

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова праця

на правах рукопису

КІЯШКО ЮРІЙ МИХАЙЛОВИЧ

УДК 338.24.021.8:342.951(477)

ДИСЕРТАЦІЯ

**АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ
ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО
МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК
ОПЕРАЦІЙ ІЗ ЦИФРОВИМИ АКТИВАМИ**

Спеціальність – «081 Право»

Галузь знань – «08 Право»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело


_____ Ю. М. Кіяшко

Науковий керівник – **Гаруст Юрій Віталійович**, доктор юридичних наук,
професор

Київ – 2025

АНОТАЦІЯ

Кіяшко Ю. М. Адміністративно-правове забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 Право. – Науково-дослідний інститут публічного права, Київ, 2025.

У дослідженні вперше реалізовано спробу формування сприятливого теоретико-методологічного, методичного та правового підґрунтя для розбудови комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Відповідні результати отримані з урахуванням міркувань провідних іноземних і вітчизняних вчених, норм міжнародного права, національного й іноземного законодавств, документів рекомендаційного характеру, практик їх застосування, проєктів, а також різного типу аналітичних матеріалів.

Доведено, що на сучасному етапі своєчасним, виправданим і обґрунтованим є оперування саме категорією «система економічної безпеки України». Запропоновано авторське розуміння зазначеної дефініції, визначено її властивості та ознаки, сформульовано мету і завдання. Розкрито та проаналізовано структуру системи економічної безпеки України. Доведено сталість її певних елементів та встановлено змінність деяких складових, що обумовлено сукупною дією різних факторів, у тому числі цифрового походження.

Проаналізовано існуючі іноземні й вітчизняні підходи до розуміння змістовного наповнення категорії «цифрові активи». Шляхом уніфікації й подальшого аналізу суджень розроблено її авторські визначення та запропоновано властивості й ознаки. Здійснено огляд і аналіз, насамперед,

тверджень закордонного походження щодо типологізації (форм) указаних активів. Установлено факт їх прогресуючого й прогресивних характерів із позиції експоненціальних темпів зростання кількості та розширення функціоналу останніх.

Визначено перелік основних загроз системі економічної безпеки України, надано авторське визначення поняття «загрози системі економічної безпеки України», охарактеризовано властивості таких загроз та виявлено ознаки відповідної категорії, а також змістовно висвітлено питання класифікації останніх. Проаналізовано загрози, які можуть виникати внаслідок операцій із цифровими активами (цифрової складової), а також досліджено основні наукові підходи до форм їх прояву. Оцінено потенціал таких засобів із позиції руйнівного впливу на характер, стійкість і темпи перебігу багатьох економічних процесів.

Підкреслено визначальну роль міжнародних й іноземних стандартів і правових механізмів у питаннях розбудови цифрових середовищ та закладенні підвалин із протидії загрозам, які можуть виникати внаслідок операцій з цифровими активами, а також оцінено їхній вплив на результати національної правотворчості. Наголошено й доведено потребу подальшого урахування таких цілей і орієнтирів, із огляду на євроінтеграційні прагнення українського народу, транснаціональний характер відповідних тенденцій, чинників і явищ, інші істотні фактори.

Розглянуто питання адміністративно-правових засад із протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами, а саме – розроблений відповідний термін і запропоновано авторську класифікацію останніх. Аргументовано зауважено на потребі стійкого й комплексного вдосконалення таких основ, ураховуючи потенціал цифрових засобів.

З'ясовано, що на сучасному державотворчому етапі компетенція багатьох державних органів передбачає залученість у процеси, регульовані наявними адміністративно-правовими засадами. Доведено, що до суб'єктів системи

економічної безпеки України зі спеціальною компетенцією, орієнтованих на протидію загрозам цифрового середовища, відносяться: 1) Міністерство цифрової трансформації України; 2) Державна служба фінансового моніторингу України; 3) Національна комісія з цінних паперів та фондового ринку; 4) Національний банк України; 5) правоохоронні органи (Бюро економічної безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України, Національна поліція, Служба безпеки України). Окремо відзначено роль Міжнародної групи з протидії відмиванню брудних грошей як суб'єкта міжнародного права. Висвітлено проблематику рівнів та напрямів функціонування вищенаведених провідних інституцій у цій сфері.

Підкреслено вагому роль консолідації зусиль із питань протидії легалізованим та іншим формам цифрових активів. Репрезентовано поняття такої взаємодії, визначено ознаки, окреслено мету та завдання, виконання яких покликане забезпечувати досягнення всіх поставлених цілей. Досліджено наявні механізми взаємодії за участі пропонованих суб'єктів за підвідомчими напрямами роботи.

Акцентовано увагу на важливості ефективного й результативного контролю і нагляду по відношенню до учасників легалізованих та інших ринків цифрових активів, а також суб'єктів, задіяних у регулятивних мірах щодо вказаної сфери. Наголошено на тому, що застосунок відповідних механізмів, окрім профілактичних кроків, може також сприяти виявленню прогалів, колізій і решти недоопрацювань.

Здійснено огляд та компаративний аналіз міжнародних (ESMA, ЄС, ЄЦБ, FATF, OECD) і провідних закордонних моделей (Австралія, Багамські Острови, Бермудські Острови, Велика Британія, Канада, Китай, Швеція, Об'єднані Арабські Емірати, Казахстан, Кіпр, Мальта, Молдова, Сінгапур, Філіппіни, Сполучені Штати Америки, Німеччина, Франція, Швейцарія, Японія та ін.) щодо протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами. Наголошено, що міжнародна спільнота вийшла на новий рівень розбудови уніфікованих підходів регламентації відносин, які виникають під час

обороту окремих типів таких активів. Відмічено, що проблематика загроз від операцій із цифровими активами в Україні досліджена фрагментарно й за рядом позицій перебуває у процесі становлення.

Проаналізовано моделі і правові механізми іноземних країн, які мають здобутки за таким вектором. На основі аналізу цих практик сформовано діапазон найпоширеніших загроз від операцій із цифровими активами, таких як: кіберзагрози, легалізація (відмивання) доходів, отриманих протиправним шляхом, недостатня дослідженість таких засобів та їх стрімке прогресування за різними характеристиками, шахрайство, інші чинники, явища, а також тенденції.

Окреслено першочергові вектори розбудови адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами: 1) розробка сприятливого теоретико-методологічного та методичного підґрунтя; 2) формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів реагування на чинники, явища та тенденції цифрового походження; 3) вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України. Зважаючи на національні законодавчі безпекові реалії, наголошено й обґрунтовано слушність і своєчасність удосконалення відповідних усталених підходів. Ураховуючи негативний правотворчий досвід осяжного минулого, аргументовано доведено необхідність слідування заданим орієнтирам.

Визначено шляхи реалізації напрямів формування комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами з урахуванням досвіду іноземних країн. Зокрема, у рамках розробки сприятливого теоретико-методологічного та методичного підґрунтя йдеться про наступні кроки: 1) виконання комплексних типологічних досліджень суб'єктами, що компетенційно дотичні до аналізованої сфери, а також зацікавленими закладами вищої освіти; 2) розробка механізмів аудиту

ефективності національної фінансової системи на предмет оцінки руйнівного впливу цифрових засобів та проведення однойменних заходів; 3) створення робочих груп за участю уповноважених суб'єктів публічно-правових відносин, а також представників вітчизняної й іноземної фахової громадськості для висвітлення та аналізу проблемних питань у цій сфері; 4) посилення різних, у тому числі неправових форм взаємодії суб'єктів правоохоронної діяльності.

Щодо формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів реагування на чинники, явища та тенденції цифрового походження, йдеться про такі кроки: 1) акумуляція результатів типологічних досліджень, результатів аудиту ефективності національної фінансової системи, підсумків дискусій у рамках міжвідомчого аналізу проблемних питань, пропозицій і висновків комітетів Верховної Ради України; 2) формування базису для розробки проєктів законів та інших нормативно-правових актів; 3) прийняття (затвердження) актів законодавства, котрі забезпечуватимуть подальший розвиток системи економічної безпеки України та розробку нових і удосконалення існуючих механізмів реагування на відповідні подразники. Відносно вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів), шляхом окреслення чітких намірів із удосконалення їх адміністративно-правового статусу, мова повинна йти про такі заключні заходи: 1) на базі сформованого юридичного підґрунтя предметно опрацювати питання щодо посилення адміністративно-правового становища суб'єктів зі спеціальною компетенцією та деяких інших установ, з метою приведення у чітку відповідність завдань і функцій таких органів орієнтирам системі економічної безпеки України; 2) всебічне і повне вивчення міжнародних стандартів та моделей, а також практик іноземних держав; 3) розробка пропозицій і рекомендацій щодо внесення змін до чинного законодавства, які формуватимуть комплексне і збалансоване адміністративно-правове забезпечення вказаної сфери. Доведено, що послідовна й неухильна реалізація таких шляхів є безальтернативною передумовою на шляху розбудови

комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Акцентовано на потребі подальшої систематичної розробки відповідних вчень як для необхідної передумови стійкості та сталого економічного розвитку держави. Наголошено, що статика наявного інструментарію – невідворотна передумова стагнації чи навіть руйнування багатьох економічних процесів критично важливих для воюючої та фінансово залежної країни.

Ключові слова: адміністративно-правові засади, адміністративно-правове регулювання, активи, взаємодія, засоби, економічна безпека, економічна злочинність, методи, механізм, контроль, нагляд, напрями, правоохоронні органи, рівні, суб'єкти, тенденції, цифрова економіка, цифрові інновації та технології, форми, чинники, явища.

SUMMARY

Kiiashko Yu. Administrative and legal means against threats to the economic security system of Ukraine that may arise as a result of transactions with digital assets – *Qualifying scientific work as a manuscript.*

Dissertation for a scientific degree of the Doctor of Philosophy in specialty 081 Law. – Scientific Institute of Public Law, Kyiv, 2025.

An attempt to form a favourable theoretical and methodological, methodical and legal basis for the development of the system and mechanisms of administrative and legal support for countering threats to the economic security system of Ukraine that may arise as a result of transactions with digital assets has been made for the first time within the study. Taking into account the opinions of leading foreign and domestic scientists, norms of international law, national and foreign legislation, documents of a recommendatory nature, practices of their application, projects, as well as various types of analytical materials, the relevant results have been obtained.

It has been proven that it is timely, justifiable and justified to use the category “economic security system of Ukraine” at the current stage. Its concept is proposed, its properties and characteristics are determined, and the purpose and task of its functioning are formulated. The issue of the structure of the latter is revealed and both the constancy of some parameters and the variability of some parameters of the specified system, which is dictated by the combined action of a number of factors, including those of digital origin, have been proved.

The existing foreign and domestic approaches to understanding the content of the “digital assets” have been analysed. By means of unification and further analysis of judgments, the author’s differentiation of groups of relevant considerations has been proposed. First of all, the review was carried out of statements of foreign origin regarding the typology (forms) of the specified assets. The fact of their progressive nature was established from the point of view of the exponential rate of growth of the number and expansion of the functionality.

The concept of threats to the system of economic security of Ukraine has been

formulated, the properties of such threats have been determined and the signs of the corresponding category have been identified, as well as the question of classification of the latter has been meaningfully considered. Special attention is paid to the threats that may arise as a result of operations with digital assets (digital component), as well as the views of the forms of their manifestation, popular in scientific circles, have been introduced. The potential of such means from the point of view of their destructive influence on the nature, stability and pace of many economic processes has been assessed.

The determining role of international and foreign standards in the issues of building digital environments and laying the foundations for countering threats that may arise as a result of operations with digital assets has been emphasized and their impact on the results of national law-making has been assessed. The need for further consideration of such goals and guidelines has been emphasized and proven, given the European integration aspirations of the Ukrainian people and other significant factors.

The issue of administrative and legal principles for countering threats to the economic security system of Ukraine, which may arise as a result of operations with digital assets, have been considered, namely: the appropriate term have been developed and the classification of the latter has been proposed. The need for sustainable and comprehensive improvement of such foundations, taking into account the potential of digital means, has been well-argued.

It has been found that the competence of some state bodies at the current state-building stage involves the processes regulated by existing administrative and legal principles. It has been proven that the following institutions are the most important among them: 1) the Ministry of Statistics; 2) the State Financial Monitoring; 3) the National Securities and Stock Market Commission; 4) the National Bank of Ukraine; 5) the law enforcement agencies (the Bureau of Economic Security of Ukraine, the Bureau of Economic Security of Ukraine, the National Anti-Corruption Bureau of Ukraine, the Security Service of Ukraine). The role of the FATF, as a subject of international law, has been specially noted. The problems of the levels and directions

of functioning of the above-mentioned leading institutions in this area have been highlighted.

The important role of consolidating efforts to combat legalized and other forms of digital assets has been emphasized. The concept of such interaction has been represented, the signs have been defined, the goal and tasks have been outlined, and their implementation has been designed to ensure the achievement of all the set goals. The existing mechanisms of interaction with the participation of the proposed main subjects have been studied.

Attention is focused on the importance of effective and efficient control and supervision in relation to the participants of legalized and other markets of digital assets, as well as some subjects involved in regulatory measures regarding the specified sphere. It has been emphasized that the application of appropriate mechanisms, in addition to preventive steps, can also contribute to the detection of gaps, collisions and other deficiencies.

A review and comparative analysis of international (ESMA, EU, ECB, FATF, OECD) and leading foreign models (Australia, Bahamas, Bermuda, United Kingdom, Canada, China, Sweden, United Arab Emirates, Kazakhstan, Cyprus, Malta, Moldova, Singapore, Philippines, United States of America, Germany, France, Switzerland, Japan, etc) for countering threats that may arise as a result of operations with digital assets have been carried out. It has been emphasized that the international community reached a new level of development of unified approaches to the regulation of relations that arise during the turnover of some types of digital assets. It has been noted that the problem of threats from operations with digital assets has been covered in a fragmentary way and is in the process of formation.

Attention has also been paid to the models of some foreign countries, which have certain achievements along such a vector. A range of the most common threats from transactions with digital assets, on the basis of the analysis of such practices, has been formed (cyber threats, legalization of income obtained by illegal means, insufficient research into such means and their rapid progression according to various characteristics, fraud, other factors, phenomena, as well as trends).

The priority vectors for the development of administrative and legal regulation to counter threats to the economic security system of Ukraine that may arise as a result of operations with digital assets have been outlined: 1) development of a favorable theoretical, methodological and methodological basis; 2) formation of legal foundations for further development of the economic security system of Ukraine and mechanisms; 3) resolution of the issue of delimitation of competence and strengthening the role of most subjects of the economic security system of Ukraine. Taking into account the national legislative security realities, the correctness and timeliness of improving the relevant established approaches are emphasized and substantiated. Taking into account the negative law-making experience of the foreseeable past, the need to follow the given guidelines is proved with arguments.

The ways of priority development of administrative and legal support for countering threats to the economic security system of Ukraine that may arise as a result of transactions with digital assets, taking into account the experience of foreign countries, have been identified. In particular, within the framework of developing a favorable theoretical, methodological and methodological basis, it is about: 1) carrying out comprehensive typological studies by subjects competently related to the analyzed area, as well as by interested higher education institutions; 2) developing a mechanism for auditing the effectiveness of the national financial system to assess the destructive impact of digital means and conducting events of the same name; 3) creating working groups with the participation of authorized subjects of public and legal relations, as well as representatives of the domestic and foreign professional community to highlight and analyze problematic issues in this area, strengthening various, including non-legal, forms of interaction between law enforcement entities.

Regarding the formation of legal foundations for the further development of the economic security system of Ukraine and mechanisms for responding to factors, phenomena, and trends of digital origin, the following steps are being taken: 1) accumulation of the results of typological studies, the results of the audit of the effectiveness of the national financial system, the results of discussions within the framework of interdepartmental analysis of problematic issues, proposals and

conclusions of the committees of the Verkhovna Rada of Ukraine; 2) formation of the basis for the development of draft laws and other regulatory legal acts; 3) adoption (approval) of legislative acts that will ensure the further development of the economic security system of Ukraine and the development of new and improvement of existing mechanisms for responding to relevant stimuli. Regarding the resolution of the issue of delimiting the competence and strengthening the role of most entities of the economic security system of Ukraine (personified bodies), by outlining clear intentions to improve their administrative and legal status, we should talk about the following final measures: 1) on the basis of the formed legal basis, to substantively work out the issue of strengthening the administrative and legal position of entities with special competence and some other institutions, in order to bring the tasks and functions of such bodies into clear compliance with the guidelines of the economic security system of Ukraine; 2) comprehensive and complete study of international standards and models, as well as the practices of foreign states; 3) development of proposals and recommendations for amendments to the current legislation, which will form a comprehensive and balanced administrative and legal support for the specified sphere. It has been proven that the consistent and unwavering implementation of such methods is an indispensable prerequisite for developing comprehensive administrative and legal support to counter threats to the economic security system of Ukraine that may arise as a result of transactions with digital assets.

Key words: administrative and legal principles, administrative and legal regulation, assets, interaction, means, economic security, methods, mechanism, control, supervision, directions, law enforcement agencies, levels, subjects, trends, digital economy, digital innovations and technologies, forms, factors, phenomena.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Слабунова Ю., **Кіяшко Ю.**, Глушко М. Значення діяльності місцевих загальних судів щодо захисту прав громадян у контексті протидії економічній злочинності як загрозі фінансовій стабільності України. *Правові горизонти*. 2019. Вип. 17 (30). С. 93–97. DOI: <http://www.doi.org/10.21272/legalhorizons.2019.i17.p:81>.

2. Кіяшко Ю. До питання визначення поняття «взаємодія суб'єктів системи економічної безпеки України» як об'єкта правового регулювання. *Юридичний науковий електронний журнал*. 2021. № 12. С. 37–40. DOI: <https://doi.org/10.32782/2524-0374/2021-12/5>.

3. Nekrasov, V., Mel'nyk, V., Kryvosheiev, K., **Kiiashko, Yu.**, Yemets, O. Interaction of law enforcement authorities as the basis of effective combating economic crime. *Journal of Law and Political Science*. 2021. Vol. 29. Iss. 4. P. 366–385 (*Web of Science*).

4. Кіяшко Ю. Поняття «системи економічної безпеки України»: адміністративно-правовий вимір. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2022. № 1. DOI: <https://doi.org/10.25313/2520-2308-2022-1-7882>.

5. Кіяшко Ю. Пріоритетні загрози системі економічної безпеки України в умовах воєнного часу: концептуальні погляди на характер та їхню типологізація. *Аналітично-порівняльне правознавство*. 2024. № 5. С. 507–513. DOI: <https://doi.org/10.24144/2788-6018.2024.05.80>

6. Кіяшко Ю. Правові засади взаємодії щодо протидії деяким загрозам економіці, які можуть виникати внаслідок операцій із цифровими активами. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2024. № 12. DOI: <https://doi.org/10.25313/2520-2308-2024-12-10540>.

які засвідчують апробацію матеріалів дисертації:

7. Гаруст Ю., **Кіяшко Ю.** Ціннісний аспект взаємодії суб'єктів забезпечення системи економічної безпеки України. *Реформування правової*

системи в контексті євроінтеграційних процесів: матеріали IV Міжнародної науково-практичної конференції: у 2-х ч. (Суми, 21–22 трав. 2020 р.). Суми: СумДУ. 2020. Ч. 1. С. 65–69.

8. Кіяшко Ю. Роль та значення взаємодії суб'єктів правоохоронної діяльності з питань протидії явищу економічної злочинності. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали V Міжнародної науково-практичної конференції (Суми, 20–21 трав. 2021 р.). Суми: СумДУ. 2021. С. 446–450.

9. Кіяшко Ю. До питання визначення поняття методів взаємодії суб'єктів системи економічної безпеки України. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали V Міжнародної науково-практичної конференції (Суми, 20–21 трав. 2021 р.). Суми: СумДУ. 2021. С. 474–478.

10. Кіяшко Ю. До питання доцільності та методологічної обґрунтованості використання в науковому обігу категорії «система економічної безпеки України». *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти*: збірник наукових праць з матеріалами III Міжнародної наукової конференції (Дніпро, 6 верес. 2024 р.). Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп». 2024. С. 69–71.

11. Кіяшко Ю. Цифрові інструменти у системі засобів впливу на темпи і характер перебігу економічних безпекових процесів. *Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference, (September 20 2024, Bern)*. Swiss Confederation: International Center of Scientific Research. P. 75–77.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ.....	17
ВСТУП.....	19
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ПРОТИДІЇ ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК ОПЕРАЦІЙ ІЗ ЦИФРОВИМИ АКТИВАМИ.....	35
1.1. Система економічної безпеки України як об’єкт публічно-правового забезпечення.....	35
1.2. Теоретико-правова характеристика категорії «цифрові активи»: поняття, ознаки, властивості та оцінка підходів щодо розуміння її форм.....	49
1.3. Поняття, властивості, ознаки й класифікація загроз системі економічної безпеки України та місце і роль серед них цифрової складової.....	72
1.4. Міжнародні й іноземні стандарти та правові механізми з протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами	88
Висновки до розділу 1	95
РОЗДІЛ 2 АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК ОПЕРАЦІЙ ІЗ ОБОРОТУ ЦИФРОВИХ АКТИВІВ.....	99
2.1. Адміністративно-правові засади з протидії загрозам системі економічної безпеки України, що виникають при проведенні операцій із цифровими активами	100
2.2. Адміністративно-правовий статус суб’єктів системи економічної безпеки України зі спеціальною компетенцією, що протидіють загрозам, які виникають при здійсненні операцій із цифровими активами.....	112
2.3. Адміністративно-правовий механізм взаємодії суб’єктів зі спеціальною компетенцією з протидії загрозам економічної безпеки України, що виникають	

під час здійснення операцій із цифровими активами.....	125
2.4. Правові основи здійснення державного контролю та нагляду при проведенні операцій із цифровими активами.....	136
Висновки до розділу 2	142
РОЗДІЛ 3 ПРІОРИТЕТНІ НАПРЯМИ РОЗБУДОВИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ З ПРОТИДІЇ ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК ОПЕРАЦІЙ ІЗ ЦИФРОВИМИ АКТИВАМИ.....	147
3.1. Огляд і компаративний аналіз міжнародних та провідних закордонних моделей щодо протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами	147
3.2. Окреслення першочергових векторів для розбудови комплексного адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами	162
3.3. Шляхи реалізації напрямів формування комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами з урахуванням досвіду іноземних країн	169
Висновки до розділу 3	185
ВИСНОВКИ.....	187
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	206
ДОДАТКИ	249

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

БЕБ – Бюро економічної безпеки України

Велика Британія – Сполучене Королівство Великої Британії та Північної Ірландії

ДБР – Державне бюро розслідувань

Держфінмоніторинг – Державна служба фінансового моніторингу України

ESMA – Європейське управління з цінних паперів і ринків (European Securities and Markets Authority)

ЄС – Європейський Союз, Євросоюз

ЗВА (ВЦ) – забезпечені віртуальні активи валютними цінностями

ЗВО – заклади вищої освіти

FATF – Міжнародна група з протидії відмиванню брудних грошей (Financial Action Task Force on Money Laundering)

КК України – Кримінальний кодекс України

КМ України – Кабінет Міністрів України

Керівництво FATF – Керівництво FATF з ризик-орієнтованого підходу віртуальні активи та постачальники послуг з переказу віртуальних активів від 2019 року

Концепція – Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки

Регламент МіСА – Регламент (ЄС) 2023/1114 Європейського Парламенту та Ради від 31 травня 2023 року про ринки криптоактивів, а також про внесення змін до Регламентів (ЄС) № 1093/2010 та (ЄС) № 1095/2010 та Директив 2013/36/ЄС та (ЄС) 2019/1937 (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)

Мінфін – Міністерство фінансів України

Мінцифри – Міністерство цифрової трансформації України

НАБУ – Національне антикорупційне бюро України

НАТО – Організація Північноатлантичного договору (North Atlantic Treaty Organisation)

НКЦПФР – Національна комісія з цінних паперів та фондового ринку

НП – Національна поліція

ОАЕ – Об'єднані Арабські Емірати

ООН – Організація Об'єднаних Націй (United Nations)

ОЕСД – Організація економічного співробітництва та розвитку (Organisation for Economic Cooperation and Development)

План заходів щодо реалізації Концепції – План заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки

СБУ – Служба безпеки України

Стратегія економічної безпеки України – Стратегія економічної безпеки України на період до 2025 року від 11 серпня 2021 р. № 347/2021

Стратегія національної безпеки України – Стратегія національної безпеки України «БЕЗПЕКА ЛЮДИНИ – БЕЗПЕКА КРАЇНИ» від 14 вересня 2020 р. № 392/2020

США – Сполучені Штати Америки

абз. – абзац

пп. – підпункт

п. – пункт

ст. – стаття

с. – сторінка

табл – таблиця

ч. – частина

ВСТУП

Обґрунтування вибору теми дослідження. Реалії цифрового десятиліття на фоні існуючих стрімко прогресуючих і потенційних викликів, загроз та ризиків для усталених засад міжнародного миру й безпеки [367] зумовлюють потребу належної оцінки потенціалу цифрових засобів ураження. Досвід осяжного минулого наочно [166; 368] продемонстрував істотні організаційні, правові, управлінські, технічні й технологічні обмеженості щодо ефективного й результативного реагування на відповідні прояви деструкції. Об'єктивна та хронічно запізнiла реакція на такий спектр подразників провокує українське суспільство предметно і всебічно підходити до розв'язання цієї проблеми, аби не допустити чи мінімізувати можливі випадки радикальних потрясінь.

Україна, вимушено перебуваючи в епіцентрі впливу від наслідків знакових геополітичних та геоекономічних трансформацій, на третій рік повномасштабного вторгнення має системно посилювати безпековий напрям, фактично не маючи інших конструктивних альтернатив. Усвідомлення невідворотного експоненціального за темпами розвитку, формами об'єктивізації, а також масштабами розповсюдження і ступенем залученості у різні сфери життєдіяльності цифрових активів, окрім явних переваг, дає також підстави розглядати їх із позиції загрозливості. Серед найуразливіших аспектів виділяється питання руйнівного впливу щодо стійкого функціонування системи економічної безпеки України. Численні авторитетні наукові доробки [176; 177; 369], джерела міжнародного права [183; 136], а також різного типу й походження аналітичні звіти [182; 81] містять аргументовані доводи реалістичності істотного впливу цих чинників, тенденцій і явищ. Наприклад, абз. 1 Розділу 1 «Вступ: кібербезпечна цифрова трансформація в складному середовищі загроз» «Стратегії кібербезпеки ЄС на цифрове десятиліття» (The EU's Cybersecurity Strategy) від 2020 р. прямо вказано, що економіка, демократія та суспільство європейської спільноти як ніколи залежать від безпеки та надійності цифрових інструментів та підключень. Окремі висновки

Звіту «Регулювання цифрових активів: Інсайти юрисдикційних підходів», оприлюдненого у жовтні 2024 р., також указують на ряд загроз саме для економічної компоненти. Тому для української економіки, яка складно перенесла наслідки від пандемії COVID-19» [370], спричиненої коронавірусом «SARS-CoV-2», й переорієнтувалась на задоволення безпрецедентного обсягу воєнних і гуманітарних потреб, украй важливо, ще при відсутності колосального попиту на цифрові активи, підготуватися до нових реалістичних загроз. Беручи до уваги зростання кількості методів гібридної агресії та поточний стан *(на екваторі третього року повномасштабного вторгнення, лише за попередніми оцінками, сумарно українська економіка втратила орієнтовно біля 20 % потенціалу. Трудові ресурси скоротилися на 20 – 25 %, зростання зовнішнього боргу досягло понад 41 %, «ослаблення» гривні дорівнює 37 %, загальна інфляція склала близько 31 % [143])*, ініційована необхідність є своєчасною та виправданою.

Слід зауважити, що на стратегічному безпековому рівні було точково звернено увагу відносно таких позицій. П. 9 Стратегії національної безпеки України «Безпека людини – безпека країни» (далі – Стратегія національної безпеки України) та абз. 3 п. 18 Стратегії економічної безпеки України на період до 2025 року (далі – Стратегія економічної безпеки України) засвідчують наміри щодо реагування на відповідні подразники. Однак, такі вказівки можна розглядати як суто декларативні, адже відсутні конкретні кроки й порядки їх реалізації. До того ж, певні категорії не мають офіційного визнання й семантично охоплюють ширше коло об'єктів матеріальної і нематеріальної площин. Такий підхід іде в розріз усталеним принципам правозастосування [371], призводячи до колізій, прогалин та інших невизначеностей. У результаті чого, це негативно впливає на стан реалізації провідних концепцій із цифрового розвитку економіки, що має наслідком неефективне використання коштів платників податків, а також ресурсів і послуг, отриманих в рамках гуманітарної й міжнародної технічної допомог.

Зв'язок теми дисертації із сучасними дослідженнями. Окреслена

проблематика носить концептуальний, малодосліджений і перспективний характер. Серед найвагоміших здобутків виділимо наукові підходи з таких фундаментальних позицій: 1) система економічної безпеки України як об'єкт публічно-правового і колективного суспільного забезпечення: Ю. Гаруст [6, с. 267; 7, с. 391], А. Гуменюк [43, с. 55-56], О. Дацко [44, с. 86; 45], С. Завгородня [46, с. 84; 47, с. 11-12; 48, с. 21], В. Мельник [49, с. 361-362; 60, с. 26; 51; 52, с. 3, 129, 146-147, 223, 398], Н. Морозюк [53], І. Ревак [54, с. 33; 55, с. 61], В. Сазонов [56, с. 97, 100; 57, с. 6, 11, 20-21; 58], В. Сухонос, В. Сухонос і О. Сластьоненко [59, с. 29-30]); 2) підходи до розуміння категорії «цифрові активи»: О. Adekoya й Е. Екпо [72, с. 3], В. Бацуца [100, 34-35; 93, с. 46-47], J. P. Buntinx [76], О. Даниленко [101, с. 152-153], О. Кудь [78, с. 2-3, 6, 7-8], Н. Кучерявенко, Д. Білінський й Є. Смичок [77, с. 7-8, 31, 128], W. S. Li [75 с. 76-77], E. Harbinja [74, с. 102], S. van Eup і J. Uitdehaag [81, с. 17, 21], M. D. Walker [73, с. 53]; 3) типові форми цифрових активів: В. Бацуца [133, с. 85, 86-87; 93, с. 86-87], О. Бутніка-Сіверський [104, с. 98], І. Гулейков [112, с. 213-214], Б. Гурін [113, с. 7-8], О. Дмитрик [114, с. 250-251, 252], О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенко, Д. Білінський і Є. Смичок [77, с. 7-8, 31, 128], А. Овчаренко [115, с. 201-202], А. Проценко [116, с. 131, 133-134]; 4) загрози системі економічної безпеки України: О. Діденко [149], М. Єрмошенко [150], С. Завгородня [151, с. 44], В. Онищенко й І. Рева [152, с. 7], Л. Шевченко [153, с. 17]; 5) роль цифрової складової у структурі загроз системі економічної безпеки України: R Auer і S. Claessens [171], А. Боровик, І. Клопотун [340, с. 207-208], D. Cumming, Z. Glatzer і O. Guedhami [176], М. Думчиков [356, с. 160-162; 57, с. 249-250, 270-271], М. Isogawa [178], А. Максименко [166, с. 43, 44], В. Mizrach [177], S. K. Muthusamy і R. Kannan [166], А. Стеблянко [294, с. 91; 247, с. 42, 92, 211], S. Foley, К. Jonathan R., Р. Talis J. [172]; 6) адміністративно-правові основи функціонування суб'єктів системи економічної безпеки України, що є визначальними для характеру впливу на регульовані відносини:

В. Авер'янов [223, с. 110], Ю. Битяк, В. Гаращук, О. Дьяченко та Н. Писаренко [226, с. 42], В. Галуцько, В. Курило, С. Короєд й О. Дрозд [362, с. 98-99], Т. Коломоєць [326, с. 58; 363, с. 37-38], В. Колпаков і О. Кузьменко [364, с. 207], К. Костовська, Ю. Назар та В. Серєда [224, с. 27], Р. Мельник і В. Бєвзенко [225, с. 61] та багато інших.

Вагоме значення у формуванні теоретико-методологічної основи також відіграли документи міжнародного походження, у тому числі – дорадчого й інформативно характеру (ESMA, ЄС, ЄЦБ, FATF, OECD) і правові норми регулятивних актів іноземних країн (Багамські Острови, Бермудські Острови, Велика Британія, Канада, Китай, ОАЕ, Сінгапур, США, Франція, Швейцарія, Японія та ін.).

Викладене вище дає аргументовані підстави вважати обрану тему дисертаційного дослідження як актуальною й такою, що об'єктивно потребує комплексної науково-дослідної розробки. Попри те, що адміністративно-правові механізми закріплені чинним законодавством, вони орієнтовані лише на частину форм цифрових активів і мають обмежений функціонал. Результати, отримані в рамках репрезентованого доробку, можна буде використати для розбудови відповідного нормативно-правового забезпечення, слідуючи міжнародним стандартам і враховуючи підходи іноземних держав.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження відповідає меті та завданням законів України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII, «Про стимулювання розвитку цифрової економіки в Україні» від 15 липня 2021 р. № 1667-IX, Цілям сталого розвитку України на період до 2030 року, від 30.06.2019 р. № 722/2019, Стратегії національної безпеки України «Безпека людини – безпека країни» від 14 вересня 2020 р. № 392/2020, Стратегії економічної безпеки України на період до 2025 року від 11 серпня 2021 р. № 347/2021, Національній економічній стратегії на період до 2030 року від 3 березня 2021 р. № 179, Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на

період до 2025 року від 17 листопада 2021 р. № 1467-р, Стратегії відновлення, сталого розвитку та цифрової трансформації малого і середнього підприємництва на період до 2027 року від 30 серпня 2024 р. № 821-р., Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки від 17 січня 2018 р. № 67-р., а також Стратегії розвитку наукових досліджень Національної академії правових наук України на 2021–2025 роки (п. п. 1.2, 1.7, 1.8, 1.10–1.12).

Окремі підсумки, що оприлюднені в дисертаційному доробку були отримані під час виконання науково-дослідних робіт у рамках наступних проєктів: 1) «Удосконалення системи правоохоронних органів щодо забезпечення фінансово-економічної безпеки України» (номер д. р. 0116U006814); 2) «Концепція нової інноваційної моделі державного управління фінансовою системою України» (номер д. р. 0118U003582); 3) «Розробка «Концепції запровадження державної системи контролю за залученням та ефективним використанням міжнародної технічної допомоги в Україні на 2021-2025 рр.» (номер д. р. 2020.02/0137); 4) «Концептуальні засади реформування системи правоохоронних органів в сучасних умовах трансформації нагляду і контролю щодо забезпечення економічної безпеки України» (номер д. р. 0122U000779). Дисертацію виконано відповідно до плану науково-дослідних робіт Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер д. р. 0120U105390).

Тему дисертації затверджено рішенням Вченої ради Науково-дослідного інституту публічного права від 10 жовтня 2023 року (протокол № 13).

