation: The dark side of digitalization and corruption in international business. *Journal of Business Research*, 145, 682–693. URL: https://doi.org/10.1016/j.jbusres.2022.03.032