

ПАЗЮК А. В.,

доктор юридичних наук,
професор кафедри міжнародного
та європейського права,
(Державний університет «Київський
авіаційний інститут»)

УДК 341

DOI <https://doi.org/10.32842/2078-3736/2025.3.2.49>

МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ РЕГУЛЮВАННЯ ВІРТУАЛЬНИХ АКТИВІВ У КІБЕРПРОСТОРІ: БАЛАНС МІЖ ЦИФРОВИМ СУВЕРЕНІТЕТОМ ТА ГЛОБАЛЬНИМИ ЗОБОВ'ЯЗАННЯМИ ДЕРЖАВ

Стаття присвячена комплексному аналізу міжнародно-правових стандартів регулювання віртуальних активів у кіберпросторі крізь призму балансу між цифровим суверенітетом держав та їхніми глобальними зобов'язаннями. Віртуальні активи, що, відповідно до визначення FATF, є цифровим представленням вартості, яке може передаватися, зберігатися або використовуватися для платежів чи інвестицій, становлять нові загрози та виклики для класичних принципів міжнародного права, які ґрунтуються на принципах державного суверенітету та територіальної юрисдикції. Їхня децентралізована природа, транскордонний обіг та відсутність єдиної правової рамки створюють ризики у сферах відмивання грошей, фінансування тероризму, шахрайства та кіберзлочинності.

Проаналізовано ключові міжнародні стандарти, такі як рекомендації Групи з розробки фінансових заходів боротьби з відмиванням грошей, що встановлюють вимоги до проведення фінансового моніторингу та обміну інформацією, положення Ради з фінансової стабільності, які впроваджують принципи технологічної нейтральності та підхід “однакова діяльність, однаковий ризик, однакове реагування”, а також нормативно-правові акти Європейського Союзу, спрямовані на гармонізацію правових режимів у межах утворення.

Розкрито сутність цифрового суверенітету як здатності держави самостійно визначати політику функціонування своєї цифрової інфраструктури, регулювати обіг даних та захищати права громадян. У той же час підкреслюється дуальність цифрового суверенітету, який передбачає не тільки права, але й обов'язки держави з дотримання міжнародних норм щодо невтручання, взаємної поваги та співпраці.

Зроблено висновок про те, що пошук балансу між цифровим суверенітетом та глобальними зобов'язаннями вимагає від держав запровадження правових норм, адаптованих до національних потреб, із одночасним дотриманням міжнародних стандартів та участю у транскордонних механізмах регулювання. Завдяки такому підходу мінімізуються ризики, що пов'язані з обігом віртуальних активів, зберігається національна безпека та забезпечується інтеграція в глобальну цифрову економіку.

Ключові слова: віртуальні активи, кіберпростір, цифровий суверенітет, міжнародні стандарти, транскордонна координація, правове регулювання, міжнародні зобов'язання.



Paziuk A.V. International Legal Standards for Regulating Virtual Assets in Cyberspace: Balancing Digital Sovereignty and the Global Obligations of States

The article is devoted to a comprehensive analysis of the international legal standards for regulating virtual assets in cyberspace through the prism of balancing the digital sovereignty of states and their global obligations. Virtual assets, which, according to the FATF definition, are a digital representation of value that can be transferred, stored, or used for payment or investment purposes, pose new threats and challenges to the classical principles of international law based on state sovereignty and territorial jurisdiction. Their decentralized nature, cross-border circulation, and the absence of a unified legal framework create risks in the areas of money laundering, terrorist financing, fraud, and cybercrime.

The article analyzes key international standards, such as the recommendations of the Financial Action Task Force (FATF), which establish requirements for conducting financial monitoring and information exchange; the provisions of the Financial Stability Board (FSB), which implement the principles of technological neutrality and the “same activity, same risk, same regulation” approach; as well as the regulatory acts of the European Union aimed at harmonizing legal regimes within the Union.

The essence of digital sovereignty is revealed as the state’s ability to independently determine the policy for the functioning of its digital infrastructure, regulate data circulation, and protect the rights of its citizens. At the same time, the dual nature of digital sovereignty is emphasized, which entails not only the rights but also the obligations of the state to comply with international norms of non-interference, mutual respect, and cooperation.