Мета та завдання дослідження. *Мета* дисертаційного дослідження полягає у тому, щоб, спираючись на аналіз наукових поглядів вчених та норм чинного законодавства, з'ясувати сутність та особливості адміністративно-правового забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. На основі узагальнення позитивного вітчизняного та зарубіжного досвіду

встановити напрями розвитку правових та організаційних засад здійснення відповідної діяльності, розробити ефективне теоретико-методологічне, методичне та правове підґрунтя для розбудови комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Керуючись орієнтирами пропонованої мети, було сформульовано наступний спектр завдань:

- дослідити категорію «система економічної безпеки України» крізь призму об'єкта публічно-правового забезпечення;
- здійснити теоретико-правову характеристику цифрових активів, сформулювавши поняття, окресливши властивості та ознаки, а також оцінивши підходи щодо розуміння її форм;
- визначити поняття, властивості, ознаки й висвітлити точки зору щодо класифікації загроз системі економічної безпеки України, а також з'ясувати місце і роль серед них цифрової складової;
- розкрити тематику виняткової важливості міжнародних й іноземних стандартів і правових механізмів із протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами та оцінити їхній вплив на результати національної правотворчості;
- окреслити та класифікувати адміністративно-правові засади з протидії загрозам системі економічної безпеки України, що виникають при проведенні операцій із цифровими активами;
- схарактеризувати адміністративно-правовий статус суб'єктів системи економічної безпеки України зі спеціальною компетенцією, що протидіють загрозам, які виникають при здійсненні операцій із цифровими активами крізь призму рівнів і напрямів їх функціонального впливу;
- розкрити сутність адміністративно-правового механізму взаємодії суб'єктів системи економічної безпеки України зі спеціальною компетенцією, що можуть виникати внаслідок операцій із цифровими активами;
- опрацювати питання здійснення державного контролю та нагляду

при проведенні операцій із цифровими активами;

– здійснити огляд і провести компаративний аналіз міжнародних та провідних закордонних моделей щодо протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами;

– окреслити першочергові вектори для розбудови адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати при проведенні операцій із цифровими активами;

– запропонувати й обґрунтувати доцільність шляхів реалізації напрямів формування комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами з урахуванням досвіду іноземних країн.

Об'єкт дослідження становлять суспільні відносини, що виникають під час реалізації заходів із протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій з цифровими активами.

Предметом дослідження є адміністративно-правові засади з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій з цифровими активами.

Методи дослідження. У ході опрацювання автором було використано ряд загальнонаукових і спеціальних методів наукового пізнання (на емпіричному й теоретичному рівнях). Застосування вказаних методів, у межах *емпіричного рівня*, забезпечило вибірку й компонування фактів про узагальнений стан системи економічної безпеки України в умовах активної дії безпрецедентно широкого спектра загроз, у тому числі цифрового походження. На основі підсумків спостережень, аналізу та узагальнення відомостей і статистичних даних висловлено мотивовану гіпотезу про істотний потенціал й широкий прогресуючий функціонал цифрових засобів ураження.

В межах такого рівня було застосовано наступні загальнонаукові методи: 1) спостереження; 2) порівняння; 3) моделювання. За допомогою методу *спостереження*, на основі статистичних даних, міркувань учених і публічних

діячів, а також, керуючись власними судженнями, зроблено висновок про складний поточний економічний стан української держави, що може бути основою для продукування низки ризиків для оборонного потенціалу країни (Розділ 1). Використання методу *порівняння* надало змогу співставити думки вчених і відомих діячів щодо міри складності руйнівного впливу на економічне середовище та темпів розвитку окремих тенденцій, продиктованих цифровими інноваціями й технологіями (підрозділи 1.2, 1.3). Метод *моделювання* забезпечив умови для прогнозування економічного становища в осяжному майбутньому, у тому числі – завдяки фактичним відомостям і статистичній інформації (підрозділи 1.3, 3.2).

Щодо *теоретичного рівня*, то автором було використано наступний спектр методів: 1) індукції; 2) дедукції; 3) синтезу; 4) прогнозування. Метод *індукції* був використаний для узагальнення наукових результатів, присвячених питанням змістовного наповнення центральних дефініцій, використовуваних у роботі (Розділи 1, 2). Застосування методу *дедукції* надало можливість всебічно дослідити категорії, що становлять предметний інтерес і важливі для досягнення мети представленої тематики (Розділи 1, 2). Використання методу *синтезу* надало змогу довести гіпотезу про необхідність виокремлення й конкретизації ключових загроз системі економічної безпеки України на сучасному етапі. Також його властивості забезпечили обґрунтування доцільності розгляду питання про позиціонування чинників, явищ і тенденцій цифрового походження в якості загроз економічній безпековій складовій (підрозділи 1.4, 1.3, Розділ 3). Це було досягнуто шляхом вивчення й аналізу кожної з їхнього числа та з урахуванням фахових оцінок щодо уразливості економічної складової в нинішній період. Його опосередкований вплив мав місце під час обґрунтування авторського судження про необхідність розробки теоретико-методологічного, методичного та правового забезпечення щодо комплексної протидії цим загрозам. Метод *прогнозування* було використано для обґрунтування доцільності й своєчасності подальшої наукової розробки цієї тематики, зважаючи на існуючу обстановку, зокрема нечіткість і

непослідовність кроків та орієнтирів, а також прогалини у стратегічних актах. Також використання його функціональних можливостей дало змогу обґрунтувати доцільність внесення змін у документи з метою поступальної й збалансованої державної правової політики щодо формування теоретико-методологічного, методичного та юридичного підґрунтя для стійкої розробки відповідного напрямку.

Стосовно спеціальних методів наукового пізнання, було використано наступні: 1) аксіоматичний; 2) еволюційної епістемології; 3) формально-юридичний. Застосування *аксіоматичного* методу надало можливість виходити з розуміння існування усталених засад регламентації відносин із питань протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій з цифровими активами (Розділ 2). Метод *еволюційної епістемології* сприяв усвідомленню базових орієнтирів розвитку національної безпекової політики (Розділи 1, 3). *Формально-юридичний* метод надав змогу здійснити аналіз норм права з протидії загрозам системі економічної безпеки, що можуть виникати внаслідок операцій з цифровими активами в Україні, на міжнародній арені та в іноземних державах (Розділи 1–3).

Сукупно вказані методи забезпечили розробку пропозицій і рекомендацій щодо розбудови комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Такі ініціативи у перспективі мають забезпечити посилення вітчизняного безпекового потенціалу і поглибити інтеграційні процеси.

Науково-теоретичне підґрунтя для виконання дисертації склали праці вітчизняних та іноземних учених у багатьох галузях наук (економічних, міждисциплінарних, обчислювальних, правових, фінансів та ін.).

Нормативну основу сформували Конституція України, міжнародні договори (в тому числі угоди, конвенції, протоколи та ін.), а також приписи рекомендаційного характеру, закони та підзаконні нормативно-правові акти (зокрема, накази, постанови, рішення тощо) й стратегічні документи з питань

забезпечення функціонування системи економічної безпеки України.

Інформаційний та емпіричний бази утворили узагальнення й практики роботи державних, міжнародних і закордонних установ, що функціонують на різних рівнях. Також взято до уваги аналітичні матеріали, довідкові видання, статистичні й інші відомості, що розміщені в публічному доступі.

Наукова новизна отриманих результатів полягає в тому, що дисертаційне дослідження є однією із перших спроб комплексно, на монографічному рівні, з використанням методів наукового пізнання і наявних досягнень правничої науки сформулювати теоретико-методологічне, методичне та правове підґрунтя для розбудови комплексного й збалансованого адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. За результатами виконаного дослідження отримано ряд положень та висновків, запропонованих дисертантом особисто. До числа найбільш вагомих пропонується віднести наступні:

вперше:

– змістовно й аргументовано розкрито потенціал цифрових активів із позиції загрозовості деяких технологій та інновацій стійкому функціонуванню системи економічної безпеки України. Доведено, що їх варто розглядати під такими кутами зору: 1) блага з унікальними ідентифікаційними (буквено-числовими) кодами, що існують у цифровій формі й перебувають в обороті виключно у цифровому середовищі, мають цінність і вартісну визначеність у платіжній, інших матеріальних і нематеріальних формах та можуть використовуватися необмежним колом осіб; 2) широкий, непрогнозовано змінний спектр типів об'єктів нематеріального змісту, що існують у цифровій формі й обертаються в цифровому середовищі; 3) прояв прав власності (володіння, користування, розпорядження), що передбачають оперування об'єктами нематеріального змісту у цифровому середовищі, в тому числі переважно безперешкодного доступу до них, незалежно від волі інших учасників відносин, зокрема й держави та суб'єктів міжнародного права; 4) у

залежності від намірів, різновидів засобів і способів підвищення або зниження рівня ефективності функціонування установ, підприємств, організацій та діяльності суспільства. Визначено властивості та ознаки цих активів, проаналізовано поширені підходи до розуміння їх типологізації (форм прояву);

– усвідомлено й доведено руйнівний потенціал загроз цифрового походження для стійкого функціонування системи економічної безпеки України на основі різного типу аналітичних матеріалів (звітів, інформаційних довідок, пояснювальних записок, роз'яснень, тлумачень тощо), міркувань визнаних дослідників та власних напрацювань;

– представлено й класифіковано суб'єктів із протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами на основі критерію меж компетенції установ (загальна та спеціальна). До носіїв загальної компетенції віднесено наступні суб'єкти: 1) Верховна Рада України; 2) Президент України та Рада національної безпеки і оборони України; 3) Кабінет Міністрів України, Міністерство економіки України, Міністерство фінансів України та інші центральні органи виконавчої влади; 4) суди (місцеві загальні суди, відповідні апеляційні суди, Верховний Суд (Касаційний кримінальний суд, Велика Палата Верховного Суду); 5) та ін. Перелік суб'єктів зі спеціальною компетенцією запропоновано представити у такому складі: 1) Міністерство цифрової трансформації України; 2) Міжнародна група з протидії відмивання брудних грошей; 3) Державна служба фінансового моніторингу України; 4) Національна комісія з цінних паперів та фондового ринку; 5) Національний банк України; 6) правоохоронні органи (Бюро економічної безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України, Національна поліція, Служба безпеки України);

– сформульовано авторське бачення дефініції «взаємодія суб'єктів із питань протидії деяким загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами», як: 1) разове, тривале чи системне вжиття спільних заходів відповідними суб'єктами системи

економічної безпеки України з метою протидії загрозам, що можуть виникати внаслідок операцій із цифровими активами, шляхом реалізації управлінських форм і методів та у способи, що не суперечать нормам чинного законодавства;

2) санкціонований вплив одного суб'єкта на іншого (чи декількох) для приведення у відповідність нормам законів і підзаконних нормативно-правових актів заходів, у тому числі недопущення зловживань із питань протидії аналізованим чинникам, явищам, а також тенденціям. Визначено ознаки відповідної категорії, з'ясовано мету і завдання однойменної діяльності;

– окреслено та обґрунтовано першочергові вектори розбудови комплексного адміністративно-правового забезпечення (1) розробка сприятливого теоретико-методологічного та методичного підґрунтя;

2) формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів реагування на чинники, явища та тенденції цифрового походження; 3) вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів), шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу);

удосконалено:

– розуміння важливості стійкого ефективного й результативного публічного-правового забезпечення функціонування системи економічної безпеки України, з огляду на безпекову ситуацію в країні, конституційні основи та виключної безальтернативної ролі для стійкості й темпів перебігу багатьох суспільних процесів;

– бачення адміністративно-правових засад з протидії загрозам системі економічної безпеки України, що виникають при проведенні операцій із цифровими активами. Встановлено, що такі основи являють собою сукупність норм адміністративного права, об'єктивованих у нормативно-правових актах різної юридичної сили, які визначають мету, завдання, принципи, функції та інші адміністративно-правові способи та засоби, за допомогою яких здійснюється регулювання предметної сфери відносин. Запропонована

наступна їх класифікація: 1) Конституція України; 2) міжнародні договори України; 3) закони; 4) підзаконні нормативно-правові акти;

– розуміння специфіки адміністративно-правового регулювання протидії деяким загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами, встановивши, що ключовими його атрибутами є: 1) адміністративно-правові засади; 2) суб'єкти; 3) взаємодія цих суб'єктів; 4) контроль та нагляд у предметній сфері;

– переконання про важливість міжнародних й іноземних стандартів із протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами та необхідність швидшого приведення у відповідність національних адміністративно-правових засад;

дістали подальшого розвитку:

– вчення про категорію «система економічної безпеки України» як багатоаспектну, складну, соціальну систему, яка включає в себе численний неоднорідний елементний склад, сполучений широким спектром зв'язків та орієнтований на постійну ефективну й результативну реалізацію заходів за такими напрямками: 1) збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній; 2) забезпечення здатності конкурентоспроможності лівової частки вітчизняних економічних галузей у світі; 3) сприяння поступальному розвитку всього економічного сектору. Також визначено її властивості, ознаки, мету, завдання та проаналізовано структуру;

– досліджувані супутні категоріальні одиниці (адміністративно-правові засади, адміністративно-правовий механізм, адміністративно-правовий статус, взаємодія, загрози, загрози системі економічної безпеки України, контроль, нагляд, напрями, рівні та ін.);

– адміністративно-правовий статус суб'єктів зі спеціальною компетенцією (Міністерство цифрової трансформації України, Міжнародна група з протидії відмиванню брудних грошей, Державна служба фінансового моніторингу України, Національна комісія з цінних паперів та фондового

ринку, Національний банк України, правоохоронні органи (Бюро економічної безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України, Національна поліція, Служба безпеки України)) у сфері протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами;

– питання форм контролю та нагляду у сфері обороту деяких типів цифрових активів у виконанні уповноважених центральних органів виконавчої влади, Міжнародної групи з протидії відмиванню брудних грошей та Національного банку України;

– міжнародні й провідні закордонні моделі, правові механізми та стандарти щодо протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами, оцінено їхній вплив на вітчизняну правотворчість, а також перспективні механізми з позиції імплементації до національного законодавства.

Особистий внесок здобувача в одержанні наукових результатів у дисертації. Дослідження виконано автором самостійно з урахуванням, а також із використанням сучасних наукових здобутків. Розроблені та сформульовані положення й висновки роботи отримані дисертантом особисто.

У науковій статті «Значення діяльності місцевих загальних судів щодо захисту прав громадян у контексті протидії економічній злочинності як загрози фінансовій стабільності України», виконаній спільно з Ю. Слабуною та М. Глушко, особисто було проаналізовано проблематику ролі явища економічної злочинності, її детермінант, а також оцінено прогресуючий ефект останньої як однієї з суттєвих перешкод у можливості безперешкодної реалізації низки прав і законних інтересів фізичних осіб, а також інтересів юридичних осіб. На основі цього було також аргументовано наголошено щодо необхідності підвищення рівня ефективності функціонування досліджуваної ланки і спеціалізації судових органів у здійсненні правосуддя за відповідними юрисдикційними напрямками.

В дослідженні «Interaction of law enforcement authorities as the basis of

effective combating economic crime», підготовленому спільно з В. Некрасовим, В. Мельником, К. Кривошеєвим, О. Ємець, здобувачем було розкрито питання форм прояву економічної злочинності, виявлено тенденцію до стійкого зростання їхньої кількості та посилення руйнівного функціоналу. З'ясовано, що одним із каталізаторів цієї ситуації є саме непоодинокі цифрові інновації та технології, які формують нові й удосконалюють існуючі способи і засоби деструктивного впливу на характер та темпи перебігу багатьох економічних процесів. Окрім того, підкреслено, що протидія відповідним чинникам і явищам потребує консолідації інтелектуального та ресурсного забезпечення всіх уповноважених суб'єктів правоохоронної діяльності.

У доробку «Ціннісний аспект взаємодії суб'єктів забезпечення системи економічної безпеки України» опублікованому з Ю. Гарустом розкрито тему виняткової значимості спільної діяльності. Наголошується й доводиться, що такий формат роботи є вкрай необхідним для ефективної протидії маловідомим явищами, чинникам та тенденціям. Зауважено, що неналежна взаємодія істотно послабить функціонал держави у відповідних заходах, негативно впливаючи на всю безпекову обстановку.

Практичне значення отриманих наукових результатів полягає в тому, що вони можуть бути використані у:

- *науково-дослідній діяльності* – формують базис для подальшого пошуку шляхів із удосконалення законодавства в предметній сфері (акт впровадження Науково-дослідного інституту публічного права);
- *правозастосовній сфері* – для удосконалення практичних аспектів роботи основних та інших суб'єктів функціонально належних і дотичних до аналізованої сфери;
- *правотворчій діяльності* – при розробці проєктів нормативно-правових актів, які регулюють відносини з питань обороту багатьох форм цифрових активів;
- *освітньому процесі* – під час розроблення та викладання навчальної дисципліни «Адміністративне право та процес: доктринальні та практичні

проблеми» (акт впровадження Науково-дослідного інституту публічного права).

Апробація матеріалів дисертації. Підсумки розроблення проблеми в цілому, окремі її аспекти, одержані узагальнення і висновки було оприлюднено на науково-практичних конференціях: «Реформування правової системи в контексті євроінтеграційних процесів» (м. Суми, 21–22 травня 2020 р.), «Реформування правової системи в контексті євроінтеграційних процесів» (м. Суми, 20–21 травня 2021 р.), «Реформування правової системи в контексті євроінтеграційних процесів» (м. Суми, 20–21 травня 2021 р.), «Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти» (м. Дніпро, 6 вересня 2024 р.), «Modernization of science and its influence on global processes» (20 вересня 2024 р., м. Берн, Швейцарія).

Публікації. Основні результати дисертації, висновки та пропозиції знайшли своє відображення в одинадцяти наукових публікаціях, з яких п'ять статей в журналах, включених МОН України до переліку наукових фахових видань з юридичних наук, одна стаття – в науковому періодичному виданні, що індексується в наукометричній базі даних Web of Science; п'ять – тези доповідей і повідомлень на міжнародних науково-практичних конференціях та круглих столах.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, що включають одинадцять підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 253 сторінки. Робота містить список використаних джерел із 386 найменувань на 43 сторінках.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ПРОТИДІЇ ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК ОПЕРАЦІЙ ІЗ ЦИФРОВИМИ АКТИВАМИ

1.1. Система економічної безпеки України як об'єкт публічно-правового забезпечення

Економічний елемент у складній, багатогранній та усталеній структурі системи національної безпеки України упродовж усього періоду незалежності займає важливе місце й відіграє одну з провідних ролей [372, с. 71-72, 73; 373, с. 155; 10, с. 137]. Будучи матеріальною основою для стійкого і своєчасного перебігу низки процесів [52, с. 22, 113-114; 6, с. 167], він фактично забезпечує функціонування безпекового й оборонного секторів у межах власних спрямувань. Нетривала історія національного державотворення наводить ряд прикладів, коли саме завдяки дії економічної складової вдавалося послабити ефект або нівелювати дію наслідків від низки негативних факторів різного характеру, знецінювати деструктивні тенденції та в інші легальні способи забезпечувати необхідну фінансову стійкість країни у багатьох сферах [374]. Навіть при чинному правовому підході, об'єктивованому у Законі України «Про національну безпеку України» (п. 4 ч. 1 ст. 1) [1], Стратегії національної безпеки України (Розділи II, III та ін.) [2], Стратегії економічної безпеки України [3] та багатьох інших вітчизняних нормативно-правових актах, помилковим буде судження про відсутність взаємозалежності між національною безпекою України та її економічною складовою. На користь цієї теорії виступають і ряд відомих українських науковців, таких як В. Гарькава [4, с. 373-374; 5, с. 32, 40], Ю. Гаруст і В. Мельник [6, с. 167; 7], К. Колеснікова, І. Маліновська й В. Чабаров [8, с. 8], Д. Повзун [9, с. 93-94],

К. Утенкова [10, с. 133-134; 11, с. 40-41, 115-116] та ін., котрі аргументовано доводять репрезентовану точку зору. До того ж, розглянуті й проаналізовані результати зазначених наукових досліджень оприлюднені та схвалені відносно нещодавно, що є свідченням відповідності сучасним реаліям.

Консенсус у питаннях системної приналежності економічної складової формує єдину систему координат для змістовної характеристики відповідних категорій, залишаючи поза увагою діаметрально протилежні або точково скориговані міркування. Відповідно, слід відзначити про розробку понятійно-категоріального апарату в межах однієї парадигми сприйняття певних обставин, явищ і процесів.

Із цього можна зробити висновок, що предметна категорія налічуватиме всі властивості вихідного терміну – «безпека», котрий є методологічним базисом для вузькопрофільних понять різних рівнів (національна безпека України, державна безпека, воєнна безпека, інформаційна безпека, кібербезпека, інвестиційно-інноваційна безпека, макроекономічна безпека, фінансова безпека, банківська безпека, грошово-кредитна безпека та ін.). Аналізуючи фундаментальні роботи таких науковців, як В. Горбулін і Ю. Даник [12, с. 16-17], [13, с. 3-4], С. Пономарьов [14, с. 69-70; 15, с. 10; 16, с. 16-17], Kim R. Holmes [17, с. 23, 24-25] й інших з проблематики дисертаційного дослідження, є доцільним для повноти і всебічності представленої роботи сформулювати спільний підхід останніх до проблем національної безпеки. Так, відповідно до результатів їхніх наукових досліджень, у сучасній вітчизняній політико-правовій формації доцільно звернути увагу на такі аспекти, як: 1) спектр умов різного спрямування, при яких формується й певний час стійко існує відчуття в більшості колективу щодо відсутності активного впливу багатьох загроз і конвертації ключових ризиків у деструктивні фактори для нормальної життєдіяльності індивідів; 2) дійсна захищеність критичних сфер санкціонованої державою публічної охорони від впливу викликів, загроз і ризиків; 3) готовність і здатність у різні форми, методи та способи запобігати й протидіяти дії лівової частки викликам,

загрозам і ризикам для існуючого, колегіально схваленого стану речей у межах території, зазвичай, держави; 4) можливість безперешкодної реалізації прав, свобод та законних інтересів усіма учасниками суспільних відносин в обсягах і межах, що не суперечать визнаним і гарантованим засадам правопорядку. Маємо глибоке й стійке переконання, що вказані характеристики національної безпеки у повній мірі відповідають запитам сьогодення на розуміння сутності вихідної категорії. Беручи до уваги стрімкі, часто непрогнозовані зміни як у локальних, національних, так і глобальних масштабах репрезентовані бачення влучно характеризують цей термін.

Відповідно й похідні категорії, попри вужче (за рівнями й сферами) спрямування, будуть орієнтовані на формування умов для досягнення кількісних і якісних показників у межах окреслених вище орієнтирів. Іншими словами, будь-яка понятійна одиниця обов'язково має відповідати тим цінностям, на котрі орієнтована власне безпека у її базовому розумінні.

Безперечно, під цим ракурсом слушно і виправдано розглядати й категорію «система економічної безпеки України», котра перебуватиме в центрі нашої уваги в ході дисертаційного дослідження. Слід зауважити, що на відміну від поширених у вжитку термінів «економічна безпека держави» чи «економічна безпека України» вказана дефініція поки не користується такою ж мірою популярності. З нечисленних фундаментальних доробків, присвячених саме вказаній дефініції, доцільно виділити результати досліджень таких вчених, як І. Білько й В. Шлемко [18], М. Єрмошенко [19; 20], Я. Жаліло [21; 22], В. Ковч [35], Є. Крихтін [40], А. Кулінська [23; 24], О. Мамулай [34], Х. Маховські [25], С. Мочерний [36], О. Новікова й Р. Покотиленко [39], Г. Пастернак-Таранушенко [26; 27; 28], С. Пирожков [41], О. Скорук [38], А. Степаненко та М. Герасимов [37], О. Шайдаров [33] та інших. Більше того, дефініція «економічна безпека» закріплена на законодавчому рівні у ст. 17 Конституції України [29], абз. 6 п. 1 Концепції економічної безпеки споживчої кооперації України від 12 листопада 2008 року [30], п. 5 Методичних рекомендацій щодо розрахунку рівня економічної безпеки України від

29 жовтня 2013 року [31], Проекті Закону про основи запобігання та боротьби з економічними правопорушеннями № 4449а від 8 серпня 2014 року [32], абз. 6 п. 66 Стратегії національної безпеки України [2], Стратегії економічної безпеки України [3]. Однак, термін «система економічної безпеки України» у правовій площині поки не знайшов свого відображення та є лише предметом публічних наукових дискусій. У цьому сенсі можна згадати лише абз. 5 п. 1 Концепції економічної безпеки споживчої кооперації України від 12 листопада 2008 року [30], у якому міститься термін «система економічної безпеки» із відповідним визначенням, однак спеціалізована (вузька) предметна орієнтованість та юридична сила цього документа унеможливають використання цієї дефініції.

При цьому значний масив напрацювань, присвячений дослідженню понять «економічна безпека держави» чи «економічна безпека України», призвів до формування усталених характеристик останньої. Активна полівекторність багатьох підходів не виключила однаковість тез щодо змістовного наповнення цих дефініцій. Убачається, що не останню роль у цьому відіграли офіційно закріплені тлумачення термінів, які в більшості випадків беруться до уваги провідними науковцями-безпекознавцями. Для наочного підтвердження численності таких підходів, а також для вирішення завдань дисертаційного дослідження пропонується виділити найпоширеніші (див табл 1.1) з метою формування належного методологічного підґрунтя для формулювання авторського понятійно-категоріального апарату.

Таблиця 1.1 Поширені підходи до розуміння понять «економічна безпека держави» чи «економічна безпека України»

Автори трактувань	Підходи до бачення предметних дефініцій
О. Шайдаров [33, с. 397], О. Мамулай [34, с. 174]	Роль і становище національної економіки, а також її інститутів
М. Єрмошенко [19, с. 26; 20, с. 46]	Спроможність держави самостійно здійснювати свою економічну політику

Продовження таблиці 1.1

Я. Жаліло [21, с. 143; 22, с. 87-88], В. Ковч [35]	Можливість задоволення власних базових потреб
С. Мочерний [36], А. Степаненко та М. Герасимов [37, с. 39]	Основна передумова економічної незалежності
Г. Пастернак-Таранушенко [26, с. 28; 27, с. 23; 28, с. 29-30], О. Скорук [38, с. 41]	Стійке економічне зростання
І. Бінько та В. Шлемко [18, с. 31], О. Новікова й Р. Покотиленко [39, с. 267]	Захист національних інтересів
Є. Крихтін [40, с. 136], С. Пирожков [41, с. 14]	Реальна здатність протидіяти загрозам і зберігати стійкість до більшості ризиків
Х. Маховські [25, с. 40]	Високий ступінь незалежності від стратегічних партнерів, які можуть мати вплив на політичні рішення

Сформовано автором на основі [18, с. 31], [19, с. 26; 20, с. 46], [21, с. 143; 22, с. 87], [25, с. 40], [26, с. 28; 27, с. 23; 28, с. 29-30], [33, с. 397], [34, с. 174], [35], [36], [37, с. 39], [38, с. 41], [39, с. 267], [40, с. 136], [41, с. 14]

Плюралізм характеристик не виключає й конгломерацію декількох тез у межах одного висловлювання щодо усвідомлення цієї категорії. Наочними прикладами такого твердження можна вважати ряд фундаментальних суджень, об'єктивованих у роботах Я. Жаліла [92, с. 21; 22, с. 87-88], А. Кулінської [23, с. 10; 24, с. 103], Г. Пастернак-Таранушенка [26, с. 28; 27, с. 23; 28, с. 29-30] й інших. З огляду на поліструктурність вказаної одиниці думка про поєднання декількох розглянутих вище описів є в ході проведення наукових досліджень. Для забезпечення повноти і всебічності наукового дослідження зазначених дефініцій доцільно та виправдано проаналізувати їх визначення в офіційних актах (*див табл 1.2*). Вказане матиме виняткове значення для формулювання й обґрунтування доцільності авторської

інтерпретації вказаного терміну.

Таблиця 1.2 Основні підходи до розуміння понять «економічна безпека» об'єктивовані в офіційних джерелах

Офіційний документ	Підходи до бачення поняття «економічна безпека»
Методика розрахунку рівня економічної безпеки України	«... такий стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз і здатний задовольняти потреби особи, сім'ї, суспільства та держави» (абз. 2 Розділ II) [42]
Концепція економічної безпеки споживчої кооперації України	«... стан захищеності суб'єктів господарювання від негативного впливу зовнішніх і внутрішніх загроз, дестабілізуючих факторів, при якому забезпечується стійка реалізація основних господарських інтересів та цілей статутної діяльності» (абз. 6 п. 1) [30]
Методичні рекомендації щодо розрахунку рівня економічної безпеки України	«... стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз, забезпечувати високу конкурентоспроможність у світовому економічному середовищі і характеризує здатність національної економіки до сталого та збалансованого зростання» (п. 5) [31]
Проект Закону про основи запобігання та боротьби з економічними правопорушеннями № 4449а від 8 серпня 2014 року	«... стан економіки, при якому забезпечується стійке економічне зростання, ефективне задоволення економічних потреб, контроль держави за рухом і використанням національних ресурсів, захист економічних інтересів країни на національному і міжнародному рівнях» (ст. 1) [32]

Сформовано автором на основі [30], [31], [32], [42]

Ураховуючи вище викладене, можемо зробити проміжний висновок, що у

вітчизняному науковому середовищі досить часто оперують термінами «економічна безпека держави» чи «економічна безпека України» (дослідницька складова), «економічна безпека» (правовий аспект), а численні доробки із цієї проблематики сформували ряд усталених підходів щодо характеристик зазначеної предметної категорії. У той же час згадані у роботі¹ й інші позиції можуть акумулюватися і комбінуватися в рамках єдиної дефініції представленої одним дослідником (колективом авторів). Трактатування, закріплені в офіційних документах, смислово істотно не різняться і не протирічать судженням учених.

Представлені популярні конклюдентні орієнтири такі, як: 1) роль і становище національної економіки, а також її інститутів; 2) спроможність держави самостійно здійснювати свою економічну політику; 3) можливість задоволення власних базових потреб; 4) основна передумова економічної незалежності; 5) стійке економічне зростання; 6) захист національних інтересів; 7) реальна здатність протидіяти загрозам і зберігати стійкість до більшості ризиків; 8) високий ступінь незалежності від стратегічних партнерів, які можуть мати вплив на політичні рішення, також корелюються із цінностями вихідної категорії «безпека», а саме: 1) спектр умов різного спрямування, при яких формується й певний час стійко існує відчуття в значній частини колективу щодо відсутності активного впливу більшості загроз і конвертації ключових ризиків у деструктивні фактори для нормальної життєдіяльності індивідів; 2) дійсна захищеність критичних сфер санкціонованою державою публічної охорони від впливу викликів, загроз і ризиків; 3) готовність і здатність у різні форми, методи та способи запобігати й протидіяти дії лівової частки викликів, загроз і ризиків для існуючого колегіально схваленого стану речей у межах території, зазвичай, держави; 4) можливість безперешкодної реалізації прав, свобод та законних інтересів усіма учасниками суспільних відносин в обсягах і межах, що не суперечать визнаним і гарантованим засадами правопорядку. Слід зазначити, що у цьому аспекті йдеться про предметний орієнтир на економічний напрям державного впливу й суспільного

¹ Див табл 1.1

забезпечення. Тобто, фундаментальні безпекові цілі повинні невідворотно забезпечуватися у сфері економічних відносин і в усіх їхніх галузях.

Однак, попри таку стійку й широку сукупність зв'язків, оперування категоріями «економічна безпека», «економічна безпека держави» чи «економічна безпека України», не дає у повній мірі розкрити потенціал цього елемента, як приналежного до системи вищого рівня – національної безпеки України. Зважаючи на явну складність, різнорівневність й багатоаспектність економічної складової, досить своєчасним, слухним і виправданим убачається намір застосування системного підходу для характеристики останньої. На користь такого судження, з-поміж іншого, виступає ряд актуальних комплексних робіт, націлених на різні грані економічної діяльності. Серед таких доробок доцільно виділити фундаментальні напрацювання А. Гуменюка [43], О. Дацко [44; 45], С. Завгородньої [46; 47; 48], В. Мельника [49; 50; 51; 52], Н. Морозюк [53], І. Ревак [54; 55], В. Сазонова [56; 57; 58], В. Сухоноса, В. Сухоноса і О. Сластьоненка [59] й інших. При цьому, окремі з них прямо вказують на необхідність саме застосування методів системного підходу у цій сфері. Наприклад, С. Завгородня переконує, що такий підхід є виправданим в умовах гострої потреби підвищення рівня ефективності державного управління у сфері економічної безпеки [46, с. 84; 47, с. 11-12; 48, с. 21]. В окресленому ракурсі А. Гуменюк загострює увагу на тому, що він передбачатиме аналіз економічного компоненту, виходячи з базових критеріїв до неї у статусі системи [43, с. 55]. Його висновки зводяться до наступних фундаментальних позицій: 1) усі системні об'єкти є елементами систем складнішого порядку; 2) будь-яка система представлена сукупністю підсистем, що утворюють певний об'єкт у якості цілісного явища або процесу; 3) кожний об'єкт із позиції системної організації має підпорядкованість рівнів; 4) така система повинна бути адаптована до зовнішнього середовища. Це дасть змогу формувати економічну політику задля усунення або зменшення кількості загроз економічній стабільності суспільства; 5) базисом цієї системи має стати діяльність

(функціонування) її суб'єктів [43, с. 55-56]. Подібні підходи прослідковуються й в інших комплексних наукових дослідженнях, наведених вище.

Ми цілком підтримуємо зазначену позицію, адже економічна складова вже давно набула контурів і параметрів самостійної системи, яка функціонує за певними принципами й непохитно орієнтована на досягнення самостійної сукупності цілей. Безперечно, такі цілі спрямовані на виконання завдань системи вищого рівня – системи національної безпеки України, однак вирізняються діапазоном типових особливостей. Це, у свою чергу, формує умови й навіть зумовлює потребу сталого функціонування автономної субстанції (системи) із відповідною приналежністю. У такому випадку слушно й виправдано розраховувати на систематичне та результативне виконання всіх сформульованих і схвалених завдань. До того ж, мотивовані судження, представлені А. Гуменюком [43, с. 55-56], дають додаткові реальні підстави застосунку саме системного підходу.

Своєчасною і доцільною вбачається ініціатива зосередити увагу на поширенні бачення змістовного наповнення дефініції «система економічної безпеки України» (див табл 1.3). Це забезпечить подальший аналіз відповідних точок зору, у тому числі з метою необхідної розробки авторського поняття, яке має значення для цілісного вирішення завдання дисертаційного дослідження.

Таблиця 1.3 Поширені наукові підходи щодо розуміння дефініції «система економічної безпеки України»

Автори	Підходи до бачення предметних дефініцій
В. Мельник [49, с. 361-362; 60, с. 26; 51; 52, с. 3, 129, 146-147, 223, 398]	«... багаторівнева, складна, динамічна соціальна система з розгалуженою мережею взаємопов'язаних і взаємозалежних елементів та зв'язків, спрямована на забезпечення захищеності та стійкості національної економіки відносно дії широкого спектра внутрішніх та зовнішніх загроз екзогенного й ендогенного походжень, а також сприяння конкурентоспроможності останній у світовій системі господарства, зберігати досягнутий рівень прогресу, самовідтворення та сталий й збалансований поступальний розвиток»

Продовження таблиці 1.3

І. Ревак [54, с. 33; 55, с. 61]	«1) підсистема, котра функціонує у рамках системи національної безпеки України й разом із іншими видами формує певний порядок; 2) спектр взаємопов'язаних і взаємозалежних елементів, які за рахунок узгоджених дій можуть протидіяти загрозам, а також гарантувати безпечний розвиток вітчизняної економіки»
В. Сазонов [56, с. 9 7, 100; 57, с. 6, 11, 20-21; 58]	«1) стан захищеності економічної систем та її інститутів від дії кримінальних практик і криміногенних факторів (загроз); 2) частина національної безпеки, що відображає прийнятний у конкретних історичних умовах рівень ураженості економіки злочинністю, а також допустимий ступінь економікокримінального впливу на політику, право, культуру та довкілля»

Сформовано автором на основі [49, с. 361-362], [51; 52, с. 3, 129, 146-147, 223, 398], [54, с. 33; 55, с. 61], [56, с. 97, 100; 57, с. 6, 11, 20-21; 58]

Аналізуючи наведені підходи, слушно відмітити, що дослідники єдині у міркуваннях про приналежність цієї складової до системи національної безпеки України. При цьому вони виділяють її наступні характеристики: 1) захищеність і сприяння розвитку національної економіки; 2) допустимі умови для перебігу економічних та суміжних процесів; 3) акцент на здатність запобігати й протидіяти новим загрозам економічній складовій; 4) один із надважливих векторів забезпечення національної безпеки України.

Загалом же, можемо відмітити одноманітність суджень щодо розуміння сутності досліджуваної категорії на сучасному етапі розвитку думки. Припускаємо, що даються в знаки усталені спільні погляди на природу цього компоненту, зміст і характер правової політики, специфіка системного підходу тощо. У цей же час, указане свідчить про одновекторність підходів, а також обґрунтованість ідей щодо ключових позицій наукового інтересу.

Із огляду на вищевикладене, убачається за доцільне представити авторське визначення поняття «система економічної безпеки України». Так,

система економічної безпеки України – це багатоаспектна складна соціальна система, яка включає в себе численний неоднорідний елементний склад, сполучений широким спектром зв'язків та орієнтована на постійну ефективну й результативну реалізацію заходів за такими напрямками: 1) збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній; 2) забезпечення здатності конкурентоспроможності лівової частки вітчизняних економічних галузей у світі; 3) сприяння поступальному розвитку всього економічного сектору [61]. Переконані, таке формулювання цієї понятійної одиниці в повному обсязі відображає уявлення про її роль і специфіку як об'єкта публічно-правового забезпечення.

Як будь-яка інша система, репрезентований предмет вирізняється певною сукупністю властивостей. Вони є закономірним проявом організаційних особливостей і функціональної специфіки системи економічної безпеки України, стійко й однотипно проявляючись під час різних форм, методів та способів впливу її суб'єктів на об'єкти санкціонованого регулювання. У ході дослідження ми виокремили наступні **властивості** системи економічної безпеки України: 1) взаємозалежність із багатьма іншими системами, насамперед безпековими (вищого, рівнозначного і нижчого рівнів); 2) взаємозалежність із навколишнім середовищем, політичною кон'юнктурою, геополітичними і геоекономічними процесами й іншими факторами; 4) динамічність функціонування; 5) емерджентність; 6) ієрархічність; 7) синергетичність; 8) сталість базових мети і завдань; 9) функціональність; 10) цілісність.

Гармонійно доповнюючою компонентою властивостей системи є її ознаки, які сукупно дають змогу ідентифікувати об'єкт уваги, у тому числі вирізнивши його з-поміж інших подібних за характеристиками. До числа **ознак** системи економічної безпеки України пропонується включити наступні: 1) багатоаспектність; 2) наявність структури з численним неоднорідним елементним складом, сполучених широким спектром зв'язків;

3) підпорядкованість системі вищого рівня (національній безпеці України);
4) предметний орієнтир на: а) збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній; б) забезпечення здатності конкурентоспроможності лівової частки вітчизняних економічних галузей у світі; в) сприяння поступальному розвитку всього економічного сектору;
5) соціальна система; б) спрямованість на ефективне й результативне функціонування.

Ураховуючи безспірний факт автономізації, доцільно виокремити існування власних мети і завдань. Як зазначалось вище, вони є похідними від функціональних орієнтирів системи національної безпеки України й націлені на сприяння реалізації останніх у межах власних сфер регулятивного впливу.

У той же час, ідеться про профілізацію векторів впливу, консолідовану спільною сферою протікання процесів. У результаті чого застосовуються подібні взаємопов'язані й, нерідко, взаємозалежні механізми для досягнення проміжних і загальних цілей. Із огляду на це, **метою** аналізованої системи пропонується вважати діапазон офіційно закріплених орієнтирів щодо збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній, забезпечення здатності до конкурентоспроможності вітчизняних економічних галузей у світі, а також сприяння поступальному розвитку всього національного економічного сектору. Для обов'язкового досягнення таких цілей і функціонує система економічної безпеки України, а для підвищення рівня її ефективності аналізуються однойменні наукові категорії.

Щодо завдань аналізованої системи, то вони, закономірно, є похідними від мети діяльності й розробляються з урахуванням поточних юридичних обмежень для регулюючого впливу. Якщо у випадку мети ми визначали лише санкціоновані наміри (орієнтири), то з позиції **завдань** слід окреслювати спектр об'єктивованих у нормативно-правових актах і стратегічних документах

установок, практична реалізації заходів по яких має забезпечити досягнення мети. При цьому кількість і типи завдань можуть корегуватися залежно від їхньої фактичної здатності задовольняти наявні інтереси, ураховуючи монопольні можливості суверена.

Пропонована нами ініціатива щодо дослідження економічної складової як системної категорії пояснюється й наявністю її власної унікальної структури, що налічує різні елементи і передбачає існування стійких зв'язків між ними. Такий підхід корелюється з поглядами багатьох вітчизняних дослідників [62, с. 6], [63, с. 48] щодо аналізованого аспекту та не суперечить поточній нормативно-правовій парадигмі. Однак, її відсутність ставить під сумнів саме класичне уявлення про природу системи та породжує суперечності у підходах до розуміння сутності. Тому у своєму дисертаційному дослідженні ми пропонуємо **структуру системи економічної безпеки України** розглядати як обов'язковий атрибут будь-якої системи, елементи котрої розташовані у певному порядку, традиційно діють (функціонують) за встановленими алгоритмами й поєднані спільними зв'язками. Унаслідок чого є можливим безпосереднє виконання всіх функцій такої субстанції [375; 376].

Проводячи своє дослідження, ми дійшли висновку, що в наукових джерелах зустрічається не багато думок щодо видового й чисельного складу елементів структури системи економічної безпеки України. Зокрема В. Мельник репрезентує й відстоює таку градацію: 1) об'єкти безпеки; 2) суб'єкти із забезпечення такої безпеки; 3) адміністративно-правові засади щодо забезпечення функціонування аналізованої системи; 4) загрози і ризики цій системі; 5) підсистеми системи економічної безпеки України [50, с. 158; 51; 52, с. 9, 27; 54, с. 3-4, 34-35, 155, 159, 224, 399]. У свою чергу І. Ревак є прихильницею наступного переліку: 1) об'єкти безпеки; 2) суб'єкти забезпечення безпеки; 3) власне сам механізм зміцнення безпеки [54; 55, с. 60]. На наше переконання, **елементний склад структури системи економічної безпеки України** має містити такі компоненти: 1) об'єкти безпеки; 2) суб'єкти із забезпечення безпеки; 3) правові засади, на

основі яких формується відповідна система і функціонують її механізми; 4) елементи суміжних систем вищого рівня, рівнозначних систем, а також підсистеми системи економічної безпеки України (виробнича, енергетична, інвестиційно-інноваційна, продовольча, фінансова та ін.). Відповідно ми можемо стверджувати, що йдеться про виокремлення об'єктів безпеки як елементів структури репрезентованої системи. Маємо переконання, що у цій тезі міститься відповідь на питання стосовно необхідності стійкого публічно-правового забезпечення економічної складової системи національної безпеки України. Зазначене пояснюється широким спектром типів об'єктів, які потребують дієвої охорони й захисту від неправомірних посягань усіх учасників правовідносин.

Також слід зазначити, що поширеним і визнаним у науковому світі є твердження, що об'єктами цього виду безпеки є національні економічні інтереси [64, с. 241-242; 65, с. 9], забезпечення котрих – якраз прерогатива суб'єктів аналізованої системи. Про їхній стійкий взаємозв'язок з безпековою компонентою також зазначають й інші вітчизняні вчені, такі як: А. Сухоруков, С. Мошенський, О. Петрук [66, с. 363], В. Сідлецька [67, с. 81] та ін. Із огляду на схвалений перелік завдань дисертаційного дослідження вказаній позиції змістовна увага буде приділена в інших підрозділах роботи.

На цьому етапі підкреслимо загальновідомий факт численної кількості груп таких інтересів у сучасних умовах. До того ж, вони мають виняткове значення для гарантування національних інтересів України, опікуваних суб'єктами під егідою системи вищого рівня.

Під таким кутом зору якраз і набуває важливого значення питання комплексного забезпечення функціонування системи економічної безпеки України публічними інституціями й суспільством. Зазначене першочергово передбачає стійке та ефективне запобігання й протидію викликам, загрозам і ризикам національній економіці. Відсутність належних санкціонованих державою форм і методів спротиву економічним загрозам неминуче призведе до деструкції ряду економічних процесів, маючи ланцюговий ефект. Його

наслідки невдовзі відчуватимуть інші представники складових національної безпеки України, що послабить оборонний та інші критичні вектори впливу держави.

Широка й прогресуюча типологізація лише самих загроз, у тому числі цифрового походження, може мати вирішальне значення на наступних етапах державотворчого процесу. Свідоме чи неумисне нехтування конституційним обов'язком відчутно й стрімко послаблюватиме необхідний економічний потенціал держави. Оскільки, навіть на перший погляд, незначні ексцеси можуть стрімко перерости в проблему регіонального чи національного масштабів, або навіть вийти за ці межі.

Убачаємо, що зазначене аргументовано доводить тезу про виключну важливість економічної складової як елемента національної безпеки України та позиціонування її саме в якості системної категорії [68, с. 70-71]. До того ж, важливим є стала колективна участь усіх сторін у питаннях її стійкості та сприяння необхідному поступальному розвитку. Будь-який альтернативний перебіг подій неминуче призведе до поступового руйнування усталених засад і знецінення авторитету держави, істотно послаблюючи економічний потенціал країни та, загалом, безпекові можливості в осяжному майбутньому.

1.2. Теоретико-правова характеристика категорії «цифрові активи»: поняття, ознаки, властивості та оцінка підходів щодо розуміння її форм

Активна й різнопланова цифровізація багатьох процесів у більшості провідних країн докорінно трансформувала погляди на ряд сфер і аспектів суспільного життя. Відсутність ефективних механізмів контролю і нагляду з боку держави, спрощення й прискорення низки процедур (у тому числі бюрократичних), дистанційність, доступність, децентралізація, оперативність, зростання ролі пересічних користувачів та інші переваги популяризували такі ресурси і системи. Довготривалий період хронічної зарегульованості багатьох

сфер управлінського впливу на фоні названих новацій лише пожвавив інтерес до проявів глобальної цифровізації, у певній мірі стимулювавши подальше стійке становлення останньої.

Такого характеру функціональні можливості дали поштовх для появи нових і розвитку багатьох існуючих процесів у різних сферах економічної діяльності країни. Оскільки з'явилися і нетривалий час успішно апробувалися концептуальні засоби, вирішення багатьох завдань у ефективні способи (починаючи від типової форми розрахунку за виконані роботи й надані послуги, оприлюднення та ідентифікація нематеріальних благ чи посвідчення майнових прав і завершуючи використанням їх у якості фіатних коштів² для придбання об'єктів нерухомості [377] чи вартісного рухомого майна [378]). Іншими словами, такі правочини й подібні дії здійснювались щодо різних об'єктів, у тому числі дороговартісного характеру. При цьому відносини будувались на взаємному волевиявленні сторін (контрагентів), без міжнародних і державних гарантій та довірі до систем, що забезпечують оборот відповідних цифрових активів. Тобто особи, усвідомлюючи настання реальних ризиків, свідомо користувалися однойменними послугами задля задоволення персональних інтересів.

Зазначене лише додатково доводить високий ступінь популяризації інструментів цифрового обороту та вказує на невідворотний розвиток останніх. До того ж поетапне, але стійке визнання державою цих засобів і способів лише підтверджує факт невідворотності відповідних процесів.

Слід зауважити, що категорія «цифрові активи» є малодослідженою вітчизняними науковцями. Причин цьому багато, але основні з них – складність і концептуальність відповідних явищ і процесів, а також нещодавнє прийняття,

² Фіатні гроші (або «фіат») – це тип грошей або валюти, цінність яких обумовлена не своєю вартістю чи гарантіями обміну на золото або іншу валюту, а волевиявленням держави у формі наказу (розпорядження тощо) («фіат») використання їх як засобу платежу. *Джерела:* 1. James Chen., Robert C. Kelly, Suzanne Kvilhaug. Fiat Money: What It Is, How It Works, Example, Pros & Cons. *Website: Investopedia.* 2024. URL: <https://www.investopedia.com/terms/f/fiatmoney.asp>. 2. Копил О., Неруш Л. Міжнародний досвід законодавчого регулювання питання функціонування криптовалют, криптовалютних бірж, майнінгу та виводу в фіат. Інформаційна довідка, підготовлена Європейським інформаційнодослідницьким центром на запит народного депутата України. *Веб-портал: ІнфоЦентр.* 2018. URL: <https://infocenter.rada.gov.ua/uploads/documents/29421.pdf>

перед повномасштабним вторгненням російських військ, у лютому 2022 року Закону України «Про віртуальні активи», який буде діяти лише після набрання чинності Законом України про внесення змін до Податкового кодексу України [69] щодо особливостей оподаткування операцій з віртуальними активами (п. 1 Розділу VI. Прикінцевих та перехідних положень) [70] та влітку 2023 року Закону України «Про цифровий контент та цифрові послуги» від 10.08.2023 р. № 3321-IX [71], якими в офіційний обіг введені терміни «віртуальні активи» (п. 1 ч. 1 ст. 1) і «цифровий контент» (п. 11 ч. 1 ст. 2), відповідно. У той же час, серед іноземних учених саме опрацьовувана термінологічна одиниця часто є предметом наукового інтересу. Із когорти всіх діячів виділимо роботи О. Adekoya й Е. Екро [72, с. 3], J. P. Buntinx [76], О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенка, Д. Білінського й Є. Смичка [77, с. 7, 31, 128], W. S. Li [75 с. 76-77], Е. Harbinja [74, с. 102], S. van Erp і J. Uitdehaag [81, с. 17, 21], M. D. Walker [73, с. 53] та інших.

Загалом дефініція «цифрові активи» у національній правовій площині не знайшла свого відображення. Як зазналось вище, законодавець пішов іншим шляхом, легалізувавши термін «цифрові речі» і включивши до них «віртуальні активи» та «цифровий контент», кожне з яких змістовно охоплює певних представників, виходячи з типового уявлення про елементний склад цифрових активів. Однак сформульована тематика дисертації підтверджує слушність розробки саме аналізованої категорії тому, що у подальшому сприятиме акумуляції й класифікації загроз системі економічної безпеки України, котрі можуть виникати внаслідок операцій із такими активами. Розуміння особливостей і кількісного складу типів цифрових активів позитивно відобразиться на формуванні уявлення про діапазон груп загроз, які мають значення для представленої роботи.

Так, на спільне переконання іноземних дослідниць О. Adekoya й Е. Екро, цифровий актив – це просто вміст, що зберігається в цифровому вигляді в будь-якому форматі і пов'язане з ним значення [72, с. 3]. Іншими словами, ідеться про електронні файли даних, якими можуть володіти та передавати особи-

власники, і які використовуються як валюта для здійснення трансакцій або в якості способу зберігання нематеріального вмісту, такого, як комп'ютеризовані твори мистецтва, відео або контрактні документи [72, с. 3]. M. D. Walker і E. Harbinja під таким активом убачають будь-які об'єкти, котрі мають оцифровану форму [73, с. 53], [74, с. 102]. W. S. Li наголошує, що це цифрова інформація, вміст якої накопичений підприємствами чи установами в процесі виробництва, експлуатації та управління, які є цінною для підприємств чи установ. Через організацію й обробку цифрових активів, можна оптимізувати структуру управління контентом підприємства, реформувати модель роботи підприємства, і дохід підприємства, можливо, підвищиться [75, с. 76-77]. J. P. Buntinx наголошує, що це будь-які цифрові дані, котрі існують у бінарному вигляді [76]. На думку дослідника, слід розглядати всі типи таких даних: від умовного кінофільму до папки на робочому столі [76]. На спільне переконання Н. Кучерявенка, Д. Білінського, Є. Смичка й О. Кудь у такому контексті вбачається інформаційний ресурс, який є похідним від права на цінність і такий, що обертається в розподіленому реєстрі у вигляді унікального ідентифікатора [77, с. 7, 31, 128], [78, с. 29, 34; 79, с. 38]. Схожі за змістом судження пропонуються й в інших наукових дослідженнях. Одне зі вказаних трактувань передбачає формулювання змістовного наповнення як такого, що це будь-які онлайн-файли або медіа, котрі мають цінність. Ідеться і про зображення, відео, документи, електронні таблиці чи будь-що інше, що приносить цінність [80]. Загалом же можемо стверджувати, що усвідомлення змісту цієї предметної дефініції істотно не різниться у представлених наукових трактуваннях. Відправними точками є однакові координати, навколо яких вибудовуються дослідниками та іншими зацікавленими особами подальші твердження, які уточнюють і доповнюють.

З-поміж наведених і деяких інших відомих знакових думок особливої уваги заслуговує Звіт «Принципи Європейського інституту права щодо використання цифрових активів як цінних паперів» [81], розроблений працівниками Європейського інституту права (S. van Erp, J. Uitdehaag та ін.) і

представлений у 2022 р. Відповідно до сформульованих трактувань пропонуються наступні варіації розуміння змісту і суті цієї дефініції: 1) він зберігається, відображається та адмініструється виключно в електронному вигляді, на віртуальній платформі чи базі даних або через них, у тому числі, якщо це запис або представлення реального, придатного для продажу активу, і незалежно від того, чи зберігається сам цифровий актив безпосередньо, чи через рахунок у посередника; 2) а) може бути об'єктом права контролю, користування чи використання, незалежно від того, чи юридично такі права характеризуються як майнові, зобов'язальні чи інші; і б) може передаватися від однієї сторони до іншої, у тому числі шляхом добровільного відчуження [81, с. 17, 21]. Ураховуючи вищезгадані іноземні та вітчизняні підходи до дефініції «цифрові активи», припускаємо, що його автори мали намір представити твердження, котре охоплює всі прояви відповідного явища, при цьому ними розглядаються як технічні й технологічні сторони, так і організаційні й правові вектори аналізованого нами питання.

Попри відсутність визначення та роз'яснень щодо природи досліджуваного терміну у вітчизняних нормативно-правових актах різного характеру, офіційні іноземні джерела були присвячені відповідній позиції. Наприклад, як зазначають Н. Кучерявенко, Д. Білінський й Є. Смичок, таким поняттям не оперують у праві Європейського Союзу (далі – ЄС), проте опосередковано про такий тип активу йдеться в пп. 3 ст. 4 Директиви Європейського Парламенту і Ради (ЄС) 2018/843 від 30 травня 2018 року «Про внесення змін до Директиви (ЄС) 2015/849 «Про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму» та «Про внесення змін до директив 2009/138/ЄС і 2013/36/ЄС» [82]. Так, у цих міжнародно-правових актах іде мова про тлумачення дефініції «майно», яка в тому числі передбачає у своєму складі активи будь-якого типу, зокрема в цифровому форматі, котрі підтверджують право власності на такі активи або ж право на їх частку [77, с. 31]. У висновках законодавчої комісії Великої Британії, опублікованих в 2022, 2023, 2024 рр. та присвячених питанням

цифрових активів, зустрічається узагальнене трактування поняття останнього. Так, при розгляді поняття цифрові активи мова повинна йти про будь-які активи, представлені у цифровому чи електронному вигляді [83], [84], [85]. При цьому укладачі звітів свідомо й цілеспрямовано використовують широке розуміння [83], що мотивується змогою чисельної варіативності здійснення наукових розвідок, відчутно посиливши дослідницький потенціал. Із огляду на те, що ці висновки готуються з кінцевою метою розробки комплексного правового забезпечення регулювання відносин щодо обороту цифрових активів у Великій Британії, самий такий підхід є доцільним і виправданим.

Попри розширене смислове навантаження так званої «робочої версії», автори зазначених вище звітів сходяться на думці, що цифровий актив може вважатися таким у разі відповідності трьом критеріям, а саме: 1) складання із даних, розміщених на електронному носії, в тому числі у формі електронного коду, цифрових, електронних та інших аналогових сигналів; 2) існування й оборот незалежно від осіб та правової системи; 3) конкурентоздатність [83]. Співмірність індикаторам всіх трьох критеріїв дає мотивовані підстави розглядати їх у якості цифрового активу із відповідними правовими й неправовими наслідками.

Досліджуючи поняття «цифрові активи», ми проаналізували відповідні нормативно-правові акти Сполучених Штатів Америки, що стосуються цієї сфери застосування. Відповідно до Уніфікованого акту «Про довірчий доступ до цифрових активів» від 2014 року (був переглянутий у 2015 році) йдеться про електронний запис, на котрий має право або є об'єктом інтересу певна (-ої) особа (-и) [86, с. 2]. Однак варто зауважити, що цей акт носить дорадчий (інформативний) характер і спрямований на подальше удосконалення правового регулювання у багатьох сферах (предметних і суміжних груп суспільних відносин). Тобто, його методологічні орієнтири слушно буде використати для розробки уніфікованої законодавчої бази з питань обороту цифрових активів.

Складно встановити факт хоч якогось обсягу і форми запозичення, однак

у 2019 р. в штаті Вайомінг набрав чинності Закон «Digital assets-existing law» [87], котрим, із-поміж іншого, передбачено визначення дефініції «цифрові активи». Відповідно, це – вираз економічних, майнових прав або прав на доступ до об'єктів, що зберігаються у комп'ютеризованому форматі, налічуючи віртуальну валюту, цифрові споживчі активи та цифрові цінні папери [87]. Таке визначення значно звужує діапазон типів цих об'єктів, порівняно з поширеними класичними уявленням. Водночас, із юридико-технічної точки зору та типових загальновідомих бачень про правову державу (К. Волинка [88, с. 82-83, 84], О. Скакун [89; 90, с. 119-120], Р. Тополевський і Н. Федіна [91, с. 97-98] й ін.) доцільним є акцент саме на правах щодо об'єктів чи можливостей доступу до останніх. Наявний, успішно офіційно апробований підхід, обов'язково буде взятий нами до уваги під час узагальнення цього питання.

У Законі «Про довірений (фідуціарний) доступ до цифрових активів» від 2015 р. (Revised Uniform Fiduciary Access to Digital Assets Act 2015, RUFADAA) [91] пропонується під цим терміном розглядати електронний запис, щодо якого особа має право або інтерес [92]. При цьому, як слушно зазначає В. Бацуца, зі змісту окремих наступних нормативних конструкцій акту «випливає», що він не включає актив чи зобов'язання, якщо ті не мають електронної форми [93, с. 46-47]. Вчений також наголошує, що цей підхід застосовується у багатьох відповідних актах інших штатів (Закон штату Массачусетс «Про доступ до облікових записів електронної пошти спадкодавця» [94], Закон штату Іллінойс стосовно цифрових активів [95] та ін.) [93, с. 47]. З огляду на специфіку федеративного адміністративно-територіального устрою США правові системи штатів містять й інші підходи до розуміння аналізованої дефініції. Водночас, розглянуте офіційне визнання є найпопулярнішим серед решти існуючих, маючи попит із різних точок зору.

Законом Канади «Про єдиний доступ до цифрових активів довірених осіб» від 2016 року (Uniform Access to Digital Assets by Fiduciaries Act 2016, UFADAA) [96] такий актив позиціонується в якості запису, що формується, записується, передається або зберігається в цифровій або іншій нематеріальній

формі за допомогою електронного, магнітного, оптичними або будь-якими іншими подібними засобами [96]. Норми ст. 2 (1) Закону Бермудських Островів «Про комерційні відносини з цифровими активами» 2018 року (Digital Asset Business Act 2018) [97] передбачають розширене тлумачення предметної дефініції. Зокрема, цифрові активи – це все те, що існує у бінарному форматі³ й пов'язане з правом на його користування, а також включає і цифрове вираження вартості, котре: 1) використовується в якості засобу обміну, розрахункової одиниці або засобу збереження вартості не є законним платіжним засобом, незалежно від того, деномінований у законному платіжному засобі чи ні; 2) призначений для представлення таких активів, як борг або власний капітал юридичної особи; 3) орієнтований для представлення будь-яких активів або прав, пов'язаних із такими активами; 4) призначені для надання доступу до програм, послуг чи продуктів засоби технології розподіленої книги; але не включає – а) трансакції, у котрих особа надає цінність у рамках програми спорідненості чи винагороди, яку вартість не можна вилучити чи обміняти з особою на законний платіжний засіб, банківський кредит чи якийсь цифровий актив; або б) цифрове представлення цінності, видане видавцем або від його імені та використане в онлайн-грі, ігровій платформі або групі ігор, які продаються тим самим видавцем, або пропонуються на одній ігровій платформі [97]. Натомість, у ст. 2 Правил Багамських Островів «Про індустрію цінних паперів (контракти на різницю)» (2020) [98] визначено, що у цьому контексті – це цифрове репрезентування вартості, котре розповсюджується через технологічну платформу розподіленої книги, де цінність вбудована, або щодо якої наявне договірне право використання, включаючи без обмежень цифрові токени [98]. Як бачимо, й на офіційному рівні це поняття знайшло власне відображення в деяких іноземних країнах. Логіка таких політик щодо легалізації відповідних механізмів має різне

³ Бінарна (двійкова) система числення – найпоширеніша позиційна система числення, що передбачає використання лише двох символів (зазвичай 0 (нуль) та 1 (одиницю)) для запису чисел. Додатково див Вишневий С. Інформатика. Частина 1. Основи програмування та алгоритми. Курс лекцій : навч. посібн. Київ : КПІ ім. Ігоря Сікорського. 2023. С. 22–23.

походження, проте факт відповідного визнання наочно свідчить про розвиток цього вектору.

Ураховуючи змістовне наповнення розглянутих відомих суджень, слушно також виділити типові характеристики цієї категорії в аналізованих вище тезах, що створить додаткове підґрунтя саме для майбутніх персональних розробок (див табл 1.4). Беручи до уваги новизну й явно недостатню дослідженність це позитивно відобразиться на кінцевих результатах дисертаційного дослідження.

Таблиця 1.4 Поширені характеристики категорії «цифрові активи» в офіційних документах та літературних джерелах

Автори трактувань	Поширені хар-ки категорії «цифрові активи»
О. Adekoуа й Е. Екро [72, с. 3], J. P. Buntinx [76], W. S. Li [75, с. 76-77], Е. Harbinja [74, с. 102], M. D. Walker [73, с. 53]	Існування й оборот у цифровому вимірі, не маючи матеріального вираження
О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенко, Д. Білінський і Є. Смичок [77, с. 7, 31, 128], S. van Erp та J. Uitdehaag [81, с. 17, 21]	Оборот у спеціальних системах
О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенко, Д. Білінський і Є. Смичок [77, с. 7, 31, 128]	Унікальний код кожного об'єкта
О. Adekoуа й Е. Екро [72, с. 3], J. P. Buntinx [76], Е. Harbinja [74, с. 102], M. D. Walker [73, с. 53], What are Digital Assets? Exploring Their Impact on E-Commerce Marketing [80]	Широка типологізація об'єктів
О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенко, Д. Білінський і Є. Смичок [77, с. 7, 31, 128], W. S. Li [75, с. 76-77], Е. Harbinja [74, с. 102], M. D. Walker [73, с. 53]	Має вартісну цінність (фінансову, нематеріальну або матеріальну)
О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенко, Д. Білінський і Є. Смичок [77, с. 7, 31, 128], Закон «Digital assets-existing law» [87]	Вираз економічних і майнових прав

Продовження таблиці 1.4

S. van Erp i J. Uitdehaag [81, с. 17, 21]	Існування й оборот незалежно від правових умов, обмежень і санкцій
S. van Erp i J. Uitdehaag [81, с. 17, 21], National Conference of Commissioners on Uniform State Laws [86]	Можуть бути об'єктами права власності (володіння, користування, розпорядження)
W. S. Li [75, с. 76-77], What are Digital Assets? Exploring Their Impact on E-Commerce Marketing [80]	Засіб підвищення ефективності функціонування установ, підприємств й організацій, а також багатьох форм діяльності суспільства

Сформовано автором на основі [72, с. 3], [73, с. 53], [74, с. 102], [75, с. 76-77], [76], [77, с. 7, 31, 128], [78, с. 29, 34; 79, с. 38], [80], [81, с. 17, 21], [86], [87]

Із позиції поточних правових реалій категорію «цифрові активи» варто порівняти з терміном «цифрові речі». Це зумовлено тим, що нормами вітчизняного законодавства, юридично закріплено саме останнє поняття, яке, у свою чергу, включає цифровий контент, віртуальні активи й інші відповідні блага (абз. 2 ч. 1 ст. 179¹ Цивільного кодексу України [99]). Тобто, виходячи з базового розуміння, ці категорії є синонімічними або ж подібними за рядом ключових ознак.

У ході свого дослідження ми дійшли висновку, що оперування саме термінологічною одиницею «цифрові активи», попри відсутність законодавчого визначення цього поняття, слід вважати виправданою ініціативою. На підтвердження цього В. Бацуца [100, с. 34-35; 93, с. 33-34, 61], О. Даниленко [101, с. 150-151, 152-153] й О. Кудь [78, с. 2-3, 6, 7-8] у своїх наукових працях аргументовано віддають перевагу саме категорії «цифрові активи». Зокрема, В. Бацуца у власному дисертаційному дослідженні до уваги бере саме такий термін, здійснюючи відповідну характеристику останнього. При цьому робота була захищена в 2024 р., тобто зі значною темпоральною різницею, якщо урахувати появу відповідних новацій [100, с. 34-35; 93, с. 61].

Йдеться про прийняття Закону України «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав», яким було легалізовано поняття «цифрові речі» [102]. О. Кудь, виходячи з наведеного вище тлумачення суті однойменної дефініції, також є прихильником цього підходу. Ураховуючи сутнісно-сміслові особливості такого феномена, крізь призму економічної, правової, інформаційної й ціннісної граней, він докладно доводить логіку оперування саме обраною варіацією [78, с. 2-3, 6, 7-8]. Змістовно проблематику доцільності вжитку саме одиниці «цифрові активи» розкриває О. Даниленко. Дослідниця резонно вказує і докладно роз'яснює, що виникають суперечності категорії «цифрові речі» у їх співвідношеннях із певними позиціями щодо правової природи об'єктів цивільних прав [101, с. 150]. Тобто, можуть з'являтися випадки колізійності, що потребуватимуть додаткового подальшого дієвого розв'язання у правотворчій чи правозастосовній площинах.

Серед аргументів на користь обраного підходу вчена загострює увагу на таких аспектах: 1) недостатня чіткість і поява неоднозначності в розумінні як поняття об'єктів цивільних прав, так правової класифікації останніх у якості матеріальних та нематеріальних благ, що може істотно ускладнити реалізацію відповідних положень. У загальних обрисах йдеться про природну неможливість існування всіх нематеріальних благ в цифровому середовищі (особисті немайнові блага тощо) [101, с. 150-151]; 2) поява суперечностей під час визначення місця власне «цифрових речей» у сформованій системі об'єктів цивільних прав. Йдеться про імовірну не відповідність властивостей певних видів цифрових речей (віртуальних активів, цифрового контенту) критерію матеріальності, що є типовим для речей [101, с. 151-152]. До слова, такі ж підсумки містяться у висновках законодавчої комісії Великої Британії [83]; 3) дискусійність щодо визначення поняття «цифрова річ». Умовне охоплення широкого спектру вже існуючих груп об'єктів цивільних прав, котрі базуються на класичних системах електронного обліку (бездокументарні цінні папери, електронні платіжні засоби тощо) [101, с. 152-153]. Ураховуючи це, можемо

стверджувати, що вказані ризики є ймовірними та виправданими й можуть слугувати підґрунтям для появи дискусійних питань в осяжному майбутньому.

Закономірним вирішенням зазначених вище потенційних неузгодженостей із урахуванням згаданих поглядів В. Бацуци [100, с. 34-35; 93, с. 33-34, 61] й О. Кудь [78, с. 6, 7-8], О. Даниленко запропоновано надавати перевагу саме терміну «цифрові активи», слушно наголосивши, що він змістовно охопить різні типи цифрових цінностей і слідуватиме західній традиції поняття «asset» у цьому аспекті [101, с. 153], [93, с. 33-34]. Ми повністю погоджуємось з цими висновками та, як неодноразово зазначалось вище, пропонований нами концепт влучно розкриє суть відповідної дефініції. Тим більше, як ми довели у своєму дослідженні, саме поняття «цифровий актив» використовується у нормах законодавства багатьох країн світу (Багамські Острови, Бермудські Острови, Велика Британія, Канада, Мальта, Франція, ОАЕ, США) та має репутацію універсального й узагальнюючого для спорідненого діапазону благ.

Із огляду на конклюдентне з національним законодавством розуміння складника «цифрові», тобто існує виключно у цифровому середовищі⁴, убачається відсутньою потреба досліджувати етимологічне походження останнього, його природи, областей застосування тощо. Виняток із цього становить категорія «цифрова форма», котрою, подекуди, оперують у профільному Законі України «Про цифровий контент та цифрові послуги» (п. п. 9, 11 ч. 1 ст. 2, ч. 2 ст. 6, ч. 1 ст. 13) [71]. В юридичній площині, у тому числі матеріалах, що формуються під час правозастосовної практики таке поняття не висвітлювалось в якості автономної одиниці. Більше того, у наукових колах йому також не присвячувалась значна увага ні у минулому, ані на сучасному етапі. Серед вагомих здобутків доцільно виділити спільний авторський доробок Г. Фороса і В. Жогова, котрі наголошують, що йдеться про спосіб фіксації змісту об'єктів права інтелектуальної власності [103, с. 16, 41-

⁴ Ч. 1 ст. 179¹ Цивільного кодексу України : Закон України від 16 січня 2003 р. № 435-IV // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/435-15#n6917>

42]. На нашу думку, зазначене є співмірним для характеристик правової природи самих цифрових активів, адже на останніх також може поширювати власну дію відповідний правовий режим. Окрім того, як слушно зауважує О. Кудь, під час розгляду поняття «цифровий» з'ясовано, що він передбачає такі аспекти: 1) числові комбінації; 2) кодування різних видів і способів; 3) переведення об'єктів у електронний формат (оцифрування, або диджиталізації) [78, с. 30]. Остання варіація докладно висвітлюється в одній із робіт О. Бутніка-Сіверського, який із-поміж іншого стверджує, що в цьому контексті йдеться про комп'ютерне оцифрування різної інформації з подальшою їх ідентифікацією та змогою розпоряджатися на власний розсуд [104, с. 98]. Виходячи з цього, перспективною вбачається гіпотеза, що легалізовані смислові конструкції («... отримання доступу ...» та «... забезпечує можливість їх використання ...») категорії «цифрове середовище» не охоплюють усі грані складника «цифрові». Поза увагою залишаються процеси щодо частки способів створення однойменних активів і певні інші технічні й технологічні позиції.

Відповідно, на законодавчому рівні у повній мірі не розкрита тематика цифрової компоненти – важливого складника досліджуваної дефініції. У цей же час, наявні правотворчі результати й науково обґрунтовані здобутки забезпечують формування уявлення про зміст, а також фундаментальні характеристики останньої.