It is concluded that the search for a balance between digital sovereignty and global obligations requires states to introduce legal norms adapted to national needs while simultaneously complying with international standards and participating in cross-border regulatory mechanisms. Such an approach minimizes the risks associated with the circulation of virtual assets, preserves national security, and ensures integration into the global digital economy.

Key words: *virtual assets, cyberspace, digital sovereignty, international standards, cross-border coordination, legal regulation, international obligations.*

Постановка проблеми. Віртуальні активи (Virtual Assets, далі – ВА) стали невід’ємним елементом сучасної цифрової економіки. Їх обіг та використання має як свої переваги, зокрема більш легке та дешеве проведення фінансових операцій, так і недоліки, такі як відсутність чіткого регулювання, вразливість до шахрайства, зловживань, ризики вчинення порушень у сфері відмивання грошей та фінансування тероризму тощо. Без належного законодавчого врегулювання ВА ризикують стати ефективним інструментом для фінансових злочинів, терористів і протизаконних режимів.

Традиційні принципи міжнародного права, які засновані на державному суверенітеті та територіальній юрисдикції, видаються не такими ефективними щодо віртуальних активів, адже вони функціонують у глобальному кіберпросторі, через що виникає конфлікт між правом держави на контроль власної цифрової території та необхідністю міжнародної співпраці. Як зазначає В. Крішнамуфті, протягом чверті століття панувала думка про те, що територіальний суверенітет застосовується в межах Інтернету так само, як у реальному світі, і досі існують обговорення про те, що суверенітет держав повинен поширюватися на кіберпростір [1]. У той же час, міжнародне право не містить достатніх запобіжників для того, щоб унеможливити для держав поділ загальної мережі на національні, що суперечить принципам глобального, відкритого та вільного інтернету.

Таким чином, актуалізується проблема пошуку балансу між цифровим суверенітетом держави, тобто її правом самостійно регулювати свій кіберпростір, та глобальними зобов’язаннями з виконання міжнародних стандартів і норм.



Дослідження має на меті системний аналіз існуючих міжнародно-правових стандартів регулювання ВА у кіберпросторі та обґрунтування способів досягнення балансу між цифровим суверенітетом держав і їхніми міжнародними зобов'язаннями. Зокрема, досліджуються найбільш впливові норми та рекомендації, щоб виявити загальні тенденції та виклики адаптації до глобальних стандартів регулювання.

Стан опрацювання проблематики. Останніми роками питання правового регулювання віртуальних активів посідає дедалі більш помітне місце у вітчизняній науковій думці, що зумовлено як стрімким розвитком цифрової економіки, так і зростанням кількості ризиків і загроз у кіберпросторі. Серед дослідників, чий науковий доробок доцільно виділити в контексті обговорюваної тематики, варто відзначити таких вчених як К.Г. Некіт, С.О. Грицай, В.Я. Новицький, В.М. Грудницький, С.М. Аксюков, Г.І. Воєводіна, В.М. Фица. Паралельно з цим, проблематика цифрового суверенітету знаходить своє відображення у працях Д. Дубова, Є. Новікова, І.М. Милосердної, О.М. Солодки, Н. Ротар, Ю.І. Калюжної та інших. Попри зростаючу увагу до цих питань, комплексне дослідження взаємозв'язку між цифровим суверенітетом держави та її міжнародними зобов'язаннями у сфері регулювання віртуальних активів залишається недостатньо розробленим, що обумовлює актуальність подальших наукових пошуків у цьому напрямі.

Виклад основного матеріалу. Віртуальні активи, за термінологією Групи з розробки фінансових заходів боротьби з відмиванням грошей (далі – FATF), є цифровим представленням вартості, яким можна торгувати, передавати в цифровому вигляді або використовувати для платежів та інвестицій [2]. При цьому, ВА не включають цифрове представлення фіатних валют, як-от електронні гроші. В Україні теж були спроби надати визначення ВА, зокрема Закон України “Про віртуальні активи” [3], що не набрав чинності, пропонує наступні дефініцію: нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Це поняття охоплює два види віртуальних активів: незабезпечені (ті, що не посвідчують жодних майнових або немайнових прав) та забезпечені (ті, що посвідчують майнові права, зокрема права вимоги на інші об'єкти цивільних прав).