Також стисло звернемо увагу на термін «актив», котрий представляє собою інший елемент базової одиниці й може нести смислове навантаження у випадку автономного використання. У популярних вітчизняних тлумачних словниках серед існуючих підходів уваги заслуговують наступні: 1) частина господарського балансу, яка відображає на необхідну дату всі матеріальні цінності, кошти й боргові вимоги, належні такому суб'єкту; 2) досягнення, надбання [105, с. 29]; 3) майнові права, що належать фізичній або юридичній особам; 4) економічні ресурси підприємства, що використовуються в господарській діяльності та перебувають у його

власності [105, с. 29], [106, с. 159], [107, с. 18-19; 108, с. 19]. Оксфордський словник з-поміж інших варіацій передбачає таке тлумачення, як «ресурси» [109]. Загалом, у теоретичній площині суть цієї дефініції є незмінною і, в загальних обрисах, передбачає наявність об'єктів, які мають цінність і вартість для фізичних чи юридичних осіб, держави тощо. Тобто, ключовим є саме питання їхньої цінності для котригось суб'єктів тих чи інших відносин.

Вказана логіка чітко прослідковується і в Міжнародному стандарті ISO 55000:2014 «Управління активами» [110]. Документом передбачено, що це ідентифікований предмет, річ або об'єкт, який вирізняється потенційною або дійсною цінністю для організації [110]. Як слушно зауважує В. Бацуца, у примітці до наведеного твердження міститься вказівка про можливість нематеріальної форми вказаної цінності [110], [93, с. 33], що, до слова, відповідає й нашим науковим поглядам. Орієнтуючись на розуміння, закріплене у пп. «іі» п. 1.2 Гарантійної угоди між Україною та Європейським Інвестиційним Банком «Логістична мережа (Модернізація та цифровізація Укрпошти)» від 06.10.2020 року [111], мова йде про існуюче і майбутнє майно, доходи і права будь-якого роду [111]. Такі концепти не суперечать і п. 1 ч. 1 ст. 1 Закону України «Про віртуальні активи» [70], у якому серед ознак однойменного поняття можна виділити «вартість». Попри те, що інша знакова група об'єктів цивільних правовідносин – «цифровий контент» у описі не містить вказівку на вартісну й ціннісну характеристики, вона знаходить своє місце у питаннях надання цифрового контенту та/або цифрової послуги [71]. Тобто, можемо стверджувати, що завідомо помилковою вбачається потенційна теза щодо відсутності критеріїв вартості й цінності відносно цифрового контенту.

Загалом же, зміст розкритих вихідних термінологічних одиниць дає мотивовані підстави стверджувати, що юридично виправдним і доцільним є обіг саме категорії «цифрові активи». Названі вище вагомими існуючі та потенційні складні протиріччя [78, с. 2-3, 6, 7-8], [100, с. 34-35; 93, с. 33-34, 61],

[101, с. 150-151, 152-153] не залишають альтернатив у частині відповідного вибору. Попри законодавчі орієнтири такі обґрунтовані бачення потребують додаткової комплексної розробки в рамках самостійних досліджень. Це сформує сприятливе підґрунтя для можливого ефективного удосконалення відповідних правових засад.

Виходячи з недостатньої розробки й здебільшого загального офіційного правового врегулювання (на міжнародному, міждержавному, подекуди федеральному та національному рівнях) пропонується також здійснити огляд щодо **типологізації (форм)** указаних активів. Не виникає сумніву, що в офіційних джерелах і наукових доробках часто матимуть місце різні підходи стосовно проявів цифрових активів у силу їхньої відносної новизни та малодослідженості. Об'єктивовані наміри щодо співставлення категорій «віртуальні активи», «віртуальні валюти», «криптовалюти», «цифрові активи», «цифровий контент», «цифрові речі» та інших можна спостерігати в знакових роботах В. Бацуци [133, с. 85, 86-87; 93, с. 86-87], О. Бутніка-Сіверського [104, с. 98], І. Гулейкова [112, с. 213-214], Б. Гуріна [113, с. 7-8], О. Дмитрик [114, с. 250-251, 252], О. Кудь [78, с. 29, 34; 79, с. 38], Н. Кучерявенка, Д. Білінського й Є. Смичка [77, с. 7-8, 31, 128], А. Овчаренко [115, с. 201-202], А. Проценко [116, с. 131, 133-134] та ін. Зважаючи на всі вищевикладені обставини у межах цього завдання нашого дисертаційного дослідження та ураховуючи його предмет, вважаємо за доцільне лише базово окреслити авторське бачення відповідної градації. Такий намір, із-поміж іншого, пояснюється спільним переконанням О. Вінник, Т. Попович і Б. Деревянко, які наголошують, що з'ясування різниці між останніми є важливим для визначення тактик управлінських заходів щодо них, а також ухвалення інвестиційних рішень і характеру правової регламентації відносин, котрі виникли чи матимуть місце у майбутньому [117, с. 197]. Це має вагоме значення й для нашої роботи, оскільки сформує основу для розробки оптимальних, адаптованих до відповідних параметрів механізмів, об'єктивованих у пропозиціях і рекомендаціях щодо удосконалення норм актів

вітчизняного законодавства, стратегічних документів та ін.

Орієнтуючись на представлені й обґрунтовані розуміння змісту і суті досліджуваної дефініції, саме таку категорію слід вважати вихідною точкою. Указане пояснюється тим, що йдеться про всі об'єкти, які існують у цифровій формі й обертаються в цифровому середовищі, а також мають певну цінність і вартість. Ураховуючи етимологічні наповнення вихідних дефінітивних одиниць, можна висловити перспективну гіпотезу, що будь-які об'єкти, іменовані «віртуальними активами», «віртуальними валютами», «криптовалютами», «цифровим контентом» й інші, обертаються в такому середовищі. Кожен із них складається з унікального буквено-числового коду (набору цифрових (двійкових) даних [79; 78, с. 31]), що дає змогу ідентифікувати останніх усіма учасниками. За наведених умов слушно вести мову про ту чи іншу форму цифрового активу, використовувану для різних цілей і потреб.

Окрім цього, істотні відмінності в таких буквено-числових кодах дають мотивовані підстави думати, що йдеться про декілька форм цифрових активів. При цьому кожен із об'єктів тієї чи іншої групи міститиме виключно унікальний код для власної персоніфікації в межах відповідної форми.

Наведені аргументи, на рівні з нещодавніми результатами правотворчої діяльності, указують не лише на існування таких форм, а й активний обіг їхніх представників. Наприклад, Н. Кучерявенко, Д. Білінський і Є. Смичок із числа таких форм виділяють наступні: 1) криптовалюти та токени; 2) фотографії, зображення, відео або ж документи, що виражені в цифровій формі; 3) пакети даних (великі збірки даних у цифровій формі тощо); 4) цифрові моделі; 5) цифрові товари (засоби цифрового збереження інформації та ін.); 6) доменні імена та засоби мережевої інфраструктури, як-от IP-адреси; 7) облікові записи користувачів (обліковий запис електронної пошти тощо); 8) інші форми [77, с. 7-8]. У висновку законодавчої комісії Великої Британії за 2022 р. [83] міститься така градація основаних форми аналізованих актів: 1) цифрові файли та цифрові записи; 2) облікові записи електронної пошти та

певні цифрові активи в грі; 3) доменні імена; 4) різні типи схеми викидів вуглецю; 5) крипто-токени [83, с. 109]. Представники міжнародної консалтингової компанії «PricewaterhouseCoopers» (PwC) і Організація економічного співробітництва та розвитку (OECD), незалежно один від одного, є прихильниками такого кількісного й видового складу: 1) криптовалюти; 2) стейблкоіни; 3) невзаємозамінні токени (Nonfungible tokens, NFT); 4) цифрові валюти центробанків (CBDC); 5) інвестиційні токени [118], [119]. В іноземних публічних джерелах часто зустрічаються наступні диференціації: 1) криптовалюти; 2) NFT; 3) стейблкоіни; 4) CBDC; 5) цифрові облігації; 6) токени [120] або 1) цифрові токени; 2) контент, цифрові активи, такі як зображення, відео, документи тощо; 3) пакети даних (великі колекції даних); 4) цифрові моделі (віртуальна реальність або збір даних Інтернету речей); 5) цифрові товари (ємність для зберігання); 6) доменні імена та активи мережевої інфраструктури, як IP-адреси, облікові записи користувачів (обліковий запис соціальних мереж, обліковий запис електронної пошти тощо) [121]. Відповідно, у науковій і фаховій сферах міститься ряд поглядів на критерії типологізації (форм проявів) цифрових активів.

Більше того, в офіційних документах міжнародного й іноземного походжень також зустрічаються базові або остаточні градації цих активів. Так, у Рекомендаціях Європейського управління з цінних паперів і ринків (European Securities and Markets Authority – ESMA), які предметно присвячені виявленню потенційних ризиків, за цим вектором їх поділяють на ті, що можуть розцінюватися фінансовими інструментами або ж навпаки [122]. Як зазначає О. Черних, французьке законодавство налічує дві загальні форми цифрових активів, а саме: 1) токени, що включають права, які можуть бути випущені, зареєстровані, збережені та передані електронним шляхом у випадку їх не класифікації фінансовими інструментами; 2) будь-які цифрові представлення вартості, які не випущено та не гарантуються центральним банком або державним органом, необов'язково прив'язані до законно встановленої валюти й не мають юридичного статусу валюти або грошей, але приймаються

фізичними або юридичними особами як засоби обміну, що можуть передаватися, зберігатися, а також реалізуватися різними способами в електронному вигляді [123]. У Швейцарії офіційно панує підхід щодо поділу їх на: 1) інвестиційні; 2) службові (сервісні); 3) платіжні; 4) гібридні; 5) інші [124]. У Законі Республіки Мальта, прийнятому в 2018 р., який регламентує сферу первинних пропозицій віртуальних фінансових активів і віртуальних фінансових активів, а також унормовує питання створення допоміжних або побічних засобів форматування, міститься наступна градація: 1) віртуальний токен; 2) віртуальний фінансовий актив; 3) електронні кошти; 4) фінансовий інструмент, котрий, по суті, залежить від технології розподіленої книги або використовує технологію розподіленої книги [125]. У законодавчому акті штату Род-Айленд США, що стосується зростання блокчейну від 2022 р., йдеться про таку градацію: 1) цифрові споживчі активи (digital consumer assets); 2) цифрові цінні папери (digital securities); 3) віртуальну валюту (virtual currency) [126]. Натомість, на рівні Європейського парламенту вже давно оперують двома загальними групами: 1) суверенні; 2) приватні [123]. Ураховуючи зазначене, можемо стверджувати, що в офіційних документах провідних держав світу ще не сформувалася уніфікована конклюдентна позиція щодо форм цифрових активів, і законодавство кожної окремої країни встановлює свої ексклюзивні форми. Убачаємо, що її відсутність продиктована наведеними вище істотними обставинами, а також специфіками правового врегулювання у тій чи іншій країні та рівнем теоретико-методологічного забезпечення й характером і ступенем суспільних запитів.

Проводячи своє дослідження, ми дійшли висновку, що у відомостях різного походження зустрічаються різні підходи щодо бачення кількісного й видового складів типів (форм) цифрових активів. При цьому відзначаємо, що численний їх орієнтовний спектр, крім позитивних сторін для економіки, несе й значну кількість загроз і ризиків, вартих нагальної уваги. Виходячи з усвідомлення істотних відмінностей багатьох різних параметрів останніх, відповідно слід розглядати й значний перелік явних і потенційних таких

факторів.

У контексті поточних вітчизняних правотворчих реалій для нас також важливим є співставлення досліджуваної одиниці із категорією «віртуальні активи», котра перебуває в офіційному обігу. При цьому ми свідомо залишаємо поза увагою інший легальний термін «цифровий контент» та популярний із позиції дослідницької уваги й практичного використання «криптовалюти». Зазначена логіка пояснюється тим, що до цифрового контенту відносяться лише комп'ютерні програми, застосунки, відеофайли, аудіофайли, музичні файли, цифрові ігри та електронні книги [71], що змістовно вужче від аналізованого явища. Натомість, криптовалюти є однією з форм віртуальних активів, про що можна зробити висновок на підставі аналізу багатьох норм Закону України «Про віртуальні активи» [70], результатів досліджень багатьох вітчизняних науковців, таких як В. Іванюк [127, с. 47, 53, 73], В. Логойда [128, с. 155-156; 129, с. 6, 25, 214], А. Овчаренко [115, с. 201], В. Сословський, В. Косовський [130, с. 239] та ін., а також фахівців визнаних міжнародних інституцій: Європейська банківська організація у 2014 р. [131], Європейський центральний банк у 2015 р. [132] тощо. Тому саме ініційоване нами порівняння має перспективне значення для нашого дослідження з точки зору уникнення прогалин і суперечностей.

Власне дискусії щодо зіспівставлення цих категорій точаться не лише у вітчизняних, а й іноземних наукових і фахових колах. Багатовекторність підходів до визначення поняття останніх, відсутність єдиних стандартів, стрімкий розвиток інформаційно-комунікаційних технологій породжують спірні дискусійні позиції.

Зважаючи на висловлене вище міркування про доцільність оперування терміном «цифрові активи» замість «цифрових речей», а також керуючись абз. 2 ч. 1 ст. 179¹ Цивільного кодексу України [99], можна слушно припустити, що «віртуальні активи» є нетотожною й вужчою одиницею. Іншими словами, йдеться про охоплення меншого спектру типів об'єктів, смислово належних до останньої категорії.

Наші висновки корелюється з поглядами деяких дослідників, у тому числі закордонних, які предметно опрацьовували висвітлену проблематику. Насамперед, висловлюється переконання, що віртуальні активи існують й обертаються виключно у віртуальному середовищі, тобто такому, яке, на думку О. Дмитрик, може бути імітовано за допомогою цифрової технології [114, с. 251]. Аналогічна за змістом точка зору представлена американською дослідницею М. Schilling, котра вбачає виключну роль цифрової складової і підкреслює її, з точки зору можливості існування віртуальних активів [134]. Інший італійський учений С. Catalini спільно з австрійським колегою J. S. Gans приходять до висновку, що саме цифрові активи є змістовно найширшою категорією, налічуючи значну кількість форм (право власності на валюту, цифровий контент, інтелектуальну власність, капітал, інформацію, контракти, фінансові та фізичні активи) [135, с. 3]. У «Рекомендаціях FATF з ризик-орієнтованого підходу до віртуальних активів та постачальників послуг» від 2019 р. [136]) стійко й активно оперують саме дефініцією «віртуальні активи» як робочим терміном. Більше того, у прим. «29» указаних Рекомендацій визначається, що «цифрові фінансові активи» («цифрові активи») є комплексним терміном, котрий налічує чисельніший діапазон позицій у сфері цифрових фінансових послуг, екосистем, уключаючи фінансову діяльність із використанням цифрових валют – як національних цифрових валют та цифрових валют, які не випущені та не гарантовані національним урядом [136, с. 50]. У своєму дослідженні ми свідомо уникнемо співставлення таких одиниць, як «цифрові активи» і «цифрові фінансові активи», лишень підкреслимо, що предметні поняття не є тотожними. Відповідно, під цими кутами зору категорія «цифрові активи», очевидно, є ширшою від «віртуальних активів». До того ж за допомогою функціоналу саме цифрових інструментів створюються й технічно та технологічно підтримуються певні автономні платформи, в яких можливий обіг тих чи інших віртуальних активів.

Ще одним вагомим аргументом саме на користь запропонованого нами наукового підходу є те, що цифровим активам може бути властива економічна

цінність і вартість. Тоді, як для віртуальних активів зазначена характеристика зустрічається в рази рідше, вони мають істотне значення лише у межах платформи, на якій обертаються. Підтвердженням нашої теорії є результати досліджень таких науковців, як С. Catalini і J. S. Gans [135, с. 22-23], І. Гулейкова [112, с. 213-214], О. Дмитрик [114, с. 251] та ін. Ми вважаємо, що в цьому контексті слушно вести мову і про вищу ліквідність цифрових активів (І. Гулейков [112, с. 213], О. Дмитрик [114, с. 251], R. Böhm, N. Christin, B. Edelman and T. Moore [137, с. 234-235], A. Zohar [138, с. 112-113]).

При цьому, як зазначає М. Schilling, відносно цифрових представників активів у глобальних масштабах спостерігається відчутніша потреба в їхньому правовому врегулюванні [134]. Із огляду на іноземні практики Великої Британії, ОАЕ, Канади, Сінгапуру, США, Японії та інших її думка вартує уваги. На відміну від України, у багатьох державах, із точки зору правової охорони, предметна увага прикута саме до змістовно ширшої категорії.

З огляду на це, виправданим є твердження, що категорії «цифрові активи» та «віртуальні активи» не рівнозначні і співвідносяться як змістовно ширша й вузла одиниці відповідно. Віртуальна складова залежить від цифрової, адже за допомогою потенціалу й функціоналу останньої є можливим існування та обертання різних її форм. У той же час, природною і виправданою вважається авторська гіпотеза, що в контексті цифрових активів слушно вбачати ширший спектр типів (форм) їх об'єктивізації.

Із-поміж іншого варто зауважити, що у зв'язку з недостатньою розробкою досліджуваної категорії в офіційній (на міжнародному, міждержавному, подекуди на федеральному та національному рівнях), науковій, а також фаховій (прикладній) площинах, не виправданим буде намір репрезентування власного бачення її типологізації (форм прояву). Експоненційні темпи розвитку в цій сфері та істотні зміни функціонального потенціалу інформаційно-комунікаційних технологій на фоні стрімких економічних трансформацій і цифровізації все більшої кількості процесів формують сприятливе підґрунтя для виникнення та популяризації нових форм цифрових активів.

Ініціатива стосовно авторської класифікації є невиправданою й із тієї точки зору, що відсутні напрацьовані та успішно апробовані критерії для вказаного упорядкування. Досвід наочно й неодноразово показує відсутність колективного переконання навіть відносно поняття криптовалют та їх похідного розмежування – найпопулярнішого типу віртуальних активів [70], що існують і перебувають в обігу ще з 2009 р. (В. Іванюк [127, с. 47, 53, 73], В. Логойда [128, с. 155-156, 157; 129, с. 6, 25, 40-41, 50, 96, 214] та ін). Тому окреслена проблематика передбачає надскладне розв'язання, для належного вирішення якої необхідний спектр відомостей із різних областей інтересу.

Беручи до уваги багатополлярність суджень щодо форм таких активів, зокрема і факт стрімкого прогресування й зростання кількості останніх, виникають додаткові складнощі у розробці авторського розуміння однойменної дефініції. Ураховуючи підходи, успішно апробовані у Звіті «Принципи Європейського інституту права щодо використання цифрових активів як цінних паперів» [81], висновку законодавчої комісії Великої Британії, опублікованому в 2022 р. [83] та інших визнаних документах пропонується репрезентувати декілька самостійних точок зору щодо змісту поняття «цифрові активи». Так, під **цифровими активами** слід розуміти: 1) блага з унікальними ідентифікаційними (буквено-числовими) кодами, що існують у цифровій формі й перебувають в обороті виключно у цифровому середовищі⁵, мають цінність і вартісну визначеність у платіжній, інших матеріальних і нематеріальних формах та можуть використовуватися необмежним колом осіб; 2) широкий, непрогнозовано змінний спектр типів об'єктів нематеріального змісту, що існують у цифровій формі й обертаються в цифровому середовищі; 3) прояв прав власності (володіння, користування, розпорядження), що передбачають оперування об'єктами нематеріального змісту у цифровому середовищі, у тому числі переважно безперешкодного доступу до них, незалежно від волі інших

⁵ Поняття «цифрове середовище» відповідає змісту п. 10 ч. 1 ст. 2 Закону України «Про цифровий контент та цифрові послуги»: Закон України від 10 серпня 2023 р. № 3321-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3321-20#Text>

учасників відносин, зокрема й держави та суб'єктів міжнародного права; 4) у залежності від намірів, різновид засобів і способів підвищення, або зниження рівня ефективності функціонування установ, підприємств, організацій та діяльності суспільства. На нашу думку, репрезентовані варіації персональних авторських визначень дають змогу сформуванню уявлення про цифрові активи й різні грані та форми їхнього прояву. Зважаючи на явну багатогранність і складність такого феномену, наведений підхід убачається оптимальним із числа поширених апробованих.

Безумовно, об'єктивований підхід до розуміння сутності останніх матиме на увазі існування властивостей та ознак останніх. До переліку **властивостей** явища цифрових активів 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 застосування 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. Щодо **ознак**, то перспективним бачиться такий діапазон позицій: 1) використання необмеженим колом осіб; 2) вираз майнових прав; 3) існування у цифровій формі та обертання в цифровому середовищі; 4) засоби і способи обороту, у тому числі фактично шляхом здійснення платежів на території України, обміну на майно (товари), роботи (послуги) тощо; 5) наявність унікального ідентифікаційного (буквено-числового) коду; 6) незалежність від наслідків впливу лівової частки заходів під егідою процесів різного рівня (міжнародного, міждержавного, національного, регіонального, місцевого, локального) та характеру (геополітичних, гео економічних, економічних, політичних, правових, соціальних, технічних, технологічних й ін.); 7) об'єкти права власності; 8) сукупність благ. Такі переліки властивостей і ознак на сучасному етапі

розробки аналізованої проблематики мають сформулювати змістовне уявлення про сутність досліджуваної одиниці. Безперечно, у ході розробки теоретико-методологічних, методичних і правових основ, а також подальшого розвитку самих цифрових активів очікуваними є зміни частки із таких характеристик.

1.3. Поняття, властивості, ознаки й класифікація загроз системі економічної безпеки України та місце і роль серед них цифрової складової

Серед численних атрибутів нинішньої формації системи економічної безпеки України чільне місце й виняткову роль мають загрози останній. Окрім типових чинників, явищ і тенденцій, визначених Розділом II Стратегії економічної безпеки України [3], за наслідками триваючої зовнішньої агресії росії відбулася трансформація поглядів на пріоритетність, характер і ступінь їх складності. Сукупний стійкий вплив геополітичних, геоekonomічних, технічних, технологічних й інших факторів, у тому числі ендogenousного походження, істотно видозмінив різні грані вітчизняної безпекової парадигми [139, с. 508; 140]. Наприклад, стратегічно визнана проблема «... уповільнення розвитку світової економіки в умовах пандемії COVID-19» [367], спричиненої коронавірусом «SARS-CoV-2» й рештою штамів цього захворювання давно втратила попередню вагу, поступившись багатьом іншим позиціям.

Поточна ситуація за низкою критеріїв, індикаторів і показників демонструє подальшу стагнацію із від'ємною динамікою [379]. Адже під приводом так званої російської «сво» реалізуються різні односторонні активні форми заходів, що стійко посягають на суверенітет, територіальну цілісність, недоторканність та інші національні інтереси України [29; 1]. Це, безумовно, має відношення і до економічної безпекової компоненти, більшість галузей якої часто перебувають в авангарді відповідних проявів деструкції.

У результаті цього, за даними, оприлюдненими у звіті Міжнародного валютного фонду у 2022 р. відбулося зниження багатьох важливих економічних

показників України, а саме: реальної заробітної плати, ВВП (на 37,2 %) та росту негативних величин, таких як рівень безробіття (до 40 %), інфляція тощо) [141, с. 4, 5]. Повномасштабне вторгнення російської федерації на територію України, за даними ООН, призвело до скорочення національної економіки більше ніж на 30 % у 2022 р. [142, с. 3], що ще раз аргументовано підтверджує вищевикладене.

На екваторі третього року повномасштабного вторгнення, лише за попередніми оцінками, сумарно українська економіка втратила орієнтовно біля 20 % свого потенціалу. Трудові ресурси скоротилися на 20 – 25 %, зростання зовнішнього боргу досягло понад 41 %, «ослаблення» гривні дорівнює 37 %, загальна інфляція склала близько 31 % [143]. Кількісно і якісно прогресуючі методи російсько-української війни пропорційно позначаються на загрозах економічній складовій, а також формують нові виклики й ризики для останньої. Безумовно, на таку ситуацію впливає й сумарна дія інших факторів різного характеру і походження. Проте часто такі здобутки цивілізаційного суспільства якраз використовуються агресором для цілей, котрі суперечать визнаним засадам міжнародного правопорядку.

Під вихідним терміном «загрози» у вітчизняних тлумачних словниках смислово прийнятні наступні трактування: 1) обіцяння заподіяння шкоди; 2) імовірність або ж неминучість виникнення чогось небезпечного (фактору, обставини й таке інше); 3) те, що може заподіювати ускладнення негативного характеру [105, с. 95], [106, с. 956], [107, с. 387], [144, с. 337]. К. Горячова та А. Пекін, незалежно одна від іншого, пропонують термін «загрози» розглядати в статусі однієї із численних форм (проявів) небезпеки [14, с. 66], [13, с. 23]. Підтримуючи такий науковий підхід, пропонуємо термін загрози розглядати як: 1) існування сукупності умов, що вказують на появу (подекуди невідворотну) деструктивних чинників для поточного бажаного стану об'єктів і перебігу процесів; 2) можливість скоювати дії або шляхом бездіяльності завдати деструктивних наслідків котримсь об'єктам; 3) безпосередня фізична дія на процеси, явища чи об'єкти, що зумовлює погіршення чинних умов [139, с. 509].

При цьому слушним бачиться авторське зауваження, що загрозами доцільно вважати як існування однієї, так і декількох названих умов або їх послідовне настання й реалізацію. У загальних обрисах, сутнісно йдеться про певний фактор (-и), активної чи пасивної дій, властивості якого деструктивно впливають на наявні параметри об'єктів, призводячи або підвищуючи імовірність настання небажаних наслідків із точки зору колективно схваленого належного становища у відповідній сфері.

Зазначене повністю відповідає мережі координат, у котрій обертається система економічної безпеки України як одна з головних підсистем провідної субстанції вищого рівня – національної безпеки України. Таку ж логіку можна прослідкувати в законодавстві [2], у тому числі лівової частки іноземних суб'єктів. Однак у цьому випадку законодавець, природно, обмежений рамками, продиктованими специфікою тієї чи іншої правової системи. Іншими словами, персоніфіковано загрози зводяться до одного знаменника, пріоритетно значимого для суспільства конкретної держави. У вітчизняній доктрині йдеться про конституційне визнання категорії «національні інтереси України», котрі смислово акумулюють у собі основні безпекові цінності, побічно відіграючи вагомую роль у формуванні критеріїв для визначення таких загроз.

Відповідно до п. 6 ч. 1 ст. 1 Закону України «Про національну безпеку України» під такими загрозами розуміють життєво важливі інтереси ключових учасників соціального діалогу (людини, суспільства і держави), реалізація котрих забезпечує державний суверенітет України, її прогресивний демократичний розвиток, безпечні умови діяльності, а також добробут її громадян [1]. Дійсно йдеться про найважливіші грані публічного й приватного життя, без ефективного забезпечення сувереном котрих хибно розраховувати на належний перебіг різних процесів, уникнення соціальної напруги, появи та розвитку небажаних тенденцій тощо. Тобто, це своєрідна центристська величина, навколо якої розбудовуються відповідні комплексні безпекові механізми для дієвого запобігання й протидії зазначеним подразникам.

Виходячи з наведеної вище логіки, загрози мають посягати або вже

руйнівню впливають на певні заходи у рамках реалізації всіх однойменних інтересів. Такий підхід корелюється із законодавчими положеннями й стратегічними орієнтирами, у яких розглядаються явища, тенденції і чинники, що унеможливають чи ускладнюють, або можуть унеможливити чи ускладнити реалізацію аналізованих інтересів, а також йдеться і про збереження національних цінностей України [1], котрі давно становлять вагому супутню складову.

Слід відмітити, що у п. 6 ч. 1 ст. 2 Закону України «Про Бюро економічної безпеки України» [147] поняття «ризик» ототожнюється з аналізованою нами термінологічною одиницею. У той же час, з огляду на етимологічний зміст дефініції «ризик» [148], схвалений підхід носить суперечливий характер.

У контексті економічної безпекової компоненти, об'єктивно, йдеться про вужче коло таких інтересів, виходячи з базового усвідомлення спектра і меж об'єктів предметної системи. На основі аналізу абз. 2 п. 1 Стратегії економічної безпеки України [3] ми дійшли висновку, що йдеться про такі фундаментальні позиції, як: 1) сталий розвиток національної економіки; 2) інтеграція України в європейський економічний простір; 3) поглиблення рівноправного взаємовигідного економічного співробітництва з іншими державами [3], [139, с. 509]. Визнана законодавством України типологізація основних національних економічних інтересів за більшістю складників корелюється з результатами досліджень відомих вітчизняних учених, таких як О. Діденко [149], М. Єрмошенко [150], С. Завгородня [151, с. 44], В. Онищенко й І. Рева [152, с. 7], Л. Шевченко [153, с. 17] та ін. При цьому слід зазначити, що наявні відмінності в таких трактуваннях зумовлені інакшим баченням конкретизації вказаних інтересів та ранніми, порівняно з набранням чинності профільного нормативно-правого акту, поглядами на предметну область. Ми вважаємо, що ці незначні за кількістю та змістом протиріччя, нерідко, є відображенням тогочасної безпекової політики в економічній сфері.

Зважаючи на вищевикладене, а також ураховуючи властивості категорії

«система економічної безпеки України» пропонується авторське бачення щодо розуміння предметної дефініції. На нашу думку, **загрозами системі економічної безпеки України** є тенденції, чинники і явища, котрі, як індивідуально, так і сукупно унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію основних національних економічних інтересів України. Убачаємо, що такий підхід оптимально відповідає законодавчим безпековим основам та гармонійно й обґрунтовано доповнює точку зору про зміст і сутність вітчизняної системи економічної безпеки в нинішніх реаліях.

Із точки зору забезпечення повноти і всебічності дисертаційного дослідження також важливим аспектом буде здійснення акценту на підпитаннях загальних **властивостей** й **ознак** вказаних загроз. Це матиме істотне значення з позиції розкриття й аналізу природи однойменних тенденцій, чинників і явищ під час зосередження уваги на цифрових аспектах.

Виходячи з аналогії розуміння категорії «властивості» відносно системи економічної безпеки України у контексті загроз, слід проаналізувати ряд унікальних характеристик. Серед числа основних за різними критеріями й показниками варто виділити наступні: 1) адаптивність (трансформація) до різних змін; 2) активна й, подекуди, стрімко прогресуюча конгломерація з іншими чинниками та явищами; 3) висока імовірність ураження об'єктів деструктивного впливу; 4) істотний вплив на формування багатьох тенденцій у цій сфері; 5) залежність від супутніх факторів (геополітичних, геоекономічних, політичних, правових, економічних, соціальних, технічних, технологічних тощо); 6) один із вагомих каталізаторів для появи нових і посилення дії існуючих викликів, загроз та ризиків для суміжних підсистем національної безпеки України; 7) різні темпи стійкої реалізації руйнівних намірів; 8) спрямованість на ключові національні економічні інтереси України; 9) часта латентність; 10) шкідливість. Вважаємо, що перераховані властивості формують змістовне уявлення про загрози досліджуваної системи.

Із приводу ознак, то, знову ж таки, застосовуючи попередні методи

наукового пізнання, спробуємо виділити основні з них. Так, відповідно до окреслених координат перспективною бачиться наступна градація: 1) визнання на офіційному рівні; 2) конституційне закріплення таких загроз як одних із пріоритетних, що впливає із ролі економічної безпеки; 3) спектр тенденцій, чинників і явищ, котрі, здебільшого, орієнтовані на одне коло типів національних інтересів України з подальшою диференціацією щодо похідних безпекових систем (виробничої, демографічної, енергетичної, зовнішньоекономічної, інвестиційно-інноваційної, макроекономічної, продовольчої, соціальної та фінансової) [31]; 4) участь держави, суспільства й кожної людини в запобіганні та протидії різним їх проявам. Переконані, що наведені загальні ознаки, доповнюючи їхні властивості, формують належне сприйняття останніх у сучасних умовах.

Знаковим аспектом можливо розцінювати й **класифікацію** такого типу загроз у багатьох джерелах, у тому числі – офіційних документах. Наприклад, у Законі України «Про основи національної безпеки України» [155], який утратив чинність, окремим блоком перераховувались загрози економічній компоненті. Багато вчених, науковців і фахівців у різні періоди також висловлювали свої погляди стосовно диференціації таких загроз. Серед тих, хто пропонував системи принципів й (або) критеріїв градації останніх, є А. Мазаракі та Т. Мельник [156, с. 10, 11-12, 14-15, 16], В. Мартиненко [157, с. 42-43], О. Маслій і А. Буряк [158, с. 30], О. Ківшик, а також М. Котелевець [159, с. 27-28], В. Приходько [160, с. 13], О. Пугач і С. Онищенко [161, с. 211-212, 213-214; 162, с. 31-32] та ін. Проте у своєму дослідженні ми будемо керуватись Стратегією економічної безпеки України [3], тому що частина загроз, про які вели мову науковці, носить морально застарілий характер і не орієнтована на реалії воєнного часу, а саме Стратегія була й залишається офіційним взірцем у предметній сфері.

Однак при цьому з-поміж численного спектру тенденцій, чинників і явищ, нагальних у нинішній період розвитку України, поза увагою залишилися загрози, які можуть виникати внаслідок **операцій із цифровими активами**

(цифрової складової). Тобто, попри експоненціальну зростаючу вагу, темпи і масштаби розповсюдження таких операцій, цьому аспекту не присвячена відповідна увага на офіційному рівні.

Так, п. 52 Стратегії національної безпеки України визначає, що ризики цифрової трансформації лежать у площині гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури [2]. До того ж самою Стратегією кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» від 26 серпня 2021 року визначено, що одним із вагомих подразників для функціонування збалансованої та ефективної національної системи кібербезпеки є швидко змінюваний цифровий світ [163], тобто існуючий і потенційний вплив інструментів цифрового середовища. Однак виходячи з офіційного розуміння поняття «національна система кібербезпеки», що міститься у ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», йдеться про сукупність відповідних заходів, покликаних забезпечувати кібербезпеку, а також здійснення захисту національних інформаційних ресурсів і кіберзахисту об'єктів критичної інформаційної інфраструктури (ч. 1 ст. 8) [164]. У свою чергу, цим же законодавчим актом визначено, що кібербезпека репрезентується як захищеність життєво важливих інтересів ключових учасників безпекового середовища під час використання кіберпростору (п. 5 ст. 8) [164]. При цьому правотворець зауважує, що наведена захищеність має забезпечувати: 1) сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 2) своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (п. 5 ст. 8) [164]. Заважаючи на таку суверенну позицію та враховуючи профілізацію механізмів кібербезпеки [163], йдеться про різні цифрові засоби, котрі руйнують, або можуть руйнувати існуючі системи (зазвичай, окремі її елементи) апаратного й програмного забезпечення захисту національних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури [380]. До слова, такий підхід корелюється з нормами Закону

України «Про критичну інфраструктуру» [165], де предметно розкриваються фундаментальні аспекти різних форм, способів і засобів захисту останньої. Тобто, розглядаються виключно технічні й технологічні грані широкої актуальної проблематики цифрових активів.

Однак, у фокусі інтересів нашого дисертаційного дослідження перебуватимуть загальні питання лише природи цифрових активів, операції з якими можуть деструктивно впливати на існування й перебіг економічних процесів. Інакше висловлюючи авторське бачення, зауважимо, що вони можуть бути і легалізовані державою та (або) легітимовані більшою частиною суспільства, але все одно становимуть загрозу існуючому стану й стійкості однойменних процесів. Очевидно, такий підхід іде в розріз політиці кібербезпеки, котра, об'єктивно, орієнтована на вужче коло граней цих аспектів.

Відповідно, ідеться про чинники та явища цифрового походження, котрі унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію основних національних економічних інтересів України, таких як сталість розвитку національної економіки, інтеграцію країни в європейський економічний простір, поглиблення рівноправного взаємовигідного економічного співробітництва з іншими державами [3]. Зважаючи на окреслені орієнтири категорії «система економічної безпеки України», варто розкрити питання стійкості цієї компоненти. Також, виходячи з об'єктивованої концептуалістики природи й типів загроз національній безпеці України, слушно і виправдано вести мову про деструктивні тенденції, що продукуються операціями із цифровими активами.

У якості додаткового вагомого обґрунтування звернемо увагу на відомі приклади руйнівного впливу чинників, тенденцій і явищ на економічні процеси, які знайшли своє відображення в наукових працях таких учених, як R Auer і S. Claessens [171], D. Cumming, Z. Glatzer і O. Guedhami [176], M. Isogawa [178], A. Максименко [166], B. Mizrach [177], S. K. Muthusamy і R. Kannan [166], S. Foley, K. Jonathan R., P. Talis J. [172]. Зокрема, необхідну конкретизацію

можна спостерігати в дослідженнях А. Максименка, який стверджує, що РФ ще з 2007 р. особливу увагу звертала на цифрові засоби ураження. Відомим прецедентним фактом їх застосування стала кібератака на Естонію, пізніше (2008 р.) вони передували вторгненню до Грузії. Починаючи з 2014 р., окрім інших активна мова йшла вже і про Україну [166, с. 43]. Безумовно, так звана «гібридна війна», яка велась РФ проти України, передбачала широке коло методів реалізації, систематично уражаючи різні безпекові вектори (у тому числі мають місце доведені факти завдання економічних збитків Грузії й Естонії [166, с. 44]). Не виникає сумніву, що економічні питання у певні періоди перебували в авангарді таких подій, порушуючи усталений порядок перебігу відповідних процесів.

При чому цей же науковець слушно зауважує, що описані події відносно Естонії змусили багато організацій (міжнародних, іноземних і національних) переглянути важливість ролі цифрових засобів із позиції реального деструктивного впливу на різні сектори безпеки. Більше того, навіть було створено Центр передового досвіду НАТО з питань кооперативного кіберзахисту (CCDCOE) [166, с. 43] та в подальшому інші інституції чи структурні підрозділи. Однак, із огляду на зміст викладеного у цьому та попередньому підрозділах, кіберзахист є лише одним із багатьох критичних аспектів реагування на вказані прояви.

Лишень на основі цього можна зробити проміжний висновок, що комп'ютерні програми, як одна з численних форм цифрових активів, є потужним глобальним інструментом впливу стосовно економічної стійкості. Таке судження доводиться не лише персональними міркуваннями і думками вчених та фахівців, а й конкретними фактами на практиці.

Як приклад, S. K. Muthusamy і R. Kannan помітили таку закономірність, що вказаний різновид технологій становить одну з проблем для корпоративного управління. Фахівці з'ясували, що середня прибутковість учасників господарських відносин знизилась за рахунок так званих цифрових інновацій. Оскільки по деяких аспектах істотно трансформувались механізми взаємодії з

контрагентами й іншими суб'єктами, змінились певні принципи конкуренції, а також це відобразилось на статтях витрат і прибутків [167]. Безперечно, такий погляд є неоднозначним і, за одних обставин, може бути виправданим, а за інших – суперечливим. Адже у частині технічної й технологічної складових цифрові новації можуть давати економічно ефективний результат, навіть на початкових етапах. Зокрема, такі явні й вагомні переваги, як зниження капіталовкладень, підвищення ефективності та продуктивності ухвалення рішень, зменшення витрат користувачами, ряд нових можливостей для створення унікальних товарів і послуг [168], інновації у бізнесі й покращення виробничих процесів у компаніях, в тому числі щодо багатьох ланцюгів поставок і взаємозв'язків між галузями [169] дають мотивовані підстави вести мову й про зворотні конструктивні рухи. Тому, у залежності від конкретної ситуації, можна стверджувати як про позитивні, так і негативні сторони цього питання. При чому нерідко йдеться про індивідуальний підхід, адже для одного суб'єкта господарювання такий інструмент може надавати вагомні переваги, порівняно з поточним станом, для іншого – ускладнювати котрісь, у тому числі супутні процеси.

Водночас, навіть попередньо негативний варіант розвитку подій у середньо- чи довгостроковій перспективі може спрямуватися в конструктивне русло. Логіка такої гіпотези пояснюється думкою J. A. Schumpeter, який увів у обіг поняття «творче руйнування», що має на увазі заміну новими застарілі технології. Наслідки від цих процесів і спочатку призводять до скорочення виробництва, але в подальшому істотно підвищують продуктивність за рахунок нових технологій [170]. Зазначене може бути прийнятним і для цифрових інструментів, котрі за період адаптації можуть пригальмувати чи зупинити певні заходи. Проте згодом, із високою долею імовірності, можливе зростання виробничого потенціалу й результатів однойменних робіт. Отже, вкотре підкреслимо тезу щодо можливості діаметрально протилежних варіантів перебігу виробничих процесів за рахунок інтеграції цифрових засобів.

Виходячи з цього, у якості загроз від операцій із цифровими активами

слід розглядати окремі випадки імплементації їх функціоналу до виробничих процесів. При неналежному підході такі варіанти розвитку подій могли призвести до істотних економічних наслідків, здебільшого, учасника господарських відносин.

У звіті фахівців (R Auer і S. Claessens) Федерального резервного банку в Далласі (США) «Cryptocurrency Market Reactions to Regulatory News» від 2020 р. зазначається про те, що висока волатильність «Біткоїна» («Bitcoin») як провідної криптовалюти у 2017-2018 рр. призвела до значних фінансових утрат багатьох інвесторів [171]. Безумовно, ці підсумки негативно відобразились на багатьох економічних показниках різних країнах. До того ж у непоодиноких випадках слушно вести мову про появу відповідних тенденцій, що вкотре доводить істотну вагу цифрових активів.

Криптовалюти як форми цифрових активів, будучи схильними до стрімкої й радикальної зміни вартості, негативно впливає на економіки країн. У результаті таких «поштовхів» багато учасників зазнають значних фінансових утрат, що створює ряд супутніх ризиків.

S. Foley, K. Jonathan R., P. Talis J. розкривають проблематику використання криптовалют у якості засобів платежу чи предметів обміну за товари, що вилучені з цивільного обороту й послуги, котрі носять неправомірний характер [172]. Окрім опосередкованого впливу на економіку, слід зазначити про стимулювання скоєння протиправних діянь, що посягають на різні складові безпекового сектору. Тобто, можемо константувати, що за рахунок появи нових способів і засобів вчинення відповідних дій завдається шкода національним інтересам, у тому числі економічним.

До слова, наведені можливості формують додаткове підґрунтя для появи й розвитку перспективних методів ведення гібридної війни агресором. Як зазначає згаданий вище А. Максименко, для росії вони забезпечили обхід багатьох санкційних обмежень, адже відслідкувати чи контролювати такі трансакції на нинішньому етапі є невиконуваним завданням [166, с. 44]. Відповідно, була побудована тіньова цифрова інфраструктура, що дала змогу

отримувати необхідні товари й послуги для досягнення військових, гуманітарних та інших цілей. Під різними кутами це позначалося на економіках багатьох країн, деформуючи визнану геоекономічну систему координат.

Власне явище «тіньової економіки» активно розвивається на теренах України завдяки потенціалу цифрових інструментів. Попри законодавчу неможливість використання тих же віртуальних активів у статусі засобів платежу на території України чи предмета обміну на майно (товари), роботи (послуги), обіг останніх за такими цільовими призначеннями – типова практика сьогодення. За словами Віцепрем'єр-міністра з інновацій, розвитку освіти, науки та технологій – Міністра цифрової трансформації М. Федорова у 2021 р. щоденний обіг лише віртуальних активів становив 1 млрд грн. Зауважено, що відповідні трансакції перебувають «у тіні» й відповідно національна економіка недоотримує значну кількість надходжень у вигляді податкових та інших обов'язкових платежів [173]. Із огляду на зміст прикінцевих і перехідних положень профільного закону щодо вступу в дію останнього та враховуючи триваючий попит стосовно вказаних активів [381], резонно припускаємо, що кількість відповідних операцій тільки зростатиме.

Безперечно, це лише поглиблює проблематику «тінізації економіки» за рахунок функціоналу цифрових засобів. Оскільки, саме завдяки маніпуляціям із їх участю створюються відповідні засоби та способи для обігу наведених активів та інших інструментів, паралельно руйнуючи легалізовану економічну систему.

Наведені й інші факти деструктивного прояву функціоналу цифрових інструментів засвідчують реальний істотний вплив на характер і темпи перебігу багатьох економічних процесів. У підсумку, нерідко, це призводить до багатьох штучних перепон, позначаючись на відповідних показниках. Тобто, у контексті економіки, зворотна сторона аналізованих активів інколи передбачає ускладнення або унеможливлення реалізації основних національних економічних інтересів України.

Зважаючи на стрімко прогресуючий феномен цих технологічних явищ, до

них давно прикута увага в різних відомствах та з боку незалежних фахівців і науковців (додатково див А. Максименко [166, с. 44] та ін.). У результаті чого, світ побачила не одна така класифікація, переважно подібного змісту.

Так, у публікації «Digital Asset Risk Assessment: A New Paradigm in Risk Management», оприлюдненій у 2022 р., наголошується на існуванні широкого спектра ризиків від активного впровадження цифрових активів [174, с. 3]. Попри те, що ми не відстоюємо позицію ототожнення категорій «загрози» і «ризик», усе ж у вітчизняній безпековій парадигмі вони перебувають поряд та доповнюють одна одну. Виходячи з такого підходу можемо припустити, що й загроз цифрового походження для економічного сектора буде вдосталь.

У контексті проблем управління цими активами, що має значення й для економічної компоненти, в одному з іноземних видань йдеться про такі аспекти: 1) послідовність і якість; 2) безпека та відповідність; 3) співпраця та інтеграція; 4) масштабованість і продуктивність; 5) вимірювання та оптимізація [175]. Однак у цьому аспекті йдеться про розширене бачення вказаних загроз, що має як переваги, так і недоліки, у рамках нашої тематики.

D. Cumming, Z. Glatzer і O. Guedhami вказують на існування таких загроз для економічної безпекової складової від операцій із цифровими активами: 1) «творче руйнування»⁶ [176] (*переважно в якості ризику – автор*); 2) волатильність криптовалют [176]; 3) значне споживання електричної енергії під час майнінгу⁷ й обороту криптовалют [176]; 4) фінансова залежність [176]; 5) вплив на кредитні показники [176]; 6) способи для розвитку тіньової економіки [176]; 7) інше. На перший погляд може здатися, що деякі аспекти є притаманними виключно криптовалютам. Однак учені у репрезентованому напрацюванні декілька разів підкреслювали, що вони є одними з форм якраз цифрових активів [176]. Тому, зважаючи на їхні об'єктивовані підходи, наведений спектр загроз вартий уваги у рамках нашого дисертаційного

⁶ Додатково див Schumpeter, J. A. (1976). *II. Capitalism, Socialism, and Democracy*, 1942 (5th ed.,). George Alwin & Unwin (Publishers) Ltd., First published in the UK in 1942. 460 p.

⁷ Майнінг – це видобуток цифрової валюти за допомогою спеціального обладнання, який здійснюють учасники мережі. Додатково див Що таке майнінг криптовалют? *Веб-портал: WhiteBIT*. 2023. URL: <https://blog.whitebit.com/uk/what-is-cryptocurrency-mining/>

дослідження.

Так, слушно врахувати результати наукових досліджень В. Mizgach, який є прихильником такої градації загроз: 1) волатильність; 2) операційні ризики; 3) шахрайство; 4) «мертві» (неіснуючі) монети; 5) відсутність застави (забезпечення частки активів); 6) високе енергоспоживання; 7) ціни комісії за окремі типи цифрових активів; 8) репресії з боку урядів певних країн; 9) тривалість торгів активами на біржах; 10) високочастотна торгівля⁸; 11) значна вартість окермих цифрових активів [177]. Однак М. Isogawa відмічає, що перспективним є наступний перелік ключових загроз: 1) хакерство; 2) фішинг⁹; 3) зловмисне програмне забезпечення; 4) соціальна інженерія¹⁰; 5) внутрішні загрози (стосуються питань, пов'язаних із співробітниками або іншими інсайдерами, які мають доступ до конфіденційних даних або програмного забезпечення) [178]. У інших наукових публікаціях фахового спрямування зустрічаються й такі диференціації: 1) керування мережею; 2) форки¹¹ та аірдропа¹² цифрових активів; 3) унікальні особливості цифрових активів; 4) волатильність цін; 5) оцінка та ліквідність; 6) кібербезпека; 7) непрозорий спотовий ринок; 8) біржі цифрових активів, посередники та зберігачі; 9) нормативно-правовий ландшафт; 10) технології; 11) комісії за трансакції; 12) відсутність регульованої схеми страхування захисту; 13) шахрайство та афери [179]. Наведені поділи форм цифрових активів свідчить про поступальний і, попри парадоксальність, стрімкий

⁸ Високочастотна торгівля – це складна автоматична торгівля, в процесі ведення якої використовуються потужні комп'ютерні програми. Додатково див Що таке високочастотний трейдинг, що таке HFT. *Веб-портал: Біржовий університет*. 2024. URL: <https://www.buniversity.com.ua/blog/shho-take-visokocastotnii-treiding-shho-take-hft#:~:text=%D0>

⁹ Фішинг – це один з різновидів шахрайства в інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів. Додатково див Що таке фішинг і фішингова атака. *Веб-портал: HOSTIQ*. 2024. URL: <https://hostiq.ua/blog/ukr/internet-phishing/>

¹⁰ Соціальна інженерія – спосіб зламу, в якому використовуються психологічні методи для обману людини. Додатково див Що таке соціальна інженерія *Веб-портал: NADIYNO*. 2023. URL: <https://nadiyno.org/shho-take-soczialna-inzheneriya/>

¹¹ Форк – це створення нової гілки від коду, що вже існує, для початку іншого проекту. Вона може розвиватися незалежно від основної, проект може мати опції, недоступні у початковому варіанті. Додатково див CryptoDiffer N. Що таке форк? Яке значення він має для блокчейну та чому відбувається. *Веб-портал: ЦЕКРИПТО*. 2023. URL: <https://tsecrypto.com/article/shho-take-fork-yake-vin-znachennya-dlya-blokchejnu-ta-chomu-vidbuvayetsya/>

¹² Аірдроп — процес безплатного розподілу токенів серед учасників віртуальної спільноти Додатково див Що таке аірдроп криптовалют: детальний гайд. *Веб-портал: wbblog*. 2024. URL: <https://blog.whitebit.com/uk/what-is-airdrop-crypto-meaning/#:~:text=%D0>

розвиток відповідних чинників і явищ, а також появу нових загроз. Окрім того, це зумовлює виникнення значної частки тенденцій, опосередковано відображаючись на різних економічних безпекових складових.

Слід відмітити, що, ураховуючи неоднакові підходи до класифікації різних форм, методів, способів та засобів економічного руйнування, в іноземних джерелах є різні підходи до ризиків, загроз і викликів безпековій складовій. При цьому, доволі часто, у контексті цифрових і решти інструментів зустрічається теорія про акцент на ризиках для економіки. Такі тактики також мають перспективне підґрунтя, адже йдеться про малодосліджені, прогресивні й прогресуючі фактори різного характеру та націленості.

До прикладу, представники центрального органу державного управління США, що здійснює контроль за виконанням закону про товарні біржі – Комісії з торгівлі товарними ф'ючерсами, в одному із опублікованих звітів фокусували увагу якраз на ризиках від аналізованих активів. А саме йдеться про такі з них: 1) операційні (торгівля без контролю, непослідовний захист клієнтів тощо); 2) кібербезпеки (хакерські атаки, втрачені або вкрадені особисті ключі та ін.); 3) ринкові (волатильність, новизна, ліквідність тощо); 4) шахрайство (влив соціальних мереж, маніпулювання даними) [180]. Аналогічний підхід можна прослідкувати в роботі С. Soto, котра, присвячуючи увагу проблемам управління цифровими активами, зосереджується саме на ризиках від операцій із останніми [181]. Автори звіту «Регулювання цифрових активів: Інсайти юрисдикційних підходів» [182], представленого у жовтні 2024 р. на Всесвітньому економічному форумі, також за відповідними позиціями, попри точкові вказівки на загрози, змістовно превалюють ризики від аналізованих активів. Ураховуючи вищевикладене, можемо стверджувати, що зазначена проблематика, попри явну та аргументовану гостроту, вимагає змістовної і всебічної наукової розробки не тільки в Україні, а й усьому світі.

З огляду на репрезентовану тематику дисертації, важливим є питання впливу та ролі операцій із такими активами на зміст, сутність і темпи перебігу економічних процесів. Так, у абз. 1 Розділу 1 «Вступ: кібербезпечна цифрова

трансформація в складному середовищі загроз» Стратегії кібербезпеки ЄС на цифрове десятиліття (The EU's Cybersecurity Strategy) від 2020 р. прямо вказано, що економіка, демократія та суспільство європейської спільноти як ніколи залежать від безпеки та надійності цифрових інструментів та підключень [183, с. 1]. До того ж, у цьому документі наголошується, що вказана діяльність посягає на міжнародну безпеку та стабільність [183, с. 2], а також наводяться приклади типових загроз від відповідних операцій (заподіяння фізичної шкоди, викрадення державних та промислових даних, що охороняються законом, доступ до персональних даних, «сіяння» недовіри та послаблення соціальної єдності) [183, с. 2]. Безумовно, і згаданий вище звіт «Регулювання цифрових активів: Інсайти юрисдикційних підходів» також указує на ряд ризиків і загроз саме для економічної компоненти [182, с. 3, 4-5, 6]. Причому окрім міжнародних аспектів йдеться також і про іноземні держави з відповідними цільовими орієнтирами [182, с. 11-12]. До слова, в Україні теж мають місце вагомні зародки вказаної ідеології. Зокрема, відносно нещодавно прийнятий Закон України «Про стимулювання розвитку цифрової економіки в Україні» [184] якраз покликаний додатково забезпечити вирішення завдань, заради котрих функціонує система економічної безпеки України. Наведені вагомні, подекуди системоутворюючі приклади дають мотивовані підстави константувати про усвідомлення ролі операцій за участю цифрових активів із точки зору їхнього потенційного впливу на економічну складову. Прогресивний і стрімко змінний сукупний потенціал цих засобів обумовить необхідність комплексної розбудови відповідної правової бази, а також постійного моніторингу ситуації на всіх рівнях. Будь-яка альтернативна стратегія реалізації функцій держави щодо цього питання невідворотно послабить позиції країни у питаннях запобігання й протидії аналізованим загрозам.

Відповідно, слушно досліджувати реальний широкий діапазон загроз від операцій із цифровими активами, що можуть посягати на стійке функціонування системи економічної безпеки України. Новітні роботи, які

містять однойменні типологізації, вказують на невідворотне прогресування таких явищ і чинників у коротко-, середньо- та довгостроковій перспективах.

1.4. Міжнародні й іноземні стандарти та правові механізми з протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами

Зворотний бік цифровізації з-поміж іншого призвів до поступового усвідомлення потреби легалізації правових засад, що сформуєть базу для запобігання й протидії багатьом руйнівним проявам для економіки. Лише частина наслідків від впливу таких інструментів показала неабияку уразливість економічних систем, не залишивши вибору, насамперед провідним країнам за різними критеріями. Події, датовані ще 2008 р. (кібератаки РФ на Естонію [166, с. 43]), заклали підвалини для здійснення наукових розвідок і фахових напрацювань за вказаним напрямом. Хронологічно послідовні відомі широкому загалу факти лише підтвердили впевненість у своєчасності та доцільності розробки і впровадження механізмів реагування.

Відповідно, на сучасному етапі маємо ряд актів міжнародного й національних рівнів та різної юридичної сили, об'єктивованих у рамках реалізації політик в предметній сфері. Попри об'єктивну обмеженість, у силу властивостей цифрових інструментів, вони формують базові засади, в тому числі визначають стандарти для поведінки учасників відповідних відносин. У результаті чого має місце поступова розбудова механізмів із запобігання й протидії загрозам, що можуть виникати внаслідок операцій з цифровими активами.

Прийняті міжнародні нормативно-правові акти, з-поміж іншого, показують характер правових політик із питань протидії цим загрозам, тим самим формуючи відповідні стандарти. У контексті ЄС й окремих інших глобальних організацій це має виняткове значення, адже йдеться про документи, котрі обов'язкові для виконання багатьма країнами, зважаючи на

зобов'язання останніх. Відповідно вважаємо, що такого рівня актам має бути присвячена виняткова увага, особливо враховуючи поступово реалізовуваний намір до уніфікації стандартів щодо популярних форм цифрових активів.

Так, Міжнародною групою з протидії відмиванню брудних грошей (Financial Action Task Force on Money Laundering – FATF) було видано декілька фундаментальних звітів, присвячених питанням протидії загрозам у цій сфері. У заключному документі «Керівництво FATF з ризик-орієнтованого підходу віртуальні активи та постачальники послуг з переказу віртуальних активів», виданого 2019 року (далі – Керівництво FATF) [136], було остаточно вирішено, навколо якої дефініції варто розробляти похідне забезпечення. На відміну від попередніх звітів, увага в останньому була сконцентрована саме навколо поняття «віртуальні активи». У подальшому вказаний підхід позначився на деяких елементах профільного вітчизняного законодавства. Загальновідомо, що на прийняття саме Закону України «Про віртуальні активи» [70] побічно вплинуло згадане керівництво, при цьому зважаючи на суверенне становище української держави та рекомендаційний характер такого висновку. Більш того, до прийняття Керівництва FATF, окремі вітчизняні законопроектні ініціативи, такі як Проект Закону про обіг криптовалюти в Україні № 7183 від 6 жовтня 2017 року [185], Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні № 7183-1 від 10 жовтня 2017 року [186] та ін., передбачали введення в офіційний обіг поняття «криптовалюти». Саме зазначеним міжнародним стандартом було сформовано певний технічний вимір і встановлено орієнтири для розробки вітчизняного законодавства. На сучасному правотворчому етапі української державності увага сфокусована якраз навколо цієї категорії та її властивостей. Це можна дослідити у нормах Цивільного кодексу України (абз. 2 ч. 1 ст. 179¹) [99], законів України «Про віртуальні активи» [70], «Про цифровий контент та цифрові послуги» [71], «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»

(п. 8 ч. 2 ст. 6, абз. 5 ч. 4 ст. 11, ст. 14, п. 5 ч. 1 ст. 18) [244] та ін.

Зважаючи на предметну діяльність FATF та її наднаціональний рівень, питання стандартизації потрібно дослідити в контексті протидії засобам щодо легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Так, Розділ III «Застосування стандартів FATF для країн та компетентних органів влади» [136] містить рекомендації, які слід застосувати країнам-учасникам під час регулювання обороту віртуальних активів та діяльності постачальників послуг, пов'язаних із вказаними засобами. При цьому рекомендації носять усебічний характер, поширюючись на різні аспекти однойменної діяльності (ризик-орієнтований підхід, національна координація, трактування термінів, що стосуються коштів чи вартості, ліцензування, реєстрація, нагляд, моніторинг, превентивні заходи тощо) [136]. Іншими словами, аналізований документ містить широкий спектр стандартів, вартих уваги, в тому числі з позиції посилення ефективності й результативності заходів із протидії досліджуваним загрозам. До того ж предметна націленість перерахованих вище кримінально-караних діянь укотре наочно демонструє можливість їхнього впливу на певні економічні процеси, що є релевантним авторським міркуванням про зв'язок останніх.

Прояви стандартизації присутні і в Стратегії кібербезпеки ЄС на цифрове десятиліття (The EU's Cybersecurity Strategy) від 2020 року [183]. Необхідно вказати, що в ній наголошується увага на зростаючій залежності безпеки, енергетики, здоров'я, телекомунікацій, транспорту, фінансів від впливу цифрових інструментів [183, с. 1]. Зважаючи на такий зміст частини преамбули однойменного документа та його юридичні властивості, цілком закономірним є існування стандартів у кіберпросторі. Ураховуючи долучення України до багатьох інтеграційних процесів та усвідомлюючи виключну значимість кібернетичної складової, відповідні стандарти є обов'язковими до врахування та виконання в нашій країні.

Досить цікавим для дослідження став аналіз положень Рекомендацій

Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року [122]. Навіть при декларативності цього документа його орієнтири, ще іменовані стандартами, слід враховувати з позиції послідовної розбудови національної цифрової інфраструктури. На нашу думку, враховуючи потребу в комплексності таких систем і механізмів, це не омине й проблематику деструктивних факторів для різних безпекових середовищ. У відповідності до змістовного наповнення цього міжнародного нормативного акту зазначаємо, що в ньому розглядаються регуляторні наслідки, коли криптоактиви кваліфікуються як фінансові інструменти [122], положення про ринкові зловживання [122], компенсації інвесторам [122] тощо.

У сучасних правотворчих реаліях Європейського Союзу, при вирішенні завдань дисертаційного дослідження, доцільно дослідити Регламент (ЄС) 2023/1114 Європейського Парламенту та Ради ЄС від 31 травня 2023 року про ринки криптоактивів, а також про внесення змін до Регламентів (ЄС) № 1093/2010 та (ЄС) № 1095/2010 та Директив 2013/36/ЄС та (ЄС) 2019/1937 (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 – MiCA) (далі – Регламент MiCA) [189], котрий упорядковує низку питань, пов'язаних із оборотом саме криптоактивів на міжнародному рівні. Для нашого дослідження аналіз положень цього документа є важливим з огляду на європейський вектор розвитку України, коли в майбутньому наша країна та решта учасників цієї групи процесів зіткнуться з необхідністю приведення у відповідність власного національного законодавства правовим нормам визначених орієнтирів. Регламент має унікальне значення, адже закладає базові стандарти для обороту й надання послуг, пов'язаних із знаковою групою цифрових активів на теренах європейського простору.

Безумовно, певні грані такого широкого питання будуть розкриті й під кутом зору безпекових складових. Попри чітку вказівку на невисокий потенціал криптоактивів, саме в якості загроз фінансової стабільності (п. 5 вступної

частини) [189] допускається ускладнення ситуації за відповідних умов. Власне, сам об'єктивований намір щодо розбудови наднаціональних систем і механізмів регламентації відносин у предметній сфері вже є реальним та вагомим здобутком у забезпечення лівової частки процесів. Тому вказаний акт із позиції безпекових цифрових орієнтирів для національної економіки має надважливе значення й вартує окремої поглибленої і змістовної уваги.

Досліджуючи міжнародні нормативно-правові акти з питань обігу цифрових активів, ми дійшли висновку, що суб'єкти міжнародного права стали почали самостійно розбудовувати національні основи правового врегулювання обороту та способів адміністрування значної частини їх форм. Указане стосується й низки безпекових підпитань, котрі представлені у перерахованих актах і, на практиці, дадуть про себе знати в контексті цієї проблематики. Зважаючи на специфіку такого рівня правової регламентації, встановлені міжнародні стандарти вартують особливої уваги для України й інших держав-учасників ЄС. Однак, у переважній більшості країн, поки йдеться лише про засади легалізації відповідних ринків. Тому й про масштабні системи і механізми з протидії виявам деструкції від цифрових засобів зарано вести мову. Однак все ж певні базові речі щодо окремих напрямів, у тому числі на основі негативного досвіду, знайшли своє відображення в різних заявах декларативного характеру, а також були об'єктивовані в нормативно-правових актах. Іншими словами, також має місце стандартизація кроків, що вартує уваги в контексті необхідності розвитку українського законодавства.

Серед країн, котрі особливо виділяються в цьому аспекті, доцільно згадати такі, як Багамські Острови, Бермудські Острови, Велика Британія, Канада, Китайська Народна Республіка (Китай), Об'єднані Арабські Емірати (ОАЕ), Республіка Сінгапур (Сінгапур), США, Французька Республіка (Франція), Швейцарська Конфедерація (Швейцарія) та Японська Держава (Японія). Національні нормативно-правові акти у цій сфері предметно націлені на вирішення ряду питань у аналізованій сфері, тим самим формуючи стандарти поведінки при обігу цифрових активів. Зважаючи на безпрецедентну

складність і непрогнозований стрімкий розвиток більшості форм цифрових засобів такий досвід також вартує уваги в рамках дослідження.

У першу чергу необхідно дослідити неоднотипні правові політики, що є очевидним, зважаючи на об'єктивну полівекторність останніх. Чого лише вартує приклад Китаю, де криптовалюти є офіційно забороненими до обороту [190]. Проте саме там здійснюється значна кількість трансакцій від сумарної кількості у світових масштабах [191, с. 37]. На додаток до цього, керівництво країни непохитно лобіює ідею всебічного розвитку саме віртуальних активів [182, с. 12-13]. Зазначене вище, аргументовано доводить виняткову складність цієї тематики, паралельно стимулюючи до її розкриття під багатьма кутами зору.

Власне, виходячи зі попереднього аналізу іноземних результатів правотворчих діяльностей, ми прийшли до висновку, що провідну роль у правових системах провідних країн світу відіграє національне законодавство, яке повністю впорядковує та регламентує суспільні відносини у сфері обігу цифрових активів. Так, на Багамських Островах діє Закон «Про цифрові активи та зареєстровані біржі» від 2022 року (Digital Assets and Registered Exchanges (Amendment) Act, 2022) [192], який було доповнено відповідними змінами у 2024 році [193], на Бермудських Островах діє Закон «Про комерційні відносини з цифровими активами» 2018 року (Digital Asset Business Act 2018) [97]), у Канаді діє Закон «Про єдиний доступ до цифрових активів довірених осіб» від 2016 року (Uniform Access to Digital Assets by Fiduciaries Act 2016, UFADAA) [96], в ОАЕ Закон «Про цифрові активи» – Закон DIFC № 2 від 2024 року (Digital Assets Law DIFC Law No. 2 of 2024) [195], в якому особливо підкреслюється «економічна вага» таких активів [196] і Закон «Про безпеку» – Закон DIFC № 4 від 2024 року (Law of Security – DIFC Law No. 4 of 2024) [197] тощо. Саме законодавчими актами визначено загальні засади стосовно існування й обороту цифрових активів та адміністрування останніх. Тому при розбудові нашого національного правового поля закордонні стандарти, об'єктивовані в законодавчих актах, також варті уваги. Адже самі юридико-

технічні характеристики закону, зокрема з позиції його місця й ролі в ієрархії нормативно-правових актів, зазвичай, істотно не різняться між собою.

Безперечно, питання відповідних загроз висвітлено фрагментарно і має стосунок лише до певних напрямів санкціонованого державного впливу. Мова йде про такі аспекти, як легалізація (відмивання) доходів, отриманих протиправним шляхом, кіберзагрози, міжнародні трансакції, шахрайство, різні суміжні маніпуляції тощо.

Деякі питання щодо сприяння поступального розвитку вказаної сфери вартують уваги в контексті роботи Грошово-кредитного управління Сінгапуру (MAS), яким ужито низку заходів для досягнення відповідної мети [198]. На нашу думку, сінгапурські практики слід розглядати як взірцеві для українських реалій, у тому числі із позиції безпекових питань.

Стрімкий розвиток нормативно-правового забезпечення аналізованої сфери, у тому числі адаптації до міжнародних приписів [199], слід зосередити увагу на моделі Франції. Тамтешній підхід з-поміж іншого вирізняється оперуванням категорією «цифрові активи» у контексті фінансових відносин. Зазначені суспільні відносини у цій сфері регулюються Валютним фінансовим кодексом Франції (*Code monétaire et financier*) [200]. Дослідження його норм становитиме особливий інтерес щодо повноти і всебічності висвітлення аналізованої проблематики.

Зважаючи на багатогранність, складність, стійке й непрогнозоване прогресування, а також транснаціональність проблемного питання, уваги вартують міжнародні й провідні іноземні стандарти. Такий підхід позитивно відобразиться на уникненні фундаментальних прорахунків у аналізованій сфері, а також посилить колективний потенціал відповідних інститутів. До того ж він корелюється з орієнтирами ЄС, котрі передбачають уніфікацію стандартів правової регламентації відносин у цій сфері та є безальтернативними, якщо вести мову про статус такої політики.

Висновки до розділу 1

1. «Система економічної безпеки України» – концептуально нова категорія, яка передбачає значний потенціал і перспективу для подальших розвідок. Вона має виняткове значення для поступального та збалансованого розвитку організаційних і правових засад стійкого ефективного забезпечення перебігу економічних і суміжних процесів, запобігання та протидії різним проявам деструкції, посилення безпекового й оборонного потенціалів України тощо.

Будучи структурно приналежною до системи вищого рівня (національна безпека України), репрезентована понятійна одиниця за смислом акумулювала в собі цінності й орієнтири вихідних категорій («безпека», «національна безпека України» та «державна безпека»). У той же час вона предметно націлена на економічні вектори (збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній, забезпечення здатності конкурентоспроможності лівової частки вітчизняних економічних галузей у світі сприяння поступальному розвитку всього економічного сектору) державної політики за своєю сферою, роблячи відповідний внесок у забезпечення національної безпеки України.

Аналізовану вище систему доцільно й виправдано позиціонувати як самостійну субстанцію, що має унікальну структуру і включає численний неоднорідний елементний склад, сполучений широким спектром зв'язків. Зазначений мотивований опис надає реальні підстави позиціонувати її саме в якості автономної соціальної системи. На користь цього виступають також наявність самостійних базових мети і завдань, типові властивості й характерна сукупність ознак останньої.

Питання стійкого ефективного й результативного публічно-правового і колективного суспільного забезпечення має вкрай вагоме значення для економічної компоненти. З огляду на численний стрімко прогресуючий

діапазон викликів, загроз і ризиків останній, відсутність належного спільного реагування є передумовою для послаблення економічного потенціалу країни й безпекових можливостей загалом.

2. Категорія «цифрові активи» є недостатньо розробленою в офіційній, науковій і фаховій площинах попри істотний прогресуючий явний потенціал. Зважаючи на превалювання інтересу щодо суміжних явищ і процесів, у силу наявності міжнародних і законодавчих орієнтирів, предметна одиниця також містить ряд відмінних особливостей, котрі варті уваги.

На основі поглибленого і змістовного аналізу результатів міжнародної, іноземної (національної і подекуди федеральної) й вітчизняної правотворчостей, позицій представників провідних організацій, а також думок учених можна зробити висновок, що, здебільшого, їх розглядають в якості: 1) благ із унікальними властивостями (існування й оборот у цифровому вимірі (середовищі), обіг у спеціальних системах, унікальний код, вартісна та цінова визначеності тощо); 2) широкого й змінного діапазону типів об'єктів нематеріального змісту; 3) прояву прав власності; 4) засобу підвищення рівня ефективності функціонування певних суб'єктів.

Зазначена категорія не перебуває в обігу на законодавчому рівні, проте її властивості, сукупно із усталеними засадами цивілістики свідчать про потребу приділення уваги цьому аспекту. До того ж на користь цієї ініціативи виступають успішні правотворчі практики багатьох закордонних держав і міжнародних організацій.

Недостатній ступінь фундаментальної наукової розробки, здебільшого базове (загальне) юридичне унормування, а також відсутність конклюдентно схвалених критеріїв породжують дискусії у частині типологізації (форм прояву) цифрових активів. Однак вбачається встановленим і аргументовано доведеним факт, що репрезентовані активи є змістовно найширшою категорією. Завдяки потенціалу й функціоналу цифрових інструментів можливим стає існування та оборот решти похідних об'єктів (віртуальних активів, віртуальних валют, цифрового контенту тощо).