Ключовою рисою ВА є їх децентралізованість та здатність до транскордонного обігу без участі традиційних фінансових посередників, що хоч і має низку переваг, зокрема швидкі перекази та залучення інновацій, також породжує ряд загроз: уникнення нагляду, відмивання коштів, фінансування злочинної діяльності, шахрайство тощо. Через ці виклики постає потреба визначити, які саме активи підпадуть під правове регулювання та в яких межах. Наразі аналіз міжнародно-правових підходів до регулювання ВА свідчить про відсутність єдності та існування різноманітних моделей, які наслідують правові традиції держави, її економічні інтереси та особливості національної правової системи [4].

На міжнародному рівні основними джерелами регулювання ВА виступають міжнародні організації та стандарти. У цьому контексті перш за все слід згадати FATF, що у своїх рекомендаціях закликає країни запроваджувати комплекс заходів протидії легалізації коштів і фінансуванню тероризму у секторі віртуальних активів. Зокрема FATF встановлює, що держави повинні розуміти ризики у цьому секторі, здійснювати ліцензування або реєстрацію постачальників послуг із обміну ВА та наглядати за ними на тому ж рівні, що запроваджується для звичайних фінансових установ [5]. У свою чергу, постачальники послуг ВА повинні застосовувати такі ж превентивні заходи, як і фінансові установи, зокрема проводити перевірку своїх клієнтів (due diligence), вести облік операцій, подавати звіти про підозрілі транзакції, а також зберігати й передавати інформацію про власників коштів. Ці вимоги покликані гарантувати прозорість транскордонних операцій із ВА та унеможливити переходування нелегальних фінансових потоків.

Загалом принцип, згідно із яким ефективно регулювання вимагає глобального підходу, наразі є одним із ключових. Зокрема FATF наголошує, що без виконання міжнародних стандартів держави ризикують відставати та створювати “лазівки” для злочинців, у той час як глобальний підхід та єдиний регуляторний режим у всіх юрисдикціях можуть забезпечити ефективні правозастосування та нагляд. У своїх рекомендаціях FATF зазначає, що



забезпечення дотримання вимог у секторі ВА потребує спільного підходу та рівномірної нормативно-правової бази в різних державах, що не тільки зменшить ризики та загрози, пов'язані з віртуальними активами, але й обмежить можливість одних постачальників мати несправедливу конкурентну перевагу перед іншими, що знаходяться в більш регульованих юрисдикціях [2]. Іншими словами, нехтування міжнародними зобов'язаннями може призвести до регуляторного арбітражу, коли постачальники послуг ВА переходять до найменш контрольованих юрисдикцій.

Рада з фінансової стабільності (Financial Stability Board, далі – FSB), яка є дорадчим органом G20 для моніторингу з питань глобальної фінансової стабільності, також опублікувала власні рекомендації з регулювання ВА [7]. Ними встановлюється “глобальна регуляторна база” для ринків віртуальних активів, а також здійснюється заклик держав до застосування правил, що є технологічно-нейтральними та орієнтованими на підґрунтя ризику. У рекомендаціях також наголошено на підході “однакова діяльність, однаковий ризик, однакове регулювання”, відповідно до якого органи влади мають застосовувати комплексне та ефективне регулювання, нагляд та контроль за ринками ВА на функціональній основі та пропорційно до тих ризиків, що становлять або можуть становити ці ринки для фінансової стабільності. Окрім цього, FSB, як і FATF, наголосила на необхідності транскордонного співробітництва, координації дій між органами влади різних держав та обміну інформацією для належного виконання повноважень та узгодження результатів регулювання та нагляду.

У міжнародному контексті важливу роль відіграє також політика Європейського Союзу (далі – ЄС) та ініціативи, які виникають в рамках цього утворення. Зокрема у 2023 році в ЄС було запроваджено Регламент ЄС про ринки криптоактивів (Markets in Crypto-assets, далі – MiCA) [8], що створив єдину нормативну рамку для ВА у межах Союзу. Документ, серед іншого, має на меті гармонізацію правил для емітентів віртуальних активів та постачальників послуг, захист інвесторів та споживачів, створення рівних умов для бізнесу на всій території ЄС.

Отже, наразі існує чітка тенденція до запровадження міжнародних стандартів боротьби з відмиванням грошей та фінансуванням тероризму, транскордонної співпраці та узгодженого регулювання ВА. У науковій доктрині підкреслюється, що хоча єдиної уніфікованої моделі не створено, майже в усіх системах прослідковуються спільні риси, такі як поділ ВА за функціями, встановлення спеціальних режимів для різних типів активів та посилення заходів протидії злочинності [4].

Державний суверенітет у кіберпросторі є багатоаспектним поняттям, адже з одного боку він закріплює за державою право на охорону власної національної інфраструктури та контроль інформаційних потоків на своїй території, а з іншого – традиційні уявлення про застосування суверенітету по всьому інтернет-простору не відповідають реаліям глобалізації [9]. Дійсно, суверенітет держави в його класичному розумінні складно поєднувати з міжнародними зобов'язаннями розвинутих демократій щодо дотримання принципів вільного та відкритого кіберпростору. Із цього приводу деякі з науковців проводять аналогію з морським правом та пропонують уявляти кіберпростір як море, де права держав нарастають при наближенні до берегів і одночасно слабшають у глобальному океані [1]. Такий підхід міг би забезпечити легітимність національних регламентів, при цьому не порушуючи принципів відкритого інтернету.

Ю.І. Калюжна наголошує на ключовій ролі цифрового суверенітету для забезпечення національної безпеки та захисту стратегічних інтересів держави, що охоплює здатність до самостійного визначення політики в кіберпросторі, ефективного контролю над національною цифровою інфраструктурою, даними, технологічним розвитком та регуляторним середовищем [10]. Є. Новіков акцентує увагу на різних підходах держав до визначення та підтримки цифрового суверенітету: у той час як деякі держави використовують концепцію “кібернаціоналізму”, що спрямована насамперед на придушення інакомислення та демократичних прав людини в кіберпросторі заради національної безпеки та задоволення геополітичних інтересів, інші розглядають суверенітет у цифровому просторі з огляду на права



громадян здійснювати автономний контроль над інформаційною інфраструктурою та ресурсами [11].

Тут слід наголосити на тому, що з концепції цифрового суверенітету випливають не тільки права держави, але й її обов'язки. Так, у позиційній заяві Китаю [9] наголошується, що суверенітет у кіберпросторі, окрім прав, передбачає для держав і необхідність поважати загальні норми міжнародного права та виконувати покладені на них зобов'язання: зокрема, жодна країна без дозволу не повинна отримувати доступ до інформаційно-телекомунікаційної інфраструктури іншої держави чи втручатися в її мережу. Це підкреслює, що цифровий суверенітет не є абсолютизмом і поєднується з принципами невтручання, взаємної поваги та співпраці.

Попри бажання держав максимально зберегти свою незалежність навіть в умовах глобального інтернету, міжнародні зобов'язання вимагають від них співпраці та кооперації. Під тиском транскордонних викликів, насамперед фінансових та безпекових, країни прагнуть до розробки різних механізмів координації. Прикладом цього є міжнародні конвенції, наприклад Конвенція про кіберзлочинність [12], угоди про обмін інформацією, двосторонні та багатосторонні договори між фінансовими регуляторами тощо. Міжнародний валютний фонд із цією метою запровадив регіональні програми навчання з регулювання фінтех-індустрії, у тому числі регулювання ВА, де надаються практичні рекомендації щодо впровадження стандартів FSB та інших міжнародних стандартів [13].

Отже, сучасне регулювання ВА формується на перетині двох тенденцій, одна з яких представляє державну стратегію цифрового суверенітету, коли кожна країна бажає захистити власну економіку та безпеку шляхом встановлення національних правил для інтернет-сектору, а інша – вимагає дотримання міжнародних зобов'язань та імплементації узгоджених норм для забезпечення спільної стабільності. Баланс між цими тенденціями має полягати в компромісі, покликаному зберегти достатній рівень нагляду та контролю для національних учасників ринку ВА, але водночас забезпечити сумісність національних правил із міжнародними рамками та стандартами.