3. Формування відповідного нинішнім реаліям кількісного та якісного спектра загроз системі економічної безпеки України – одне з провідних завдань науковців, учених і фахівців. З огляду на їх властивості та враховуючи критичний стан багатьох економічних процесів на тлі триваючої гібридної війни, така проблематика нарівні із воєнними загрозами вирізняється центристською роллю. Відсутність належного комплексного реагування суттєво ускладнить із без того поточну безпекову й оборонну ситуації. Особливої важливості це набуває і внаслідок обмеженості ресурсного забезпечення, лєвова частка якого закономірно та безальтернативно задіяна для задоволення інших потреб (військових, геополітичних, гуманітарних тощо).

Наявний спектр чинників, явищ і тенденцій не відповідає економічним реаліям сьогодення, зумовлюючи нераціональне використання нинішнього потенціалу. Зважаючи на об'єктивні складні обставини, виходячи із багатьох статистичних даних і враховуючи погляди значної кількості публічних діячів, вказане є нагальною потребою сучасності.

Серед перспективних напрямів у рамках такого питання вбачається група загроз, що можуть виникати внаслідок здійснення операцій із цифровими активами (цифрової складової). Наочні приклади, міркування вчених і фахівців, у тому числі градації таких чинників й явищ, а також результати правотворчої діяльності на міжнародному рівні, в іноземному та вітчизняному законодавствах аргументовано доводять авторську гіпотезу. Причому в період так званого «цифрового десятиліття» виправдним є розрахунок на подальше їх прогресування з позицій форм прояву, ступеня складності, потенційної міри ураження, взаємозв'язків із іншими методами економічної деструкції тощо. Виходячи з цього, окреслений тип загроз має вагомий дослідницький інтерес і вартує змістовної розробки з позиції розробки адміністративного-правової регламентації.

4. Створенню ефективних та результативних механізмів запобігання і протидії маловідомим чинникам, а також явищам має передувати змістовний аналіз існуючих підходів для реалізації відповідних цілей. Виняткове значення

має усвідомлення саме засадничих положень, які визначають характер правових політик регламентації відносин у предметній сфері. Тобто мова йде про схвалені й об'єктивовані стандарти, на основі та із неухильним дотриманням яких проводяться заходи з протидії певним загрозам.

Зважаючи на багатогранність, складність, стійке й непрогнозоване прогресування, а також транснаціональність проблемного питання уваги вартують міжнародні й провідні іноземні стандарти та правові механізми. Такий підхід позитивно відобразиться на уникненні фундаментальних прорахунків в аналізованій сфері, а також посилить колективний потенціал відповідних інститутів. До того ж він корелюється з орієнтирами ЄС, котрі передбачають уніфікацію стандартів правової регламентації відносин у цій сфері (Керівництво FATF, Регламент MiCA та багато інших).

Питання стандартизації відповідних практик у контексті безпекової складової зводиться до таких аспектів, як легалізація (відмивання) доходів, отриманих протиправним шляхом, кіберзагрози, міжнародні трансакції, шахрайство тощо. Відповідні позиції об'єктивовані в установчих договорах, висновках, директивах, регламентах, рекомендаціях, рішеннях та інших документах, покликані залучити до їх наслідування якомога більше держав-учасників.

На рівні більшості розглянутих країн йдеться про об'єктивізацію таких стандартів у законодавчих актах, що зумовлено їх юридико-технічними властивостями та місцем у системі джерел права. Загалом, вони істотно не різняться від міжнародних орієнтирів і левова частка специфік продиктована особливостями національних правових режимів. Навіть попри переважну кореляцію з міжнародними основами вирізнятимуться особливості, продиктовані індивідуальними специфіками тамтешніх правових систем.

РОЗДІЛ 2

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК ОПЕРАЦІЙ ІЗ ОБОРОТУ ЦИФРОВИХ АКТИВІВ

Вивчення та всебічне і змістовне дослідження будь-якого об'єкта з позиції адміністративно-правової науки безальтернативно передбачає аналіз відповідного регулювання останнього. Зважаючи на його сутність і винятковий діапазон властивостей (Л. Головій, В. Курило та І. Курило [201, с. 119], В. Желінський [202, с. 278], Ю. Князева [203, с. 33], Я. Лакійчук [204, с. 119], Т. Стоєва [205, с. 302]), цей аспект не може залишитися поза увагою, ураховуючи формулювання тематики роботи.

У загальних обрисах наведене регулювання передбачає застосування особливих (галузевих) механізмів на поведінку учасників тих чи інших відносин. Вказані механізми врегульовані нормами адміністративного права [201, с. 119], [202, с. 278], [203, с. 33], [204, с. 119], [205, с. 302], що із одного боку доводить їх унікальність і важливість, а з іншого – відповідає концепції дисертаційної роботи. Тому предмет, а головне – отримані результати матимуть істотне значення для вирішення завдань заключного розділу нашого дисертаційного дослідження.

Зазначене регулювання налічує ряд самостійних напрямів, котрі сукупно охоплюють різні грані функціонування (життєдіяльності) об'єкта впливу. З огляду на властивості предметного явища та ураховуючи характер і тенденції адміністративно-правового регулювання, пропонується зосередити увагу щодо таких фундаментальних позицій: 1) адміністративно-правові засади; 2) суб'єкти; 3) взаємодія цих суб'єктів; 4) контроль та нагляд у предметній сфері. Відповідно, навколо таких позицій і будуть побудовані дослідження в межах цього, переважно практико орієнтованого розділу.

2.1. Адміністративно-правові засади з протидії загрозам системі економічної безпеки України, що виникають при проведенні операцій із цифровими активами

Безпосередньо зосереджуючи увагу на ґрунтовному аналізі специфіки вказаного регулювання, першими конструктивним кроком має стати власне визначення самих адміністративно-правових засад. Розуміння зазначених основ сформує орієнтири для належного висвітлення інших аспектів у цьому підрозділі, забезпечуючи змістовність роботи.

Також, маючи на меті уникнення теоретико-методологічних невизначеностей і суперечностей у подальшому, варто приділити увагу дослідженню термінологічної складової. Зважаючи на зміст вирішуваного завдання дисертації, пропонується зосередитися щодо категорії «засади», «правові засади» та «адміністративно-правові засади». Усвідомлення суті цих понятійних одиниць сформує сприятливе підґрунтя для авторської розробки дефініції «адміністративно-правові засади протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами». На додаток до цього отримані проміжні результати належним чином відобразяться на класифікації й персоніфікації вказаних засад відносно аналізованої сфери відносин.

Щодо поняття «засади», то у тлумачних словниках містяться наступні смислово відповідні трактування останнього: 1) основа чогось; 2) те головне, на чому базується, ґрунтується що-небудь; 3) вихідне, головне положення, принцип; 4) основа світогляду, правило поведінки; 5) метод, спосіб здійснення чого-небудь [105, с. 300], [106], [107, с. 419]. Виходячи з таких, роками підтримуваних суджень, можемо припустити, що мову доцільно вести про базис, на основі якого відбувається перебіг певних процесів чи існування котригось явищ. Його відсутність об'єктивно унеможливить бажаний стан речей або ж деформує наявну систему, забезпечуючи їй недосягнення більшості чи всіх поставлених цілей. Зміст указаних засад має корелюватися з іншими

вихідними положеннями суспільного устрою, сприяючи необхідній належній взаємодії із елементами решти систем, приводячи в дію спільні механізми.

Ми вважаємо, що зазначену категорію слід розглядати як методологічно широку одиницю, яка охоплює різні сфери суспільного життя. При цьому вона окреслює лише базові контури, природно не враховуючи специфіку частки процесів і явищ у динаміці та статиці. Зазначена обставина істотно обмежує дослідницький потенціал такої категорії, провокуючи на пошук оптимальних та науково обґрунтованих рішень.

У контексті спеціальності, за якою виконується дисертаційна робота, зважаючи на типову, роками визнану модель національної правової системи [88], [89; 90], [91] та ураховуючи численні дослідження, ми вважаємо, що доцільно буде оперувати категоріями «правові засади» й «адміністративно-правові засади». Відносно першої позиції, то в новітніх наукових розробках особлива увага їй приділена такими вченими, як Р. Бойчук [206, с. 22], В. Горбачевський і Я. Ліховицький [207, с. 93], Р. Козьяков [208, с. 141], Д. Кошиков [209, с. 168; 210, с. 101-102, 124-125], О. Меньяйлов [211, с. 13], О. Птухіна [212, с. 47], В. Староста [213, с. 52], А. Чанцева [214, с. 50-51] й багатьма іншими. Щодо її змістовного наповнення та сутнісних орієнтирів, систематизувавши наявні переконання з цього питання, вважаємо, що доцільно розглядати наступну градацію: 1) законодавчо передбачена можливість здійснювати що-небудь [207, с. 93]; 2) система нормативно-правового забезпечення, котра становить базис однойменного регулювання [206, с. 22] або нормативно-правових актів [212, с. 47] для таких цілей; 3) сукупність певних правил, закріплених у нормах права, що містяться в законах та підзаконних актах [209, с. 168; 210, с. 101-102, 124-125]; 4) спектр основних принципів, що забезпечені, реалізуються та гарантуються державою [211, с. 13], [213, с. 52], [214, с. 50-51]; 5) сукупність правових засобів (правові норми, правові відносини, акти застосування права, у тому числі індивідуальні акти управління) [208, с. 141]. З таких авторитетних сучасних поглядів можемо зробити висновок, що мова йде про базис, який

утворений за допомогою норм права, об'єктивованих у нормативно-правових актах, що входять до системи законодавства України. З огляду на думки більшості названих учених [206, с. 22], [209, с. 168; 210, с. 101-102, 124], [212, с. 47], [213, с. 52], мову слід вести не лише про принципи, зважаючи на класичне розуміння останніх [105, с. 693], [107, с. 1125], а й решту нормативних конструкцій. Це пояснюється тим, що наведені елементи правотворчої діяльності слугують обов'язковим взірцем для поведінкових реакцій учасників регульованих відносин.

Зазначена категорія, урахувавши її властивості, надає певні вагомі переваги для використання функціоналу останньої. Проте сформульована досліджувальна проблематика нашої роботи потребує спеціалізації та орієнтуру на державне й, можливо, самоврядне регулювання предметної сфери, чому якраз і зарадять «адміністративно-правові засади». Більше того, це забезпечить концентрацію саме навколо необхідних питань, уникаючи мультидисциплінарного підходу в котрому відсутня потреба на цьому етапі.

Як і розглянута одиниця, категорія «адміністративно-правові засади» часто є об'єктом досліджень провідних вітчизняних учених. Із переліку вагомих здобутків сучасності особливої уваги заслуговують напрацювання у виконанні таких публічних діячів, як В. Залужний [215, с. 95-96], М. Коваль [216, с. 159; 217, с. 46], В. Курява [218, с. 99; 219, с. 78-79], О. Остапенко, М. Ковалів, С. Єсімова, а також Л. Гулак [220, с. 73-74], Ю. Тарасюк [221, с. 121; 222, с. 74] та ін. Зважаючи навіть на попередній діапазон новітніх здобутків виділимо, на нашу думку, найбільш удалі з них, що стосуються змістовного наповнення цієї дефініції, а саме: 1) норми, предметом регулювання яких є процеси функціонування органів державної влади, процеси управління тощо [215, с. 95-96]; 2) сукупність адміністративно-правових норм, що фактично лежать в основі нормотворчої і розпорядчої діяльності органів виконавчої влади [216, с. 159; 217, с. 46]; 3) параметри (характеристики) суспільних явищ і правовідносин, котрі потребують урегулювання шляхом використання адміністративно-правових засобів [218, с. 99; 219, с. 78-79];

4) формально визначені правила поведінки, що становлять предмет адміністративного права і надають учасникам відносин юридичні права та покладають на них однойменні обов'язки [220, с. 73-74]; 5) норми, об'єктивовані у нормативно-правових актах [221, с. 121; 222, с. 74]; 6) інші міркування. Досліджуючи цю дефініцію, ми прийшли до висновку про відсутність консенсусу [216, с. 159; 217, с. 46], [218, с. 99; 219, с. 78-79] серед науковців щодо визначення зазначеного поняття, тому, з огляду на це, вважаємо, що ключовим критерієм для диференціації таких засад є галузева приналежність норм права і власне природа останніх. Наша гіпотеза корелюється з поглядами багатьох визнаних правників-теоретиків, які, за відповідним критерієм, поділяють на норми: 1) конституційного права; 2) адміністративного права; 3) кримінального права; 4) цивільного права; 5) інші [88, с. 138-139, 140], [89; 90, с. 281-282], [91, с. 147-148]. Зважаючи на спектр, у тому числі унікальних властивостей усіх цих груп, а також виходячи з десятиліттями усталених традицій щодо їх поділу за галузевим принципом, ініційований підхід заслуговує уваги.

Відносно норм адміністративного права, то їх зміст і сутність докладно висвітлені у знакових доробках таких учених, як В. Авер'янов [223, с. 110], К. Костовська, Ю. Назар та В. Середя [224, с. 27], Р. Мельник [225, с. 61], Н. Писаренко [226, с. 42], В. Хомулянський [227, с. 47] та ін. У цілому під вказаними нормами пропонується розуміти обов'язкові правила поведінки, метою яких є врегулювання суспільних відносин, що виникають, змінюються і припиняються саме у сфері державного управління [225, с. 61], [226, с. 42], [227, с. 47]. Предметний акцент на державну й самоврядну управлінські сфери виправдовує визначення та аналіз вказаної групи норм. Порівняно з іншими самостійними елементами конституційного, адміністративного, кримінального та цивільного права [88, с. 138-139, 140], [89; 90, с. 281-282], [91, с. 147-148]), саме їхній функціонал надає змогу реально розв'язати поставлені в дисертаційному дослідженні завдання.

Зважаючи на викладене, ураховуючи результати наукових досліджень

зазначених вище вчених та правозастосовну практику пропонуємо авторське визначення дефініції – «адміністративно-правові засади протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами». Так, **адміністративно-правові засади протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами** – це сукупність норм адміністративного права, об'єктивованих у нормативно-правових актах різної юридичної сили, які визначають мету, завдання, принципи, функції й інші адміністративно-правові способи та засоби, за допомогою яких здійснюється регулювання предметної сфери відносин. Слушним і обґрунтованим видається незалежне колективне міркування Д. Заброди й І. Литвина щодо обов'язкового їх закріплення у відповідних нормативно-правових актах [228, с. 49], [229, с. 117; 230, с. 19-20, 29]. Ми схвально відносимося до такого переконання, тим паче, що це доводиться певними конституційними принципами, пов'язаними зі питаннями оприлюднення волі суверена, а ч. 1 ст. 9 Закону України «Про правотворчу діяльність» [231] визначає градацію таких документів.

Зважаючи на відсутність у правовій площині категорії «цифрові активи», увагу слід зосередити на легалізованих формах її прояву. Доцільним є не загальний аналіз усього національного законодавства із цього питання, а лише дослідження норми адміністративного права, котрі регламентують загальну безпекову діяльність, а також заходи із забезпечення належного стійкого обороту віртуальних активів, цифрового контенту і цифрових послуг (санкціонованих форм цифрових активів). Ми у своєму науковому дослідженні виділили основні дотичні до визначеної проблематики з них, а саме:

1. Конституція України. З огляду на виправдану ієрархію, у першу чергу, це основний закон – Конституція України [29], яка, складаючись із норм прямої дії, визначає фундаментальні основи й провідні орієнтири вітчизняної безпекової політики. У контексті нашої тематики дослідження слід виділити ст. 17 документа, яка визначає найважливіші функції держави і справу всього

українського народу [29]. Серед нечисленних таких пріоритетних напрямів своє чільне місце відведено економічній безпеці як одній із особливо важливих. Зважаючи на вище доведену доцільність оперування саме категорією «система економічної безпеки України» замість економічної безпеки, рахуємо, що дієве забезпечення постійного функціонування такої системи також є одним із головних завдань.

Виходячи з цього, моніторинг нових реальних загроз із подальшим відповідним реагуванням становить об'єктивну необхідність сьогодення. Оскільки більшість аналізованих здобутків цивілізаційного суспільства, окрім багатьох переваг, можуть і загрожувати вітчизняним економічним процесам, то й увага до них має бути прикута з боку всіх учасників суспільних відносин. Відповідно, з-поміж іншого, роль Основного Закону на сучасному етапі державотворення зводиться і до передбачення необхідності покладення зобов'язань із виявлення й формалізації загроз від операцій із цифровими активами.

2. Міжнародні договори України. Наступною знаковою групою нормативно-правових актів доцільно й виправдано вважати міжнародні договори, котрі давно зайняли унікальне і вагоме місце у національній законодавчій мережі. Значимість останніх для вітчизняної правової системи доводять багато вітчизняних науковців, серед них: А. Албу [232, с. 84], М. Вернигора [233, с. 327], Ю. Градова [234, с. 32], Є. Зверев [235, с. 43], О. Кізлова [236, с. 105] та ін. Абз. 2 ст. 2 Закону України «Про міжнародні договори України» передбачено, що ці документи укладені у письмовій формі з іноземною державою або певним суб'єктом міжнародного права, який регулюються таким правом [237]. У цілому, в ході нашого дослідження ми проаналізували міжнародні договори, елементи чи правові механізми яких імplementовано до національного законодавства у сфері цифрових активів з метою підвищення ефективності регулювання цієї сфери за різними критеріям, індикаторами і показникам.

Україна, будучи активним учасником міжнародного діалогу та стійко

реалізуючи більшість відповідних зобов'язань, побічно гармонізує власне законодавство за багатьма векторами. У контексті репрезентованої теми й зважаючи на стан її розробки у міжнародному середовищі та іноземних країнах, доцільно виділити наступні документи: 1) Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом від 8 листопада 1990 року [238]; 2) Угода про асоціацію між Україною та ЄС від 27 червня 2014 року [187]; 3) Директива Європейського Парламенту і Ради (ЄС) 2015/849 від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, про внесення змін до Регламенту Європейського Парламенту і Ради (ЄС) № 648/2012 та про скасування Директиви Європейського Парламенту і Ради 2005/60/ЄС та Директиви Комісії 2006/70/ЄС від 20 травня 2015 року [188]; 3) Рекомендації Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року [122]; 4) Керівництво FATF [136]; 5) Регламент MiCA [189]; 6) інші акти. Вважаємо, що цю групу джерел слушно розглядати як елементи національного законодавства з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами.

3. Закони. Особливу роль у цій сфері відіграють вітчизняні законодавчі акти, що зумовлюється юридичною силою останніх, охопленням критичних аспектів та власне значимістю для документів нижчого рівня. Ч. 1 ст. 10 Закону України «Про правотворчу діяльність» визначає закони як вітчизняні нормативно-правові акти, які регламентують найбільш важливі суспільні відносини [231], що, безперечно, стосується і безпекових питань. Виняткову важливість законів для системи економічної безпеки України доводять відомі вітчизняні дослідники, такі як О. Бочковий [239, с. 44], В. Доненко, А. Кондратьєв [240, с. 43-44], Н. Мельник [241, с. 118-119], М. Рій [242, с. 243], С. Ткачук, Ю. Юринець [243, с. 150] й ін., підкреслюючи їх знаковість для всіх граней суспільного життя. До слова, практика виключого значення саме законодавчих актів у цій сфері має місце у іноземних країнах. Закон «Про цифрові активи та зареєстровані біржі» від 2022 року [192] діє на

Багамських Островах, Закон «Про комерційні відносини з цифровими активами» 2018 року [97] – Бермудських Островах, Закон «Про єдиний доступ до цифрових активів довірених осіб» від 2016 року [96] – Канаді, «Про цифрові активи» Закон DIFC № 2 від 2024 року [195] – ОАЕ, законодавчі акти різних штатів США та ін.

У вітчизняній системі економічної безпеки центральне місце, на нашу думку, відведене Закону України «Про національну безпеку України» [1] як основоположному нормативно-правовому акту з вихідними безпековими складовими: метою, завданням, функціям, принципами, суб'єктам реалізації відповідних заходів, демократичного цивільного контролю та ін. Якщо Основним Законом закладаються фундаментальні засади й провідні орієнтири безпекової політики, то аналізований акт формує контури вказаної політики, у межах і з дотриманням рамок котрих формуються механізми реагування на відповідні подразники. За такої постановки питання його роль хибно недооцінювати, оскільки всі похідні системи і механізми перебувають у взаємозв'язку, забезпечуючи необхідну одноманітність та збалансованість державної політики в безпековій сфері. Безумовно, питання цифрових засобів ураження в загальному їх розумінні не розкрито у цьому нормативно-правовому акті, навіть у рамках планування безпекової політики. Відповідно, він також не передбачає зобов'язання щодо затвердження спеціалізованої стратегії чи розробки планів і державних програм, проте, із огляду на законодавче трактування цифрового контенту¹³, в окресленому вимірі доцільно звернути увагу відносно кіберзагроз. Отже, можемо константувати, що певні прояви аналізованих чинників, явищ і тенденцій все ж перебувають у полі зору законодавця, хоча й під іншим кутом.

У частині протидії таким загрозам уваги вартує лишень Закон України «Про віртуальні активи» [70], зважаючи на інакше спрямування Закону України «Про цифровий контент та цифрові послуги» [71]. Тому зосередимо

¹³ П. 11 ч. 1 ст. 2 Закону України «Про цифровий контент та цифрові послуги»: Закон України від 10 серпня 2023 р. № 3321-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3321-20#Text>

увагу саме на документі, що присвячений різним фундаментальним питанням віртуальних активів.

Загальновідомо, що вказаний нормативно-правовий акт спрямований на регулювання діяльності учасників ринку віртуальних активів (будь-які особи, котрі здійснюють відповідні операції та постачальники послуг, пов'язані з оборотом указаних активів (п. 12 ч. 1 ст. 1 [70])). У цьому випадку вказана формація – безальтернативний стан речей із огляду на фізичну неможливість обмежувати чи унеможливити обіг самих криптовалют та більшості інших віртуальних активів [382].

Документом визначена компетенція провідних суб'єктів із реалізації державної політики у предметній сфері – Національної комісії з цінних паперів та фондового ринку (далі – НЦКПРФ) та Національного банку України (далі – НБУ). Під егідою мір державного регулювання ст. 16 цього акту визначено завдання та повноваження НЦКПРФ, частина із них націлена на недопущення виникнення різних загроз, у тому числі для економіки під час обороту таких засобів. Наступною статтею цього закону вже окреслено повноваження НБУ, неухильне ефективне й результативне здійснення яких має у певній мірі позитивно відобразитися на стійкості та темпах перебігу значної кількості економічних процесів.

Також документом визначено базові засади співпраці та координації (ст. 20 [70]), що має посилити колективні зусилля, у тому числі й із безпекових питань. Увага присвячена і тематиці контролю (ст. 22 [70]) за виконання відповідного законодавства та міжнародній взаємодії (Розділ V «Міжнародне співробітництво у сфері обороту віртуальних активів» [70]). Убачаємо, що названі міри, при належному застосунку відповідних інструментів, також матимуть вагоме значення у питаннях запобігання і протидії загрозам від цих й окремих форм цифрових активів.

Також, на нашу думку, важливим нормативно-правовим актом у сфері використання цифрових активів слід визнати Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом,

фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [244]. Ним передбачено ряд заходів, які реалізуються Державною службою фінансового моніторингу України (далі – Держфінмоніторинг) та іншими суб'єктами фінансового моніторингу, покликаних запобігати й протидіяти однойменним діянням. У законодавчому акті чітко визначається, що загрозовість віртуальних активів (за конкретних умов) (абз. 4 ч. 4 ст.11 [244]) є одним із новітніх засобів для досягнення таких неправомірних цілей. Відповідно, здійснення цих повноважень якраз і покликано мінімізувати чи знівелювати більшість деструктивних проявів від операцій із такими об'єктами.

У цьому аспекті варто послатись на Кримінальний кодекс України [245] та Кримінальний процесуальний кодекс України [246]. Так, першим актом визнана суспільна небезпечність і винність діянь, що розцінюються як легалізація (відмивання) доходів, одержаних протиправним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення (ст. ст. 209, 209¹) [245]. Окрім цього, слід погодитися з думкою А. Стебляно, яка вказує на важливу роль так званих «предикатних злочинів» (ст. 190. «Шахрайство», ст. 222. «Шахрайство з фінансовими ресурсами», ст. 364. «Зловживання владою або службовим становищем» та ін.) [247, с. 55-56, 57], що релевантне окремим аспектам указаної тематики.

Відносно Кримінального процесуального кодексу України [246], то ним урегульовані основні процедурні питання щодо досудового розслідування однойменних правопорушень. У цьому аспекті можна виділити закони України «Про організаційно-правові основи боротьби з організованою злочинністю» [248] і «Про оперативно-розшукову діяльність» [249] ч. 4 ст. 6 якими визначено, що наявність відповідних матеріалів від Держфінмоніторингу є однією з підстав для проведення однойменних мір [249]. Стосовно іншого документа, то ним визначені базові засади протидії явищу й проявам організованої злочинності, представники якої нерідко скоюють якраз названі правопорушення.

Також досить специфічними є норми Закону України «Про стимулювання

розвитку цифрової економіки в Україні» [184], котрими закріплено механізми, що можуть розцінюватися в якості превентивних мір із протидії руйнівним чинникам, явищам, а також тенденціям. Зокрема, ч. 2 ст. 12 цього закону визначено, що уповноважений орган – Міністерство цифрової трансформації України (далі – Мінцифри) забезпечує формування та реалізацію державної політики щодо розвитку та функціонування правового режиму Дія Сіті [184]. Узагальнено такі заходи передбачають визначення статусу резидента однойменного правового режиму, сприяння технічному й технологічному забезпеченню перебігу необхідних процесів, різні напрями контролю, у тому числі щодо дотримання законодавства, взаємодію з іншими державними органами, суб'єктами міжнародного права та компетентними інституціями іноземних держав тощо [184]. Безумовно, низка питань у рамках указаних кроків буде присвячена різним безпековим аспектам у регульованій сфері.

Перераховані й інші акти дають підстави стверджувати, що саме закони є найзмістовнішими документами, котрі регламентують безпекові заходи за репрезентованим напрямом. На основі їх нормативних конструкцій розбудовуються комплексні адміністративно-правові механізми, покликані забезпечувати невідворотне досягнення всіх безпекових намірів.

4. Підзаконні нормативно-правові акти. Заключною групою таких легалізованих форм, безумовно, є документи, спрямовані на реалізацію законодавчих цілей, завдань і функцій (ч. 1 ст. 17 [231]). Вони гармонійно доповнюють норми права, об'єктивовані в актах вищої юридичної сили, а також деталізують певні позиції й усувають більшість прогалів. Завдяки їм, на думку таких вітчизняних вчених, як Є. Гетьман [250, с. 110; 251, с. 98], А. Камінський [252, с. 66], Н. Обушенко [253, с. 104], Е. Шуберт [254, с. 213] та ін., якраз уже і повноцінно функціонують адміністративно-правові механізми, регулювання відносин у тій чи іншій сфері.

Зважаючи на нормативну логіку, як ми встановили, основного нормативно-правового акту в сфері економічної безпеки – Закону України «Про національну безпеку України» [1], лівова частка похідних питань розв'язується

шляхом розробки стратегій, державних програм, планів тощо. Водночас, такі документи затверджуються (схвалюються) якраз підзаконними нормативно-правовими актами, заповнюючи умовний вакуум у важливій сфері суспільних відносин і доповнюючи законодавчі інструменти.

Наочними та влучними прикладами можна вважати Стратегію національної безпеки України [2], Стратегію економічної безпеки України [3], Стратегію кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» [163], Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки [255] та багато інших. До слова, акцент на таких документах зумовлений їхньою приналежністю щодо обраної тематики наукового інтересу. Зокрема, п. 52 Стратегії національної безпеки України основним завданням системи кібербезпеки визначено гарантування кібербезпеки та кіберстійкості національної інформаційної інфраструктури насамперед в умовах цифрових трансформацій [2]. Очевидно, що такі положення знайшли відображення у Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» [163], у якій неодноразово загострюється увага на загрозах, продиктованих цифровим середовищем і його трансформаціями.

Можемо зазначити, що дотичний підхід міститься у Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [244]. Для належної реалізації норм, присвячених віртуальним активам, затверджено підзаконні нормативно-правові акти [256], як приклад – Порядок інформаційної взаємодії суб'єктів первинного фінансового моніторингу та Державної служби фінансового моніторингу України від 4 червня 2021 р. [257]. Із викладеного можна також зробити висновок, що присутність такої групи джерел є не лише важливою, а й необхідною в умовах потреби нормативної деталізації і конкретизації багатьох питань. З позиції правотворчої процедури їх скасування та зміна є реалістичнішою процедурою, порівняно із законодавчими актами. Це посилить

вітчизняний правовий інструментарій зі сторони адаптивності й оперативності, особливо в умовах стрімких і, переважно непрогнозованих, цифрових інновацій.

Відповідно, представлена група джерел також має істотне значення з точки зору адміністративно-правового регулювання предметної сфери. Їхні унікальні характеристики надають додаткові необхідні можливості для дієвого вирішення поставлених завдань.

У такому контексті можемо стверджувати про наявність в Україні сприятливого законодавчого підґрунтя для легалізації відповідних загроз та закріплення юридичного інструментарію задля можливості протидії останнім. Очевидні властивості законів і підзаконних нормативно-правових актів та схвалена ініціатива щодо посилення різновекторної цифровізації дає підстави розраховувати на успішну інтеграцію майбутніх інструментів із елементами діючих безпекових механізмів. Сукупно вони сформують підґрунтя для роботи відповідних інституцій, легалізувавши адміністративно-правове становище останніх із питань протидії досліджуваному типу загроз.

2.2. Адміністративно-правовий статус суб'єктів системи економічної безпеки України зі спеціальною компетенцією, що протидіють загрозам, які виникають при здійсненні операцій із цифровими активами

Практична реалізація заходів щодо запобігання й протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами, відбувається за рахунок функціонального впливу певних інституцій. Навіть при відсутності офіційного визнання й конкретизації відповідних чинників, явищ і тенденцій деякі напрями такої політики вже перебувають у полі зору. Зазначений стан речей, насамперед, пояснюється фізичною можливістю використання вказаних активів у якості засобів платежу і предметів обміну на майно (товари), роботи (послуги), попри законодавчу

заборону здійснення таких операцій щодо окремих їх форм¹⁴. Переваги від відповідних трансакцій й суміжних маніпуляцій [383] стимулюють до використання останніх в неправомірних цілях, що позначається на економічній складовій.

Їхня стійка поступальна інтеграція в різні сфери відносин, охоплених іншими, вже регульованими системами, передбачає залученість у процеси реагування відповідних суб'єктів. Такий підхід носить безальтернативний характер, адже будь-які відмінні моделі зумовляють появу небажаних ситуацій, особливо в затяжний виснажливий період під сукупною дією викликів і ризиків воєнного часу. Відповідно, навіть при незначній розробці окресленої тематики, все ж окремі її аспекти є предметом регуляторного впливу з боку деяких інституцій.

Безумовно, якщо вести мову про цілісне бачення, то слід ураховувати й роль суб'єктів із компетенцією загального характеру. Це стосується як націленості на багато сфер державного регулювання, так і власне поширення щодо різних аспектів цифрового середовища. Під таким кутом зору слушно й виправдано стверджувати про приналежність до суб'єктів системи економічної безпеки України наступних державних інституцій: 1) Верховна Рада України; 2) Президент України та Рада національної безпеки і оборони України; 3) Кабінет Міністрів України, Міністерство економіки України, Міністерство фінансів України та інші центральні органи виконавчої влади; 4) суди (місцеві загальні суди, відповідні апеляційні суди, Верховний Суд (Касаційний кримінальний суд, Велика Палата Верховного Суду); 5) та ін. Водночас, їх завдання та функції є зрозумілими [258, с. 244, 245; 259, с. 84-85] і не потребують додаткового висвітлення, отже, й відсутній дослідницький інтерес.

Інше питання – державні суб'єкти, які наділяються спеціальною компетенцією, що застосовується у разі проявів загроз при здійсненні операцій із цифровими активами. Особливо цілком обґрунтованим є дослідження

¹⁴ Ч. 7 ст. 4 Закону України «Про віртуальні активи» : Закон України від 17 лютого 2022 р. № 2074-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>

установи, яка забезпечує формування й реалізацію державної політики з питань цифровізації та цифрової економіки. Виходячи з завдань нашого наукового дослідження, вважаємо за доцільне визначити перелік таких державних установ, до якого включити наступні інституції: 1) Мінцифри; 2) Держфінмоніторинг; 3) НКЦПФР; 4) НБУ; 5) правоохоронні органи (Бюро економічної безпеки України (далі – БЕБ), Державне бюро розслідувань (далі – ДБР), Національне антикорупційне бюро України (далі – НАБУ), Національна поліція (далі – НП), Служба безпеки України (далі – СБУ)), а також міжнародну організацію по боротьбі з легалізацією та відмиванням доходів, одержаних злочинним шляхом – FATF. Із огляду на представлену класифікацію, сфокусуємо власну увагу щодо зазначених установ. Зважаючи на фрагментарність цих питань у нормативно-правовій площині, особливу увагу слід присвятити рівням та напрямам їх функціонального впливу.

Паралельно у такий спосіб можливо буде окреслити адміністративно-правове становище цих інституцій саме як суб'єктів, що протидіють загрозам, які виникають при здійсненні операцій із цифровими активами. Оскільки функціонування на тому чи іншому рівні та за певними напрямами передбачає реалізацію відповідної компетенції (повноважень, прав і обов'язків), а також матиме місце проявів решти атрибутів, нормативно приналежних досліджуваній установі.

Ініційований підхід релевантний класичним уявленням про категорію «адміністративно-правовий статус» та базовий елементний склад останнього [220, с. 49-50], [226, с. 39-40]. Відповідно, пропонована характеристика способів функціонального впливу всіх органів та їхня нинішня усіченість (обмеженість), із-поміж іншого, забезпечать висвітлення загального бачення адміністративно-правового статусу суб'єктів.

Репрезентована ініціатива семантично не йде в розріз етимологічному змісту категорії «статус», яка є визначальною для похідної термінологічної одиниці. У тлумачних словниках статус розглядається в наступних проєкціях: 1) становище, стан; 2) стан чого-небудь [105, с. 671]; 3) становище індивіда,

групи індивідів; 4) сукупність прав та обов'язків фізичних й (або) юридичних осіб; 5) соціальна роль кого-, чого-небудь; 6) інше [107, с. 1387; 108]. Стосовно інших елементів конструкції – «правовий» та «адміністративно-правовий», то вони були розглянуті й проаналізовані у попередньому підрозділі, що робить недоцільним буквально дублювання отриманих результатів.

Виходячи з цього, під **адміністративно-правовим статусом суб'єктів системи економічної безпеки України, що протидіють загрозам, які виникають при здійсненні операцій із цифровими активами** слід розуміти компетенцію (повноваження, права, обов'язки) та інші атрибути, визначені нормами адміністративного права, що сукупно окреслюють їхнє місце й визначають роль на всіх рівнях та за напрямками функціонального впливу. На відміну від засад, у яких йдеться про об'єктивізацію адміністративно-правових способів і засобів у актах чинного законодавства з метою їх легалізації, в досліджуваному питанні акцент зміщений саме на становищі інституцій у підвідомчих процесах.