На практиці це означає, що держава встановлює законодавчі норми щодо ВА (зокрема про ліцензування, звітність і захист даних), виходячи із національних інтересів та особливостей, але при цьому має брати на себе зобов'язання щодо міжнародного співробітництва у цій сфері. Прикладом слугують випадки, коли правоохоронні органи однієї з держав передають інформацію органам іншої, якщо того вимагає закон, або коли регулятори впроваджують процедури сумлінного фінансового моніторингу, які відповідають міжнародним стандартам. З іншого боку, визнається право держав обґрунтовано регулювати технології на своїй території.

Висновки. Із розвитком цифрових технологій і поширенням ВА міжнародна правова спільнота перебуває в процесі опрацювання нових стандартів, аби забезпечити безпеку глобальних фінансових систем. При цьому найбільш поширеною є думка, що ефективно регулювання має поєднувати як національну волю держав, так і міжнародну відповідальність. Більшість країн уже завершили або знаходяться в процесі адаптації національного законодавства до світових стандартів і рекомендацій, у тому числі від FATF, FSB та ЄС.

З одного боку, держави мають право встановлювати правила для захисту власних інтересів і безпеки у цифровому просторі, а з іншого – їх міжнародні зобов'язання вимагають не використовувати цю свободу надмірно, інакше відбудеться розмивання глобального інформаційного простору. Оптимальним шляхом тут є винайдення компромісу: забезпечення домінуючої ролі закону та контролю в національних юрисдикціях, за умови належного виконання міжнародних норм і стандартів через співпрацю та гармонізацію.

Список використаних джерел:

1. Krishnamurthy, Vivek (2025) "Anchoring Digital Sovereignty," *Chicago Journal of International Law*: Vol. 25: No. 2, Article 2.



2. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Офіційний сайт “*FATF*”, Paris. 2021. 109 p. URL: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>
3. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX. *Відомості Верховної Ради України*. 2023. № 15. Ст. 51. URL: <https://zakon.rada.gov.ua/laws/show/2074-IX#Text>
4. Сидоренко В., Дутов М. Міжнародно-правові підходи до правового статусу віртуальних активів: виклики для українського законодавства. Соціальний розвиток: економіко-правові проблеми. 2025. Вип. № 6. 9 с.
5. Updated International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Офіційний сайт “*FATF*”, Paris. 2025. 148 p. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
6. FATF. Virtual Assets. Офіційний сайт “*FATF*”. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
7. High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets. Офіційний сайт “*FSB*”, 2023. URL: <https://www.fsb.org/uploads/P170723-2.pdf>
8. 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. URL: <https://eur-lex.europa.eu/legal-content/%20EN/TXT/?uri=CELEX%3A32023R1114>
9. China’s Views on the Application of the Principle of Sovereignty in Cyberspace. Офіційний сайт “*UNODA*”, 2021. URL: <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf#:~:text=territories%20according%20to%20law,ICT%20activities%20outside%20their%20territories>
10. Калюжна Ю.І. Цифровий суверенітет як фактор національної безпеки ЄС та України. *Національні інтереси України*. 2025. Вип. № 6(11). С. 1094-1124.
11. Novikov Y. Digital Sovereignty: conceptual challenges and constitutional implications. *Конституційно-правові академічні студії*. 2024. Вип. № 1. С. 61-69.
12. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23 листопада 2011 року. *Офіційний вісник України*. 2007. № 65. Ст. 2535.
13. Adrian T. The Changing Landscape of Crypto Assets—Considerations for Regulatory and Supervisory Authorities. Офіційний сайт “*IMF*”, 2024. URL: <https://www.imf.org/en/News/Articles/2024/02/23/sp022324-changing-landscape-crypto-assets-considerations-regulatory-and-supervisory-authorities#:~:text=The%20establishment%20of%20robust%20global,work%20more%20effectively%20and%20efficiently>