Зокрема, у контексті рівнів – це фундаментальні ідеї, закладені в основу розробки державної політики, організації й реалізації певних заходів відносно предметної сфери [260, с. 4]. Можемо стверджувати про сукупність управлінських форм та методів вжитку певних кроків у місцевих [260, с. 4], регіональних [261, с. 469], [262, с. 6] чи загальнодержавних [263, с. 250-251] масштабах. Отже, у такому аспекті вважаємо за необхідне зосередитись саме на питаннях територіального санкціонованого впливу. Це матиме істотне значення, зважаючи на типові властивості аналізованих загроз, представлених і охарактеризованих нами вище. З огляду на існування дослідницького інтересу (І. Жмурко і Л. Федоришина [261, с. 469], П. Курмаєв [262, с. 6], А. Сава й Б. Сидорук [263, с. 250-251], Н. Шевчук [260, с. 4]) та враховуючи специфіку регульованої сфери, вказана позиція варта уваги.

Усвідомлюємо, що вітчизняна управлінська парадигма передбачає активну участь усіх суб'єктів публічно-правових відносин у міжнародних і міждержавних заходах, особливо на фоні євроінтеграційних процесів. У той же

час, попри парадоксальність цієї гіпотези, очевидним є й те, що одні суб'єкти особливо вирізняються в межах одного рівня (FATF), а решта іншого (Мінцифри, Держфінмоніторинг, НКЦПФР, НБУ, правоохоронні органи). Зважаючи на це, укотре аргументовано доводиться, що проблематика носить складний і багатогранний характер в сучасних умовах.

Відносно напрямів, то і їм присвячена неабияка увага в роботах вітчизняних науковців, особливо заслуговують уваги такі, як О. Бандурка, О. Литвинов, Є. Огородник [264, с. 42; 265, с. 300], Б. Гамалюк, Ю. Харун, М. Одрехівський, У. Когут [266, с. 26; 267, с. 80], П. Хряпінський [268, с. 118], А. Черненко, А. Шиян [269, с. 348]. Загалом, напрями прийнято розглядати як соціально значущі сторони функціонування держави, для реалізації яких задіяні всі її органи, а не окремі ланки. Із першою частиною ми висловлюємо згоду, адже дійсно мову слушно вести про провідні самостійні питання, з позиції належної реалізації зобов'язань держави перед населенням. Стосовно другого елементу термінологічної конструкції, то все ж доцільно вбачати залученість не всіх інституцій, а частину останніх. Багатополярність державної і самоврядної робіт, а також слідування дерегуляційним орієнтирам надає перевагу нашій гіпотезі.

Ураховуючи пропоновану систему координат, уже безпосередньо дослідимо участь згаданих інституцій у забезпеченні економічної безпеки України при проведенні операцій із цифровими активами. Отримані результати мають забезпечити уявлення про ступінь залученості держави у відповідні процеси з боку інституційного регулювання.

1. Міністерство цифрової трансформації України. Зазначена інституція наділена статусом головного органу в системі центральних органів виконавчої влади із забезпечення формування та реалізації державної політики у сферах цифровізації, цифрових інновацій і технологій, цифрової економіки й цифрового розвитку [270]. Саме від ефективності функціонування останнього залежать характер і темпи вказаних заходів. Законодавство України визначає, що Мінцифри має розробляти та проводити необхідні ефективні заходи із

розбудови вітчизняного цифрового середовища на загальнодержавному рівні з подальшим їх упровадженням щодо механізмів регіонального, а також місцевих спрямувань. Попри технічні й технологічні переваги вказаних інструментів, маємо зазначити, що все ж таки градація за критерієм рівності має місце за деякими аспектами діяльності.

Серед визначених перед міністерством завдань з узагальнення практики застосування відповідного законодавства, розробки проєктів нормативно-правових актів, Мінцифри бере участь у: 1) формуванні державної політики з питань криптографічного та технічного захисту інформації; 2) забезпеченні стійкого розвитку віртуальних активів (форм цифрових засобів), «блокчейну», токенизації й штучного інтелекту, 3) розбудові цифрової інфраструктури України [270]. Ця діяльність передбачає організацію протидії окремим загрозам вітчизняного цифрового середовища. Насамперед, ідеться про визначення характеру державної політики, у тому числі й безпекових прерогатив, формування, реалізацію та моніторинг ефективності державних санкційних мір, різні форми участі в розбудові систем захисту інформації, розвитку однойменних активів тощо. Ці й інші заходи мають значення з позиції ступеня готовності державного та самоврядного апаратів, економічних галузей і власне громадян до значної частини загроз українського цифрового середовища. Нормативно-правові засади, запроваджені Мінцифри, виконуються іншими центральними органами виконавчої влади для реалізації відповідних форм і методів державного управління, що стосуються тих чи інших граней предметного питання.

Окремо слід виділити таке завдання Мінцифри, як здійснення державного регулювання і нагляду в сфері запобігання та протидії легалізації (відмиванню) злочинних доходів, одержаних шляхом фінансування тероризму та фінансування розповсюдження зброї масового знищення відносно постачальників послуг, пов'язаних із оборотом віртуальних активів [270]. Враховуючи особливу важливість цього напряму у відповідному контексті, питання нагляду за відповідними діями має виключне значення. Зважаючи на

змістовне наповнення й сутнісні орієнтири категорії «нагляд» (на чому буде зосереджена увага у підрозділі 2.4), його ефективна реалізація – одна із запорук належного регулювання суспільних відносин у предметній області нашого дослідження.

2. Міжнародна група з протидії відмивання брудних грошей.

Зазначена інституція є суб'єктом міжнародного права, тому її функціонування виходить за умовні межі національних рівнів. Однак, Україна є стійким учасником різних заходів під егідою вказаної організації, визнаючи та приймаючи її рекомендації шляхом імплементації їхніх норм у вітчизняне законодавство. Ураховуючи це, цілком виправданим є включення установи до репрезентованої мережі і зумовлює дослідження напрямів роботи FATF.

Аналізуючи діяльність Міжнародної групи з протидії відмивання брудних грошей, маємо виділити такі основні напрямки її діяльності, а саме: 1) поширення відомостей стосовно заходів боротьби з відмиванням грошей на всіх континентах і в усіх світових регіонах; 2) моніторинг за неухильною реалізацією «Сорока Рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) від 25 вересня 2003 р. [271]; 3) огляд тенденцій, присвячених питанням відмивання коштів і реалізації відповідних контрзаходів (типологічні дослідження) [272]. Слід зазначити, що в діяльності FATF вагоме значення відіграє саме інформативна складова, з огляду на міжнародний рівень організації.

FATF постійно розробляє нові та модернізує вже наявні практики щодо відповідних стандартів із протидії відмиванню злочинних доходів та фінансуванню тероризму. Серед таких моделей останнім часом особлива увага привернута до форм цифрових активів, котрі, як відомо, є перспективним і популярним засобом для скоєння однойменних протиправних діянь. Рішення, об'єктивовані в методологіях і рекомендаціях цієї установи, мають вирішальне значення для розробки й приведення у відповідність національних правових механізмів реагування щодо дії багатьох відповідних подразників.

Іншою перевагою обраного підходу є долучення FATF як до

міжнародних, так і міждержавних заходів із запобігання й протидії відповідним загрозам. Зокрема, це забезпечує додаткове стимулювання національного економічного розвитку та посилює стійкість галузей України щодо руйнівного впливу частки загроз ендогенного й екзогенного походжень.

3. Державна служба фінансового моніторингу України. Установа є уповноваженим Україною суб'єктом фінансової розвідки. Приписи FATF мають виняткове значення для роботи цього центрального органу виконавчої влади, що реалізує державну політику з питань запобігання і протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення [273]. Дотримуючись державницьких орієнтирів установа провадить визначені публічні заходи й відносно протидії загрозам від операцій із формами цифрових активів.

Здійснюючи власну діяльність на всіх рівнях, зазначена державна установа реалізує однойменну політику за базовим напрямом, що передбачає проведення низки комплексних заходів. Одним із ключових завдань Держфінмоніторингу є проведення аналізу (операційного і стратегічного) інформації про фінансові операції, що, відповідно до законодавства України, підлягають фінансовому моніторингу. Відносно самого практичного здійснення процедури фінансового моніторингу операцій із віртуальними активами на суму, що дорівнює чи перевищує 30 тис грн, то їх реалізують суб'єкти фінансового моніторингу первинного рівня [244]. Проте окрему групу заходів реагування щодо таких операцій реалізує виключно Держфінмоніторинг. У цьому випадку йдеться про можливість визначення джерел походження віртуальних активів із так званих «ризикових операцій» шляхом доступу до відповідних аналітичних продуктів. Самі відомості про ризиковість трансакцій надходять від суб'єктів первинного фінансового моніторингу. У подальшому аналізований центральний орган виконавчої влади за результатами перевірок хоч і фізично не скасує такі перекази, але має змогу заблокувати відповідний гаманець [274]. Зазначені способи й засоби реагування дають підставу вести

мову про Держфінмоніторинг як орган, який уповноважений державою для здійснення контролю за вказаним напрямом.

Окрім того, аналізований суб'єкт визначає рамкові критерії ризиковості всіх фінансових операції. Попри те, що всі представники первинного фінансового моніторингу формують власну критеріальну шкалу, обов'язковою є її кореляція зі стандартами Держфінмоніторингу [244]. Ураховуючи вищевикладене, можемо стверджувати про визначальну роль у системі економічної безпеки України при проведенні операцій з цифровими активами Державної служби фінансового моніторингу України, яка у своїй практичній діяльності керується відповідними рішеннями FATF та перебуває з нею в тісній співпраці. Доказом цього є відповідний наказ «Про Критерії ризиків легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення» від 28 грудня 2022 року, затверджений Міністерством фінансів України, відповідно до якого провідна методологічна роль з напрацювання відповідного базису відводиться якраз Держфінмоніторингу [256].

4. Національна комісія з цінних паперів та фондового ринку. НКЦПФР є державним колегіальним органом, який підпорядковується безпосередньо Президенту України та виконує наглядові та регуляторні функції у зазначеній сфері. Відносно форм цифрових засобів (віртуальні активи) саме НКЦПФР відіграє системотворну роль. Згідно п. 1 ч. 2 ст. 16 Закону України «Про віртуальні активи» зазначена установа монополюсно відповідальна за формування й забезпечення реалізації державної політики відносно наступних базових позицій: 1) розвиток і функціонування ринку віртуальних активів; 2) сприяння адаптації відповідного законодавства до міжнародних стандартів [70]. Певним чином це стосується й безпекових питань, адже такий компонент є обов'язковим до уваги в межах загальної регламентації. Оскільки в зазначеному вище законодавчому акті серед заходів державного регулювання цієї сфери передбачено й запобігання та протидію зловживанням і порушенням на відповідних ринках. Ураховуючи вище викладене, можемо зробити

висновок, що утворення відповідних засад, у тому числі, здійснюється з акцентом на безпечне середовище для всіх учасників. Це, закономірно, передбачає виявлення й аналіз загроз від таких форм цифрових активів із подальшою мінімізацією проявів останніх.

Слід зазначити, що питання формування й забезпечення реалізації такої політики стосується всіх цих типів засобів обороту. Натомість, у контексті державного регулювання, виняток становлять забезпечені віртуальні активи валютними цінностями (далі – ЗВА (ВЦ)), котрі є предметом впливу у виконанні іншої установи. Тобто, регулювання у виконанні НКЦПФР має стосунок не до всіх існуючих віртуальних активів, що перебувають в обігу на території України.

Пропонована широка юрисдикція цієї державної установи, у тому числі і стосовно окремих форм цифрових активів, дає нам підстави окреслити основні напрями роботи НКЦПФР саме з позиції безпекової складової, а саме:

- 1) формування та забезпечення реалізації державної політики з протидії загроз, що можуть виникати внаслідок операцій із віртуальними активами;
- 2) координація та взаємодія з іншими державними органами у цій сфері;
- 3) упорядкування, контроль і нагляд за ринком віртуальних активів;
- 4) узагальнення практики застосування профільного законодавства та розроблення пропозицій щодо його вдосконалення;
- 5) захист прав учасників ринку віртуальних активів;
- 6) забезпечення та здійснення у межах власних повноважень контролю за виконанням законодавства з питань запобігання й протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення учасниками однойменних ринків.

Виходячи з цього, можемо стверджувати про істотний безпековий вплив НКЦПФР на ринок віртуальних активів як однієї з форм цифрових активів.

5. Національний банк України. Є головним банком України та ще однією провідною інституцією з питання регулювання ринків віртуальних активів. У контексті нашого наукового дослідження НБУ як суб'єкт системи

економічної безпеки, зважаючи на його природу, є відповідальним лише щодо впливу стосовно ЗВА (ВЦ), які перебувають за межами регуляторної уваги з боку НКЦПФР. У той же час, НБУ не уповноважений на формування та забезпечення реалізації державної політики в цій сфері. Саме у цьому й криється головна управлінська відмінність між вказаними інституціями.

Відносно напрямів санкціонованого впливу, то більшість із них є закономірним віддзеркаленням властивостей ЗВА (ВЦ) і специфіки роботи НБУ як кредитно-фінансової установи. У контексті безпекових аспектів пропонуємо наступну диференціацію векторів діяльності НБУ: 1) державне регулювання обороту ЗВА (ВЦ); 2) нагляд за діяльністю постачальників послуг, пов'язаних із обігом такої групи віртуальних активів; 3) проведення планових та позапланових інспекційних перевірок постачальників послуг, пов'язаних із оборотом ЗВА (ВЦ); 4) встановлення вимог щодо забезпечення інформаційної безпеки та кібербезпеки постачальників послуг, пов'язаних із обігом цієї групи віртуальних активів; 5) застосування заходів впливу до таких постачальників послуг. Ураховуючи вищевикладене, можемо стверджувати, що функціонування розглянутої інституції має вагоме значення з позиції безпековості обороту окремих віртуальних активів.

6. Правоохоронні органи (Бюро економічної безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України, Національна поліція, Служба безпеки України). З огляду на характер загроз, що можуть виникати внаслідок операцій із цифровими активами, особливе місце в нашому дослідженні слід відвести правоохоронним органам як суб'єктам системи економічної безпеки України при здійсненні операцій із цифровими активами. Попереднє розуміння типологізації загроз вказаного походження, представлене у підрозділах 1.3, 1.4 й інших та деякі напрями впливу висвітлених інституцій, засвідчують виправданість цього підходу.

У зазначеному контексті перш за все уваги заслуговує тематика легалізації майна й інших засобів отриманих неправомірним шляхом. Якщо вдаватися до конкретизації, то слід зазначити, що в Кримінальному кодексі

України містяться ст. 209. «Легалізація (відмивання) майна, одержаного злочинним шляхом» та ст. 209¹. «Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», які охороняють відповідні відносин і гарантують настання негативних наслідків [245]. Як було уже наголошено, окремі форми цифрових активів можуть виступати в якості засобів для досягнення протиправних цілей, що підпадають під кваліфікацію наведених статей КК України. Зважаючи на тісний зв'язок таких діянь із економікою, можемо стверджувати, що їхня реалізація несе дійсні істотні загрози різним її галузям. Відповідно й цифрові засоби в такому контексті вартують уваги якраз із боку названих органів.

Ініційована чисельність правоохоронних інституцій обумовлена специфікою підслідності, об'єктивованої у нормах чинного законодавства. Зокрема, ч. 9 ст. 216 Кримінального процесуального кодексу України визначено, що досудове розслідування за такими складами кримінальних правопорушень здійснюється слідчим того органу, який розпочав досудове розслідування або ж до підслідності якого відноситься кримінальне правопорушення, що передувало легалізації (відмиванню) майна, одержаного злочинним шляхом [246]. Закріплюється безальтернативна присутність у цій умовній групі НАБУ [246]. Законодавець чітко визначає безумовність здійснення досудового розслідування службовими особами останнього, якщо такі діяння є підслідними саме вказаній установі.

Стосовно суб'єктів правоохоронної діяльності, то в рамках нашого наукового дослідження заслуговують уваги висновки А. Стеблянка про роль так званих «предикатних злочинів» [247, с. 55-56, 57], тобто тих, що передують неправомірній легалізації. Більшість із них (ст. 190 КК України «Шахрайство», ст. 201² КК України «Незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги», ст. 206 КК України «Протидія законній господарській діяльності», ст. 222

КК України «Шахрайство з фінансовими ресурсами», ст. 364 КК України «Зловживання владою або службовим становищем» та ін.) підслідні БЕБ, ДБР, НП та СБУ. З огляду на це, слушно й виправдано досліджувати діяльність декількох суб'єктів правоохоронної діяльності, підсумки роботи яких мають значення для аналізованої сфери відносин.

Варто також зазначити, що склади кримінальних правопорушень за ст. 190. «Шахрайство», ст. 222. «Шахрайство з фінансовими ресурсами» та інші за певних умов також самостійно можуть нести відповідні загрози. Безумовно, і в цьому контексті підкреслюється, важлива роль не одного з перерахованих суб'єктів правопорядку (БЕБ і НП).

Окрім того, в осяжному майбутньому можна розраховувати на вирішення питання оподаткування операцій із віртуальними активами. У такому разі частка складів правопорушень, присвячених податковим відносинам, становитимуть інтерес у рамках окресленої тематики. За цих умов істотно зросте роль БЕБ, зважаючи на поточну підслідність останнього та власне специфіку самих активів.

Ще одним вагомим аспектом можна розцінювати проблематику кіберзагроз, які, попри національну стратегічну риторику, усе ж становлять загрозу багатьом економічним процесам [275, с. 58-59, 60-61]. Зазначене також корелюється з важливими міжнародними позиціями Стратегії кібербезпеки ЄС на цифрове десятиліття [183], доводячи слушність й обґрунтованість наведеної тези.

Під цим кутом зору уваги заслуговує НП, у якому сьогодні діє Департамент Кіберполіції як уповноважена державна інституція. Водночас, репрезентована грань проблематики має складне походження, що потребує змістовної розробки на сучасному етапі.

Загалом же представлену класифікацію провідних суб'єктів можна розглядати як таку, що варта уваги в контексті основного наміру подальшої комплексної розбудови цифрового середовища. Безумовно, наявна модель є недосконалою й обмеженою за багатьма векторами впливу. У той же час вона

формує сприятливий базис для розробки безпекової траєкторії з позиції інституційного забезпечення.

2.3. Адміністративно-правовий механізм взаємодії суб'єктів зі спеціальною компетенцією з протидії загрозам економічної безпеки України, що виникають під час здійснення операцій із цифровими активами

Епізодичність національного адміністративно-правового регулювання предметної сфери відносин із-поміж іншого знаходить місце для деяких аспектів взаємодії зазначених вище суб'єктів системи економічної безпеки України. Безумовно, у цьому аспекті необхідно звернути увагу на дослідження компліментарності таких інструментів або їх присутності у межах заходів управлінського, правоохоронного й іншого характерів. На нашу думку, оминати увагою окреслений вектор санкціонованої регламентації є хибним кроком, зважаючи на об'єктивну потребу всебічного і повного висвітлення проблематики загалом.

Традиційно, перш за все, спробуємо дослідити понятійний апарат. Обраний нами підхід корелюється з висновками Ю. Баранової, І. Царьової, А. Черней, котрі наголошують на обов'язковому попередньому визначенні термінології, з'ясування місця останньої в науці, встановлення її ролі у суспільному житті тощо [276, с. 10-11; 277, с. 163-164], [278, с. 50-51], [279, с. 12]. Ми підтримуємо таку позицію науковців, адже чітке розуміння змістовного наповнення дефініції надає ряд істотних переваг, важливих для ефективної розробки. Серед їх числа доцільно виділити наступні фундаментальні аспекти: 1) висвітлення тієї чи іншої проблематики у відповідності з системою координат, заданих теоретико-методологічними орієнтирами аналізованої категорії; 2) уникнення лєвової частки неоднозначностей і нечіткостей у рамках характеристик предметних процесів

та явищ; 3) відмежування термінологічної одиниці від інших, у тому числі її подібних категорій; 4) розвиток конкретних учень і поглядів щодо самої проблематики. Наведені позитивні сторони дають вагомі підстави вести мову про життєздатність, доцільність і виправданість апробованого нами підходу.

Власне щодо самого поняття «взаємодія», то в тлумачних словниках пропонують наступні варіанти визначення: 1) взаємний зв'язок між предметами (ким-, чим-небудь) у дії [105, с. 346]; 2) погоджена дія між ким-, чим-небудь [107, с. 125; 108, с. 125], [106, с. 287]; 3) об'єктивна універсальна форма руху і розвитку, що визначає існування й структурну побудову будь-якої системи [280, с. 216]; 4) взаємний вплив певних об'єктів, що зумовлює зміну стану їхнього руху [107, с. 125]. Деякі з цих трактувань зустрічаються і в іноземних словниках [109], [281], орієнтованих на термінології із різних галузей знань.

У науковій площині з позиції державного управління такої дефініції увага присвячувалась в публікаціях за авторством К. Ібрагімова [282, с. 289-293], В. Кікінчук [283, с. 82], С. Кожушко [284, с. 247-252], О. Колянко [285, с. 119], Ю. Косенко [286, с. 170], В. Круглий [287, с. 134], М. Лемещук [288, с. 134], М. Папучі і М. Наконечної [289, с. 309], А. Патик [290, с. 26; 291, с. 9-10, 78, 192], М. Подберезького [292, с. 31], Л. Сугакової та Е. Копилова [293, с. 279], а також багатьох інших. Попри численність досліджень із цієї проблематики, ми прийшли до висновку, що хибно вести мову про плюралізм поглядів щодо змістовного наповнення аналізованого терміну. Можемо зробити висновок, що різняться лише характеристики такої діяльності за участю суб'єктів публічно-правових відносин.

Однак, на нашу думку, у вітчизняній науці можна виділити три основні підходи, які заслуговують особливої уваги. Перший визначає взаємодію як процес безпосереднього або ж опосередкованого впливу двох і більше суб'єктів одне на одного [285, с. 170], [286, с. 134]. Другий, більш догматичний погляд, передбачає спільну узгоджену роботу відповідних суб'єктів для досягнення поставлених цілей [283, с. 247-252], [284, с. 119]. І третій підхід до дефініції

«взаємодія» зводиться до центристської ідеї відносно специфічної форми соціальних зв'язків, у яких перебувають ті чи інші суб'єкти [282, с. 289-293], [290, с. 31]. Окрім того, у літературі мають місце і так звані комбіновані підходи, включаючи декілька перерахованих вище характеристик [289, с.10, 78], [291, с. 279], [283, с. 82], [287, с. 134]. Не будемо заперечувати існування й інших альтернативних світоглядів, зважаючи на активний інтерес до цієї тематики та її охоплення широкого діапазону сфер управлінських і самоврядних відносин.

Необхідно додатково наголосити, що перераховані наукові підходи корелюються з поглядами багатьох учених-адміністративістів, котрі свого часу вивчали цю категорію у рамках власних фундаментальних досліджень, серед них слід зосередити увагу на здобутки Ю. Гаруста [6, с. 267-268; 7, с. 391], В. Мельника [52, с. 345, 394; 51], А. Стеблянка [294, с. 91; 247, с. 42, 92, 211], В. Фесюніна [295, с. 35-36] й ін. Відповідно, подальші наші висновки, які ми плануємо підготувати у формі пропозицій і рекомендацій, не йтимуть у розріз фундаментальній парадигмі розуміння суті відповідних явищ та процесів.

Ураховуючи викладений теоретико-методологічний базис нашого дослідження, пропонуємо поняття **«взаємодії суб'єктів зі спеціальною компетенцією з протидії загрозам економічної безпеки України, що виникають при проведенні операцій із цифровими активами»** розглядати як: 1) разове, тривале чи системне вжиття спільних заходів відповідними суб'єктами системи економічної безпеки України з метою протидії загрозам, що можуть виникати внаслідок операцій із цифровими активами, шляхом реалізації управлінських форм і методів та у способи, що не суперечать нормам чинного законодавства; 2) санкціонований вплив одного суб'єкта на інший (чи декілька) з для приведення у відповідність нормам законів і підзаконних нормативно-правових актів заходів, у тому числі недопущення зловживань із питань протидії аналізованим чинникам, явищам, а також тенденціям. Такий підхід семантично охоплює весь суб'єктний склад, форми, методи («... групи

санкціонованих способів та прийомів юридичного (державновладного) впливу ...» [296, с. 476-477]), способи і засоби регулювання, при комбінованому й упорядкованому наборі елементів, з яких можуть провадитися сумісні заходи [297, с. 39] в регульованій сфері. Переконані, зазначена варіація тлумачень дефініції сформує змістовне уявлення про останню, сприяючи розвитку відповідного напрямку у декларованих нами намірах.

Безумовно, у цьому контексті слід зазначити про життєздатність таких трактувань та їх взаємодоповнюваність, ураховуючи багатогранність вітчизняної державної політики в економічній сфері. Вочевидь, у обох випадках виникатимуть специфічні форми соціальних зв'язків, приводячи у дію певні спільні механізми, тобто, лобійовані вище аспекти матимуть місце на різних стадіях консолідації зусиль відповідних учасників. Окрім того, провадження вказаних заходів матиме місце винятково у сфері публічно-правових відносин. При цьому кожен із таких учасників декларативно орієнтований на реалізацію відповідного управлінського інструментарію у способи та за допомогою засобів, націлених раціонально використовувати своє матеріально-технічне забезпечення й інші спроможності, а також виконувати всі завдання в передбачені строки чи терміни.

Варто зауважити, що активна спільна дія тих чи інших суб'єктів та її врегульованість нормами адміністративного права дає підстави вести мову і про функціонування спеціального механізму, фактично приводячи в упорядкований рух елементи відповідної системи. Ураховуючи ту обставину, що взаємодія природно виключає статику, а всі заходи регламентовані згаданими нормами, об'єктивовані актами чинного законодавства, вказані характеристики релевантні класичним уявленням про адміністративно-правовий механізм [220, с. 68, 94], [224, с. 25]. Наприклад, колектив авторів у складі К. Костовської, Ю. Назара та В. Середи, окрім самого поняття, також наводить бачення елементів такого механізму. Вони переконують, що відповідна градація має містити наступні позиції: 1) норми адміністративного права, об'єктивно виражені у законах та інших нормативних актах;

2) адміністративно-правові відносини; 3) акти застосування норм адміністративного права; 4) акти тлумачення норм адміністративного права; 5) правова культура; 6) законність; 7) правосвідомість [224, с. 25]. Під таким кутом зору можна розглядати й вивчати питання взаємодії суб'єктів зі спеціальною компетенцією з протидії загрозам економічної безпеки України, що виникають при проведенні операцій із цифровими активами. Базовий термін «механізм» зазвичай розглядається у таких, смислово близьких до тематики роботи, формаціях: 1) те, що передає або перетворює рух; 2) внутрішня будова чого-небудь; 3) послідовність дій окремих елементів; 4) метод, спосіб [105, с. 695], [107, с. 665; 108]. Із огляду на це, у контексті запропонованої взаємодії слушно вбачати відповідний механізм здійснення різних форм однойменних заходів.

Слушним буде уточнення і про можливість взаємодії не лише між автономними установами, а й структурними підрозділами останніх. На такому різновиді конгломерації загострюють увагу О. Панова і М. Щербина [298, с. 186-187, 188-189], А. Полянський [299, с. 99-100, 178] та інші. Безумовно, указане є прийнятним для нашої тематики дослідження, зважаючи на організаційно-штатні структури аналізованих вище суб'єктів.

Проте, беручи до уваги формалізоване розуміння завдання дисертаційної роботи, сфокусуємо увагу саме на відомчій взаємодії. Ураховуючи ступінь розробленості тематики наукового інтересу, ініційована тактика є правильною у нинішніх умовах.

Як і всі поняття, аналізована категорія має власні особливості, що надає змогу умовно відмежувати її від інших, у тому числі подібних за смисловим навантаженням. Опрацьовуючи значний масив сучасної літератури, присвяченої колу питань щодо методології наукових досліджень, а також робіт, предметно орієнтованих на різні аспекти взаємодії із питань захисту національної економіки, вбачаємо за доцільне сконцентруватись стосовно ознак, мети і завдань цієї діяльності.

Відносно ознак, то враховуючи бачення В. Сущенка, А. Смирнова,

О. Коваленка і А. Смирнова [300, с. 298-299], С. Тюріна [301, с. 103] й інших запропонуємо наступну градацію **ознак** досліджуваної категорії, а саме: 1) важливе значення міжнародних стандартів у цій сфері; 2) сукупність груп регульованих процедур спільного характеру; 3) участь двох і більше суб'єктів; 4) разовість, тривалість або системність ужиття таких мір; 5) спрямованість на розбудову безпечного цифрового середовища з урахуванням технічних і технологічних новацій та орієнтиром на відомі виклики й ризики осяжного майбутнього; 6) провадження спільних заходів, які не суперечать приписам чинного законодавства; 7) існування форм і методів реалізації таких кроків; 8) наявність визначеними нормами адміністративного права спектру засобів та способів здійснення колективних мір [302]. Такий перелік ознак зазначеної дефініції найбільш вдало, на нашу думку, розкриває зміст предметної категорії й влучно відображає нинішню обстановку з питань розбудови вітчизняного цифрового середовища і формування бажаних безпекових механізмів.

Стосовно визначення мети і завдань, то маємо їх позиціонувати як базові орієнтири й шляхи досягнення результату завдяки ефективному використанню спільного функціоналу відповідних суб'єктів. За таким підходом доцільно розглядати один чи декілька, у залежності від обраного вектора діяльності, кількісних або якісних показників, яких необхідно досягти в перспективі. На наше переконання, **метою** такої взаємодії слід вважати своєчасне і повноцінне досягнення задекларованих державою намірів у предметній сфері шляхом оптимальної консолідації наявного інтелектуального, матеріально-технічного й іншого ресурсного забезпечення та раціонального застосування форм і методів діяльності останніх. Відносно **завдань**, то маємо розуміти спектри самостійних персоналізованих, нормативно допустимих настанов, виконання котрих є прерогативою певного кола учасників відповідних спільних заходів. Таке бачення лишень змістовно й аргументовано розкриє сутність указаної категорії наукового пізнання. Більше того, обраний підхід продемонструє цінність колективних мір [303, с. 68-69] за аналізованими вище напрямками.

Із правозастосовної точки зору сфокусуємо увагу на спільних заходах у

виконанні представлених суб'єктів системи економічної безпеки України. Зважаючи на місце в ієрархії управлінських інституцій та беручи до уваги напрями функціонального впливу, питання взаємодії є особливо важливим для **Мінцифри**. Це обумовлено і тим, що саме вказана установа реалізує заходи відносно створення та забезпечення функціонування системи електронної взаємодії органів виконавчої влади (абз. 3 пп. 3 п. 4 [270]), котрі акумулюють у собі й розкриті вище напрями роботи.

У рамках питань щодо формування та реалізації державної політики в сферах цифровізації, цифрових інновацій і технологій, цифрової економіки й цифрового розвитку, організації та координації діяльності органів виконавчої влади, що пов'язана з інтеграцією України до Єдиного цифрового ринку ЄС (EU Digital Single Market) проводяться кілька форм спільної діяльності з позиції регулюючого впливу на інші центральні органи виконавчої влади. Ураховуючи відсутність прямої нормативної вказівки, можна вести мову про побічний вплив на контури заходів у виконанні Держфінмоніторингу і НКЦПФР. Так, пп. 18¹ п. 4 Положення про Міністерство цифрової трансформації України від 18 вересня 2019 р. установа здійснює державне регулювання і нагляд із питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, а також фінансуванню розповсюдження зброї масового знищення [270]. Попри те, що вказані кроки реалізуються лише відносно постачальників послуг, пов'язаних з обігом віртуальних активів [270], їх підсумки матимуть значення для роботи Держфінмоніторингу, котрий, як відомо, узагальнює практику застосування законодавства з питань, що належать до його компетенції (пп. 1 п. 4 [273]). Така постановка питання робить недоцільним потенційне судження про відсутність впливу одного суб'єкта на інший.

Водночас має місце й взаємодія, що представлена і в другому авторському трактуванні її сутності. Порядком обміну інформацією між Державною службою фінансового моніторингу України і Міністерством цифрової трансформації України для підвищення ефективності здійснення

нагляду за дотриманням суб'єктами первинного фінансового моніторингу вимог законодавства з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення від 1 вересня 2020 р. визначено механізм обміну відомостями між останніми щодо зазначеного кола питань [304]. Ураховуючи це, можемо стверджувати про системне вжиття спільних заходів для досягнення поставлених цілей та виконання завдань, визначених державою. Також перспективною є подальша розбудова цифрового фінансового середовища, в чому мають допомогти названі інституції.

У питаннях взаємодії особливе місце відведено **FATF**, що пояснюється становищем і профілізацією останньої. У цьому аспекті доцільно зосередити увагу на проведенні спільних заходів із Держфінмоніторингом, котрий фактично є ретранслятором багатьох об'єктивованих ініціатив суб'єкта міжнародного права.

Так, абз. 4 пп. 6 п. 4 Положення Про Державну службу фінансового моніторингу України від 29 липня 2015 року прямо встановлено, що цей орган забезпечує співробітництво з FATF [273]. Відомим є той факт, що Україна активно співпрацює із вказаною організацією протягом тривалого часу. Ми наводили приклад радикального й авторитетного впливу їхніх актів, коли навіть було легалізовано поняття «віртуальні активи» замість «криптовалюти», «криптоактиви» тощо. Безперечно, стандарти, розроблені FATF, перебувають у полі зору Держфінмоніторингу під час правотворчості останнього.

На додаток до цього, згадані стандарти є у фокусі НКЦПФР. Так, ч. 3 ст. 24 Закону України «Про віртуальні активи» визначено, що установа враховує міжнародний досвід розвитку ринку віртуальних активів, рекомендації міжнародних чи міжурядових організацій. Також вона забезпечує імплементацію відповідних міжнародних стандартів і приписів FATF [70]. Відповідно, слушно вести мову про взаємодію таких інституцій відносно удосконалення національного правового регулювання обороту деяких форм цифрових активів.

Слід зосередити увагу, що **Держфінмоніторинг**, відповідно до ч. 1 ст. 19 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» передбачено обов'язок суб'єктів державного фінансового моніторингу (зокрема й НБУ, НКЦПФР, Мінцифри) і правоохоронних органів (у тому числі БЕБ, ДБР, НАБУ, НП, СБУ) формувати комплексну адміністративну звітність у однойменній сфері [244]. У подальшому вона подається до Держфінмоніторингу з дотриманням Порядку формування та оприлюднення комплексної адміністративної звітності у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення від 5 серпня 2020 року [305]. Окрім FATF таке зобов'язання покладається на решту представлених нами провідних суб'єктів із питань протидії певним загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами.

Слід також зауважити, що суб'єкти державного фінансового моніторингу, такі як НБУ, НКЦПФР, Мінцифри, Держфінмоніторинг, будучи наділеними відповідними статусами, мають особливе становище у поточній структурі інституцій зазначеного спрямування [244]. Об'єктивно, указаний статус передбачає консолідацію зусиль останніх для досягнення спільної мети. Це стосується ініціювання та (або) проведення спільних перевірок більшості груп суб'єктів первинного фінансового моніторингу (за винятком тих, які перебувають у відповідному підпорядкуванні НБУ) щодо дотримання всіх норм застосовуваного законодавства останніми [273]тощо.

Досліджуючи діяльність **НКЦПФР** і **НБУ** в окресленій сфері, слід зазначити, що, окрім розглянутих вище можливостей і зобов'язань спільної діяльності, вказані міри провадяться й безпосередньо між ними. Стійка синергія таких установ обумовлена специфічною юрисдикцією останніх. Підсумовуючи, можемо стверджувати, що вітчизняне законодавчо передбачає, що між ними

має бути налагоджений механізм обміну відомостями з наступних питань (див табл 2.1):

Таблиця 2.1 Основні напрями взаємодії між НКЦПФР і НБУ із питань забезпечення функціонування ринку віртуальних активів

НКЦПФР – НБУ	НБУ – НКЦПФР
<ul style="list-style-type: none"> – банки і небанківські фінансові установи, котрі отримали дозвіл на надання послуг, пов'язаних з оборотом віртуальних активів; – постачальників послуг, пов'язаних із обігом ЗВА (ВЦ), які є банками або небанківськими фінансовими установами, щодо закінчення строку дії дозволу на надання послуг, пов'язаних із оборотом віртуальних активів, його переоформлення або анулювання 	<ul style="list-style-type: none"> – небанківських фінансових установ, які мають намір надавати послуги, пов'язані з оборотом ЗВА (ВЦ) і отримали ліцензію від НБУ; – постачальників послуг, пов'язаних із обігом ЗВА (ВЦ), які є небанківськими фінансовими установами, про прийняте рішення НБУ про відкликання (анулювання) ліцензії на провадження діяльності з надання фінансових послуг, на здійснення валютних операцій; – постачальників послуг, пов'язаних із оборотом ЗВА (ВЦ), які є банками, про прийняте рішення НБУ про віднесення банку до категорії неплатоспроможного або про відкликання банківської ліцензії та ліквідацію банку

Сформовано автором на основі [70]

Разом із тим НКЦПФР здійснює загальну взаємодію й координацію з питань функціонування вітчизняних ринків віртуальних активів та сприяння розвитку останніх [70]. Враховуючи вищезазначене, можна зробити висновок, що такі заходи поширюються і на НБУ. Наведена закономірність пояснюється винятковою роллю державного колегіального органу, а саме формування і забезпечення реалізації політики щодо всього кола суб'єктів та учасників таких відносин [70]. Отже, саме НКЦПФР, із дотриманням всіх законодавчих орієнтирів, визначає характер колективних мір, обов'язкових до виконання іншими суб'єктами з питань забезпечення стійкого функціонування згаданих

ринків. Решта представників цієї сфери, у тому числі НБУ, за окресленими напрямками є лише у межах систем координат, заданих провідною установою.

Вивчаючи роботу в сфері обігу цифрових активів, перерахованих вище **суб'єктів правоохоронної діяльності**, слід визначити, що проведення спільних заходів властиве й цим інституціям. Профільними законодавчими актами врегульована взаємодія цих установ щодо різного кола підвідомчих, а також підслідних питань (ст. 7 [147], Розділ IV [306], ст. ст. 19¹, 19² [307], ст. 5 [308], ст. 17 [309]). Проведення спільних заходів визначено і нормами кримінального процесуального законодавства, а також законів України «Про організаційно-правові основи боротьби з організованою злочинністю» [248] і «Про оперативно-розшукову діяльність» [249]. Як бачимо, на законодавчому рівні сформовані умови і деталізовані механізми такої взаємодії [310] та ін.

Прямі вказівки щодо діяльності в досліджуваній сфері можна віднайти в Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». Основними з них є: 1) отримання доступу до документів або інформації, що міститься в розпорядженні суб'єктів первинного фінансового моніторингу. Отримання відомостей від банків, що становлять банківську таємницю у порядку й обсязі, передбаченому Законом України «Про банки і банківську діяльність» [311] (п. 19 ч. 2 ст. 8 [147]); 2) отримання від суб'єктів державного фінансового моніторингу (НБУ, НКЦПФР, Мінцифри, Держфінмоніторинг) відомостей, що можуть свідчити про ознаки вчинення правопорушень (пп. 2, 4, 5 п. 5 [273]), (ч. 3 ст. 18 [147]); 3) надання інформації органам іноземних держав (абз. 3 ч. 2 ст. 31 [147]); 4) тощо. Вочевидь, засобами вчинюваних діянь можуть бути й форми цифрових активів, що доводить слушність і виправданість проведення спільних заходів.

Окрім викладеного, доцільно зосередити увагу на взаємодії вітчизняних правоохоронних органів з FATF щодо певних аспектів роботи. Сама колективна діяльність також регламентована відповідним законодавством (ст. 6 [147], п. 15 ч. 1 ст. 6 [306], п. 9 ч. 1 ст. 16 [307], ст. 4 [308], ст. 16 [309]). Відносно

FATF, то можемо виокремити обмін досвідом щодо предметних аспектів, ознайомлення з типологічними дослідженнями тощо [272]. Значиме місце відведено питанням урахування практик міжнародної організації під час здійснення досудового розслідування, оперативно-розшукових заходів і решти форм та методів роботи вітчизняних установ («Керівництво щодо протидії фінансуванню розповсюдження зброї масового знищення» від 2018 року [311], Керівництво FATF [136] та ін.).

Наведені й аргументовані чинним законодавством судження дають підстави вести мову про наявність правових підвалин для спільної діяльності з питань забезпечення розвитку цифрового середовища. Це стосується і тематики колективної протидії виявам відповідної деструкції, які можуть впливати на економічну складову.

Іншими словами, наявне правове підґрунтя вбачається перспективним для подальшої розбудови відповідних систем і механізмів у національних масштабах, орієнтованих на міжнародні та іноземні стандарти. Ураховуючи виняткову значимість спільних зусиль і зважаючи на багатогранність цієї області, питання взаємодії також матиме вагоме, подекуди виняткове значення.

2.4. Правові основи здійснення державного контролю та нагляду при проведенні операцій із цифровими активами

В умовах лише поступової розбудови цифрового середовища та вимушеної статичності механізмів державного регулювання обороту віртуальних активів, у зв'язку з відтермінуванням вступу в дію Закону України «Про віртуальні активи», тематика контролю й нагляду у цій сфері носять обмежений характер. Ураховуючи їх беззаперечну значимість і виняткову практичну роль, окремі його прояви варті уваги в рамках представленої роботи. Саме функціонал контролю та нагляду часто забезпечує підтримку правопорядку в регульованих сферах. Результати відповідних заходів сприяють стійкому

перебігу тих чи інших процесів, у тому числі за рахунок мінімізації порушень прав, обмежень свобод і законних інтересів учасників конкретного кола відносин, що спонукає до розгляду останніх під кутом адміністративно-правового регулювання. Такі підсумки матимуть значення і в контексті однієї з провідних ініціатив щодо окреслення першочергових шляхів відповідного забезпечення з протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами. Лишень наведених аргументів, переконані, достатньо, щоб сфокусувати дослідницький інтерес до окресленої тематики.

Слід зауважити, що з теоретико-методологічної точки зору вказані категорії користуються попитом у багатьох авторів. У контексті відразу обох позицій (зокрема і з ціллю порівняння останніх) мову слід вести про фундаментальні наукові доробки у виконанні таких діячів, як В. Гаращук [312, с. 12; 313, с. 82-83], В. Журавель [314, с. 76], І. Кайло [315; 316, с. 28], С. Ківалов та Л. Біла [317, с. 63], Р. Козьяков [318, с. 362; 208], С. Колісніченко [319, с. 43], В. Кравченко [320], А. Мельниченко [321, с. 229], Л. Сорока [322, с. 173], А. Філіпенко [323, с. 318], Є. Хайнацький [324, с. 69], О. Ярошенко [325, с. 104] та багатьох інших.

У загальних рисах ці понятійні одиниці, на нашу думку, слід вивчати під наступними кутами зору: 1) нагляд: а) стеження, спостерігання; б) пильнування, слідкування за ким-, чим-небудь для контролю, забезпечення порядку тощо [105, с. 49], [107, с. 707]; 2) контроль: а) перевірка, облік діяльності кого-, чого-небудь; б) установа або організація, що здійснює нагляд за ким-, чим-небудь або перевіряє його [105, с. 271], [107, с. 568]. Із позиції лексико-фразеологічного підходу зазначені категорії не є синонімічними і несуть різне смислове навантаження, попри схожість певних контурів окремих елементів. Їх змістовне наповнення дає мотивовані підстави вживати нетотожні одиниці, що призводить до неоднакового академічного вжитку й практичного застосування.

Науковці, посилання на яких зроблено вище, у своїх працях також дотримуються і стійко розвивають траєкторію їхнього розмежування, про що

свідчать відповідні здобутки. Більшість сходиться на думці відносно важливості цих груп управлінських інструментів [314, с. 76], [321, с. 229], [323, с. 318], [325, с. 104]. Деякі розкриті судження нашттовують на думку про їх взаємодоповнюючий ефект [319, с. 43], [320], [321, с. 229], [322, с. 173], [325, с. 104], із чим ми погоджуємося, зважаючи на коло методів і способів державного регулювання. Так, В. Кравченко і Л. Сорока, незалежно один від одної, навіть наводять перелік спільних ознак обох категорій (єдина базова мета, предмет впливу, способи та форми їх адміністративно-правового забезпечення і реалізації тощо) [320], [322, с. 173]. Зазначене додатково належно аргументує слушність їх суміжного позиціонування в якості одного з векторів чинної адміністративно-правової регламентації.

Відносно ж змістовного наповнення останніх, то мову доцільно вести про наступні найпопулярніші бачення: 1) нагляд: спостереження для забезпечення дотримання режиму правопорядку. Такі заходи провадяться без втручання в поточну роботу об'єктів нагляду [312, с. 12; 313, с. 82-83], [315; 316, с. 28]; 2) контроль: здійснення інспекцій, перевірок із метою виявлення і встановлення порушень дотримання законодавства [312, с. 12; 313, с. 82-83], [315; 316, с. 28] та (або) співставлення очікуваних результатів дійсним підсумкам, визначення різниці між ними, з'ясування причин появи неочікуваного становища тощо [325, с. 69]. Відповідні процедурні міри можуть бути реалізовані шляхом втручання в оперативну роботу об'єктів контролю. При цьому Т. Коломоець і Г. Гулевська взагалі вважають, що подекуди може мате місце навіть тимчасового перебрання на себе функцій управління контрольованої одиниці на користь власне суб'єкта контролю [326, с. 58]. Ми висловлюємо згоду з такими висновками, оскільки чинне законодавство передбачає випадки наведеної ротації з певних об'єктивних підстав. І мова йде саме про зміну, обумовлену результатами здійснення інспекцій, перевірок та інших форм контролю [327].

Наведені фундаментальні відмінні характеристики вкотре доводять важливість однойменних груп інструментів, паралельно виправдовуючи

доцільність висвітлення останніх. Їхній функціонал забезпечить ефективний розвиток ініційованого комплексного напрямку, мінімізуючи прояви делінквентної поведінки й решти відхилень від заданих параметрів систем і механізмів.

Як зауважувалось вище, нинішня ситуація у сфері обігу цифрових активів особливо негативно відображається щодо контролю і нагляду навіть відносно деяких легалізованих форм цифрових активів. Разом із тим, непоодинокі прояви у предметній сфері заслуговують уваги крізь призму роботи досліджуваних нами інституцій.

Зокрема, **Мінцифри** здійснює наглядові заходи у сфері запобігання й протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення відносно постачальників послуг, пов'язаних з обігом віртуальних активів, а також здійснює формування та виконання Національної програми інформатизації [270]. Виходячи з окресленого вище бачення концепції нагляду [312, с. 12; 313, с. 82-83], [315; 316, с. 28], [325, с. 69], можемо зазначити про постійне спостереження для забезпечення дотримання режиму правопорядку з питань обороту таких активів суб'єктами, які ліцензовано надають відповідні послуги.

Ураховуючи адміністративно-правовий статус міністерства та беручи до уваги сутнісне розуміння форм і методів наглядових заходів, убачаємо, що деякі його прояви зустрічаються у рамках усіх підвідомчих напрямів. Безумовно, це стосується й тих, які націлені на сферу наукового інтересу і розкриті нами у підрозділі 2.2. Тому в контексті нагляду йдеться про вагому роль аналізованого центрального органу виконавчої влади на сучасному етапі державотворення.

З приводу проведення контрольних заходів, то зазначена установа застосовує відповідні повноваження в таких важливих для нас питаннях: 1) контроль за виконанням власної державної політики всіма підвідомчими установами (пп. 1 п. 5 [270]); 2) відповідність заявників та резидентів Дія Сіті

законодавчим вимогам для набуття і наявності однойменного правового статусу (пп. 9⁵ п. 4 [270]), (ч. 5 ст. 6 [328]); 3) формування та виконання Національної програми інформатизації (пп. 5 п. 5 [270]); 4) виконання власних наказів (пп. 8, п. 5 [270]); 5) інші заходи. Відповідно й питанням різних напрямів і форм та методів у виконанні Мінцифри також відведена своя чільна увага. З-поміж іншого, це також підтверджує тези про взаємодоповнення [319, с. 43], [320], [321, с. 229], [322, с. 173], [325, с. 104] останніх у структурі засобів впливу на поведінку учасників регульованих відносин.

Стосовно **FATF**, то, зважаючи на специфічне, порівняно з рештою суб'єктів, становище, особливо виділятимуться якраз наглядові заходи. У цьому контексті мову слушно вести про наступні вектори: 1) поширення відомостей стосовно заходів боротьби з відмиванням грошей на всіх континентах і в усіх світових регіонах; 2) моніторинг за неухильною реалізацією Сорока рекомендацій в країнах – членах «FATF» (Сорок Рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) від 25 вересня 2003 року) [271]; 3) огляд тенденцій, присвячених питанням відмивання коштів і реалізації відповідних контрзаходів (типологічні дослідження) [272]. Усі перераховані напрями знеціняться без реалізації широкого діапазону і різного характеру наглядових заходів. Не останню роль під таким кутом зору відіграють і самі організації як у міжнародному, так і в національному вимірах.

Попри чітку вказівку щодо застосування згаданих заходів у межах другої позиції, питання поширення відомостей і огляду тенденцій повною мірою може бути реалізоване винятково за підсумками наглядової роботи. За таких умов можливим є отримання чіткої картини, що відповідає дійсним реаліям певного підпитання щодо легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Із урахуванням цих відомостей слушно й виправдано розраховувати на подальше інформування учасників заходів про профілактичні та інші міри ефективного і результативного реагування. Указане є прийнятним і

для виконання типологічних досліджень, котрі потребують актуальної інформації з ціллю чіткого усвідомлення ступеня складності проблеми та подальшої розробки й наукового обґрунтування перспективних шляхів вирішення дискусійного питання.

Відносно **Держфінмоніторингу**, то згідно з власною профілізацією та специфікою компетенції слушно вести мову про істотне превалювання контролюючих заходів. Ураховуючи поточну роль Мінцифри за аналізованим вектором та зважаючи на норми профільних нормативно-правових актів, доцільним убачається виокремлення контролю за виконанням виданих наказів [273]. Безперечно, деякі наглядові й контролюючі заходи щодо предметної області нашого дослідження, з позиції завдань установи, можна прослідкувати в роботі останньої. Проте, знову ж таки, ураховуючи недостатню розробленість цієї проблематики, у тому числі на офіційному рівні, зазначені аспекти перебувають у процесі тривалого становлення.

Зосереджуючи ж увагу на місці та ролі **НКЦПФР** і **НБУ**, попри вимушений паралітичний стан відповідних механізмів, указаний аспект вартує загальної уваги. Вище було підкреслено, що установи провадять широкий діапазон заходів, іменованих «державним регулюванням», яке передбачає й застосування інструментів контролю та нагляду за напрямками предметного впливу [70]. Безумовно, слід ураховувати суворе і виправдане розмежування сфер санкціонованої регламентації між обома суб'єктами. Відповідно, НБУ, крім засадничих аспектів, є націленим винятково на ЗВА (ВЦ), у той час, у контексті НКЦПФР, мову будемо вести про решту типів віртуальних активів.

Законодавчий підхід до структури компетенцій, із-поміж іншого, передбачає здійснення нагляду та контролю за дотриманням учасниками відповідних ринків однойменного законодавства [70]. Такі домінанти релевантні повноваженням установи і, в осяжному майбутньому, будуть реалізовані при наявності відповідних підстав.

Однак на відміну від завдань, повноваження передбачають реалізацію таких заходів лише відносно постачальників послуг, пов'язаних із оборотом

віртуальних активів [70]. У контексті НБУ це лише нагляд щодо вказаної групи суб'єктів (п. 6 ч. 1 ст. 17 [70]), однак інші повноваження засвідчують наявність і окремих типів контролюючих дій.

Виходячи з цього, ми можемо стверджувати про наявність наглядових і контролюючих заходів відносно певних форм цифрових активів. Із точки зору правоохоронного напрямку ці вектори націлені на внутрішньоорганізаційні загальні питання функціонування установ. Тому недоцільним убачається їх висвітлення в межах розкритого питання, котре передбачає інакші сутнісні орієнтири. У той же час усі перераховані суб'єкти мають потенціал для розбудови безпечного цифрового середовища із належним використанням аналізованих груп регулятивних інструментів.

Висновки до розділу 2

1. З огляду на відсутність у правовій площині категорії «цифрові активи» та відмінну правову природу такої одиниці, як «цифрові речі», об'єктивною убачається недостатня розробка комплексних адміністративно-правових засад із протидії загрозам системі економічної безпеки України, які можуть виникати внаслідок операцій із цифровими активами. Їх обмеженість також доводиться окремими теоретико-методологічними суперечностями і власне лише тривалою розбудовою відповідного напрямку.

Реалії сьогодення демонструють, що такі питання врегульовані фрагментарно (залежно від легалізованих форм цифрових активів), а в цілому перебувають у процесі тривалого становлення. Така тенденція релевантна міжнародній правотворчості й практикам більшості іноземних країн, котрі, попри визнання цифрових активів, тільки починають усвідомлювати зворотні сторони відповідних процесів. У національних масштабах зазначеному аспекту присвячена увага з позицій державно-правового регулювання поведінки учасників ринків віртуальних активів, запобігання й протидії легалізації

(відмиванню) доходів, одержаних неправомірним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, реагування на кіберзагрози, а також недопущення зловживань суб'єктів, на яких поширює свою дію спеціальний правовий режим Дія Сіті.

Указані засади представлені нормами адміністративного права і об'єктовані в нормативно-правових актах різної юридичної сили, що також предметно спрямовані на багато сфер санкціонованої охорони. Формалізовано і персоніфіковано йдеться про наступний спектр документів: 1) Конституція України; 2) міжнародні договори України; 3) закони; 4) підзаконні нормативно-правові акти.

2. Деякі форми цифрових активів становлять предмет фахової уваги з боку нечисельних уповноважених інституцій. Особливості адміністративно-правового забезпечення однойменної сфери, закономірно, зумовлюють лише фрагментарну участь державних та інших органів у відповідних процесах. У цей же час світові тенденції розвитку цього напрямку свідчать про необхідність масштабування, зростання варіативності форм і методів, а також нарощування кількості об'єктів регуляторного впливу.

Нинішня когорта представлена незначною кількістю суб'єктів адміністративно-правового статусу, котрі лише частково (в силу функціональної обмеженості) забезпечують змогу реалізації відповідних мір. Залежно від характеру компетенції й місце в ієрархії публічних інституцій, мова йде про один із головних органів у системі центральних органів виконавчої влади, представника міжнародного права, самих центральних органів влади, у тому числі суб'єктів правоохоронної діяльності, а також центральний банк України.

Функціонування таких інституцій переважно здійснюється на міжнародному та загальнодержавному рівнях. Водночас, окремі з їхнього числа особливо вирізняються в міжнародному вимірі (FATF), а решта – на національному загальнодержавному рівні (Мінцифри, Держфінмоніторинг, НКЦПФР, НБУ, правоохоронні органи). Наявна специфіка доведена

персональним становищем кожної інституції, а також особливостями національної управлінської парадигми.

До основних напрямів, реалізованих цими суб'єктами, слід віднести такі позиції, як формування та реалізація державної політики з питань цифровізації, цифрових інновацій і технологій, цифрової економіки й цифрового розвитку; запобігання і протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, розвитку і функціонування ринку віртуальних активів, зокрема й приведення останніх у відповідність міжнародним стандартам; поширення відомостей стосовно заходів боротьби з відмиванням грошей на всіх континентах і в усіх світових регіонах, моніторинг за неухильною реалізацією рекомендацій із розробки фінансових заходів боротьби з відмиванням грошей, виконання типологічних досліджень; здійснення заходів під егідою державного фінансового моніторингу; правоохоронна діяльність за відповідними складами правопорушень; тощо. Реалізація відповідних кроків у межах перерахованих та інших напрямів хоч і фрагментарно, але покликана вирішити низку нагальних проблемних питань у цій сфері.

3. Адміністративно-правовий механізм взаємодії основних суб'єктів із питань протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами, є важливим атрибутом адміністративно-правового регулювання. Зважаючи на недостатню розробку цієї проблематики та враховуючи загальновідомі властивості останніх, консолідація наявних зусиль – надзвичайно важлива засада в умовах невідворотного розвитку цифрового середовища.

На сучасному етапі її виправдано розглядати під декількома кутами зору, які охоплюють усі аспекти колективних мійр. По суті – це методи впливу двох і більше суб'єктів для реалізації певних заходів у коротко- середньо- та довгостроковій перспективах. Такі конгломерації покликані посилити організаційні, управлінські, правоохоронні й інші санкціоновані кроки для ефективного і результативного вирішення предметних питань. Відсутність чи

обмеженість відповідного спектра механізмів послабить потенціал адміністративно-правового регулювання досліджуваної сфери.

Усі суб'єкти з протидії аналізованим вище загрозам є активними учасниками колективних заходів, здійснюваних відносно окремих форм цифрових активів. При цьому, це різні аспекти спільної діяльності на всіх рівнях і за багатьма векторами санкціонованого впливу. Зважаючи на компетенцію конкретного суб'єкта, взаємодія може відбуватись із декількох незалежних питань, одного напрямку або єдиної правозастосовної траєкторії зі широким діапазоном процедурних сумісних заходів.

Особливо цей аспект нормативно закріплений із позиції загального регулювання діяльності постачальників послуг, які надають їх з обороту віртуальних активів і запобігання й протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, розвитку і функціонування ринку віртуальних активів. Спільні заходи у рамках діяльності Мінцифри, FATF, Держфінмоніторингу, НКЦПФР, НБУ та правоохоронних органів (БЕБ, ДБР, НАБУ, НП, СБУ) складають невід'ємний функціональний атрибут останніх.

4. Проблематика стійкого ефективного нагляду і контролю із безпекових мотивів у цифровій сфері має надважливе значення. В умовах гострої потреби дієвого застосування всіх груп санкціонованих регулятивних заходів вказані аспекти вирізняються виключною важливістю та сприяють належному виконанню багатьох суміжних завдань і реалізації функцій.

Навіть при поточній вимушеній обмеженості відповідних механізмів їх значимість хибно недооцінювати. Серед численних передумов для такого міркування виділяються властивості цифрових активів, що передбачають необхідність усебічної залученості держави у відповідні процеси. Враховуючи попередньо висвітлені погляди на їхню загрозливність та складність, виникає потреба дієвого реагування на відповідні виклики.

Категорії «нагляд» і «контроль» є не тотожними, але доповнюваними одна одну групи інструментів державного регулювання. Їх застосунок має

мінімізувати прояви делінквентної поведінки й решти відхилень, що ускладнюють чи унеможливають перебіг конструктивних для економіки процесів і розвиток бажаних тенденцій.

Суб'єкти, наділені таким інструментарієм, поки в не достатній мірі впливають на відповідні об'єкти як у силу певних умов, так і факторів. Щодо певних об'єктів компетенція останніх взагалі не передбачає засобів для досягнення безпеково значущих цілей. Це породжує певні ризики варті уваги з точки зору реального та істотного руйнівного впливу представників цифрової сфери на досліджувані відносини.

Водночас, нормативно-правове забезпечення для функціонування останніх формує сприятливе підґрунтя для подальшої системної розбудови цифрового середовища із урахуванням безпекових запитів. При чому йдеться не лише про урахування поточних викликів і загроз, а й багатьох тих, що можуть виникнути у середньо- та довгостроковій перспективах. Безумовно, не виконуваним завданням бачиться визначення всіх майбутніх явищ, чинників і тенденцій національної безпекової деструкції. Тим не менш, деякі орієнтири видаються імовірними з огляду на характер перебігу багатьох процесів у локальних, національних і міждержавних масштабах. Відповідно, посилення контрольних і наглядових заходів, як провідних атрибутів адміністративно-правового регулювання є одним із пріоритетних питань.

РОЗДІЛ 3

ПРІОРИТЕТНІ НАПРЯМИ РОЗБУДОВИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ З ПРОТИДІЇ ЗАГРОЗАМ СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ, ЩО МОЖУТЬ ВИНΙΚАТИ ВНАСЛІДОК ОПЕРАЦІЙ ІЗ ЦИФРОВИМИ АКТИВАМИ

3.1. Огляд і компаративний аналіз міжнародних та провідних закордонних моделей щодо протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами

Проблематика ризиковості й загрозовості нарощування потенціалу цифровізації поступово починає розвиватися на більшості континентів, зважаючи на явні сингали для економічних галузей. В умовах непередбачуваності новітнього функціоналу таких засобів і технічної неможливості оперативно розробляти дієві механізми реагування на ці подразники, питання регулювання цих суспільних відносин набуває виняткової гостроти. Зазначені й інші фактори на тлі геополітичних і геоекономічних потрясінь вимагають уваги до окресленого вектору наукового інтересу.

Слід зазначити, що вагомі кроки з таких питань здійснено в країнах ЄС, котрі давно стали орієнтиром для багатьох інших країн. Водночас, необхідно зауважити, що саме категорія «цифрові активи» не фігурує ні в установчих договорах, ні у висновках, директивах, регламентах, рекомендаціях чи рішеннях. Зі змісту таких документів можна зробити висновок, що національна політика цих країн спрямована на ринки криптоактивів і цифрових валют. Окремо слід виділити результати роботи Міжнародної групи з протидії відмиванню брудних грошей, котра в актуальному звіті Керівництва FATF [136] почала застосовувати термін «віртуальні активи». Як ми зазначали вище, такий підхід позначився на елементах профільного українського законодавства, а саме: норми були імплементовані в Закон України «Про

віртуальні активи».

Однак такі підходи не відповідають усім ключовим запитам обраної тематики дослідження, адже стосуються лише певної частки форм аналізованих засобів і меншою мірою стосується загрозливості останніх. Виходячи з цього, слушно зауважити, що відповідні стандарти ЄС орієнтовані на вузький спектр відносин (відповідні форми цифрових активів), що іде в розріз із ініційованими нами орієнтирами. У контексті саме загроз для економічного сектору України деякі їх приписи варті уваги. Вкотре звертаємо увагу на взірцеву роль відповідної політики FATF для лівової частки інших країн, у тому числі представників не європейського континенту.

У згаданій вище Стратегії кібербезпеки ЄС на цифрове десятиліття (The EU's Cybersecurity Strategy) від 2020 року [183] акцентується увага щодо все більшої залежності різних сфер життєдіяльності (безпека, енергетика, здоров'я, телекомунікації, транспорт, фінанси тощо) від дії цифрових засобів [183, с. 1]. При цьому відмічається, що так званий «ландшафт» загроз ускладнюється геополітичною напругою на глобальному та відкритому рівнях [183, с. 1], підкреслюючи неодноразово зазначену нами стрімку динаміку всебічного розвитку останніх.

У цьому документі наголошується, що кібербезпека має бути комплексно інтегрованою в усі цифрові інвестиції, особливо провідні, такі, як квантові обчислення, шифрування, штучний інтелект і решта [183, с. 5]. Також зафіксовано ключові напрями кіберпростору, що вартують уваги з позиції гарантування забезпеченості останніх у найближче десятиліття, і звернено увагу на інші аспекти різного спрямування.

Окремо слід виділити такі міжнародні документи, як Рекомендації Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року [122] та Керівництво FATF [136]. Відносно першої позиції, то станом на 2019 р. її автори відкидали ідею репрезентування криптоактивів у якості загроз фінансовій стабільності [122, с. 17]. Із приводу керівництва, то з огляду власне на мету і завдання самого FATF, природно, йдеться про використання

віртуальних активів у якості засобів із відмивання коштів, фінансування розповсюдження зброї масового знищення, а також спонсорування тероризму [136, с. 2]. Безумовно, користування вказаною формою цифрових активів у таких цілях становить загрозу для економічних відносин. Залежно від ситуації, мова може йти як про прямий, так і опосередкований руйнівний впливи. Попри те, що документ носить рекомендаційний характер, додатково слід відмітити: описані міри реагування на аналізовані подразники сукупно мають обмежений функціонал. Його слід розглядати як своєрідну «дорожню карту» із нечіткими межами, котра варта уваги з позиції уніфікації практик та гармонійного розвитку спільних заходів із протидії наведеним чинникам.

Зауважимо, що питання загроз указанного походження як надважливих і тих, що обов'язково вартують уваги, міститься в Розділі VI: Фінансове співробітництво та положення щодо боротьби із шахрайством Угоди про асоціацію між Україною та ЄС від 27 червня 2014 року [187] в контексті також відповідних зобов'язань для української сторони. Такі аспекти деталізовані у Директиві Європейського Парламенту і Ради (ЄС) 2015/849 від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, про внесення змін до Регламенту Європейського Парламенту і Ради (ЄС) № 648/2012 та про скасування Директиви Європейського Парламенту і Ради 2005/60/ЄС та Директиви Комісії 2006/70/ЄС від 20 травня 2015 року [188], у якій, із-поміж іншого, окремі типи цифрових інструментів за певних умов розцінюються в якості однойменних загроз (п. «b» ч. 4 ст. 41, ст. ст. 60, 63, 65) [188]. Однак, знову ж таки, помітно превалюють питання загального спрямування, що передбачають зобов'язання країн учасників у різні форми й методи реагувати на відповідні деструктивні прояви.

Наостанку, не можливо оминати увагою концептуальний акт Регламент МіСА [189], котрий покликаний урегулювати низку питань, пов'язаних із оборотом саме криптоактивів. Слушним є уточнення В. Бацуци, яке релевантне нашим висновкам щодо нормативного акценту лише на певну частину типів

досліджуваних активів [93, с. 92]. Аналогічне застереження зустрічається в звіті «Регулювання цифрових активів: Інсайти юрисдикційних підходів», датованого жовтнем 2024 р., в якому зазначається, що необхідно розрізняти криптоактиви, які підпадають під межі регулювання Регламенту MiCA [189], та фінансові інструменти в цифровій формі, котрі розглядаються в статусі цінних паперів [182, с. 9] відповідно до законодавства ЄС. Тобто, легалізоване розуміння змісту однойменного терміну не різниться від більшості висновків наукового й фахового походжень і, відповідно, не є синонімічним поняттю «цифрові активи».

Відносно логіки його появи, то переслідується стійкий намір сформувати єдині засадничі стандарти для всіх учасників європейської спільноти з метою уніфікації правових методів і засобів регламентації відносин у цій сфері. Загальновідомо, що деякі їхні положення ідуть у розріз із вітчизняним Законом України «Про віртуальні активи», на що предметна увага буде звернена в заключному розділі дисертаційної роботи.

Стосовно саме проблематики загроз, то за аналогією з Рекомендаціями Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року [122] автори аналізованого документа стверджують, що ринки криптоактивів усе ще скромні за розміром і наразі не становлять загрози для фінансової стабільності (п. 5 вступної частини) [189]. У той же час, наголошується на імовірності широкого прийняття їх роздрібними власниками, що може породити складнощі із наступних точок зору: 1) безперебійна робота платіжних систем; 2) передача монетарної політики або монетарного суверенітету; 3) фінансова стабільність (п. 5 вступної частини) [189]. Тобто, в осяжній перспективі допускається можливість появи істотних загроз для фінансових процесів і, як наслідок, певних граней економічної складової.

Окрім того, цим актом закріплено норму про обов'язок компетентного органу відмовляти в дозволі на обіг криптоактивів, які можуть становити загрозу перерахованим вище обставинам, також цілісності ринку (п. 45 вступної частини) [189]. Центральні банки мають наділятися змогою вимагати

від компетентного органу відкликати дозвіл емітента таких токенів, пов'язаних з активами, при доказовому розумінні настання цих же загроз (п. 62 вступної частини) [189]. Попри такі базові засади вбачати закріплення цілісних стійких механізмів було б невиправданою ідеєю. Це пояснюється тим, що мова йде щодо можливості настання вказаних загроз і обов'язкового варіанту поведінкової моделі контролюючих чи наглядових суб'єктів. До того ж акцент здійснений на етап становлення вказаних кроків, що передбачає подальшу розробку похідного законодавства на рівні ЄС та імплементацію таких інструментів країнами учасниками.

Отже, можемо зробити висновок, що в країнах європейського співтовариства, окрім декларованих намірів, уже вжито базові заходи щодо комплексного дієвого правового забезпечення обігу найпопулярніших (за різними умовними критеріями) типів цифрових активів. У той же час питанням щодо протидії й запобіганню загроз від операцій із останніми приділена загальна (фрагментарна) увага. Ураховуючи орієнтири існуючих нормативних приписів у відповідних установчих договорах, висновках, директивах, регламентах, рекомендаціях і рішеннях можемо констатувати імовірність настання несприятливих наслідків для економік, однак предметний акцент на способах і засобах реагування не спостерігається. Із такої тенденції помітно виділяються питання забезпечення кібербезпеки й протидії відмиванню коштів, фінансування розповсюдження зброї масового знищення, а також спонсорування тероризму. На наше переконання, йдеться про значно ширший діапазон дискусійних положень, які потребують визнання на офіційному рівні.

Коло питань щодо правового забезпечення протидії таким чинникам, явищам і тенденціям на порядку денному перебувало у фокусі компетентних (контролюючих та правоохоронних) органів іноземних держав. Для цього у країнах ЄС були прийняті (затверджені) відповідні нормативно-правові акти різного рівня, предметно націлених на регулювання суспільних відносин за відповідним напрямом. Зважаючи на малодослідженість власне феномену цифрових активів і суміжних явищ («віртуальні активи», «віртуальні валюти»),

«криптовалюти», «цифрові активи», «цифровий контент», «цифрові речі»), можемо стверджувати, що у більшості розглянутих нормативно-правових актів йдеться про загальне окреслення правових засад зазначених категорій.

Крім того, у ході свого наукового дослідження ми дійшли висновку, що деякі країни пішли іншим шляхом, пріоритетно звернувши увагу лише на категорію криптовалюти. До їх числа слід віднести такі, як Австралійський Союз (Австралія), Королівство Швеція (Швеція), Республіка Казахстан (Казахстан), Республіка Кіпр (Кіпр), Республіка Мальта (Мальта), Республіка Молдова (Молдова), Республіка Сінгапур (Сінгапур), Республіка Філіппіни (Філіппіни), Федеративна Республіка Німеччина (Німеччина), Швейцарська Конфедерація (Швейцарія) та інші. Національне законодавство цих країн, як і українська модель, або в загальних обрисах фокусується на цифровій складовій, або взагалі залишає його поза офіційною увагою.

Серед указаних держав специфічною щодо аналізованого напрямку є ситуація в Китаї. Загальновідомо, що криптовалюти заборонені до обороту у цій країні протягом тривалого строку [190]. Проте новітні відомості наочно показують, що її громадяни продовжують залишатися активними користувачами цих засобів. Так, із липня 2022 р. по червень 2023 р. Гонконг займав п'яте місце за обсягом відповідних трансакцій із показником близько 64 млрд дол США [190]. До того ж, як зазначає Г. Некіт, у цій країні сконцентровано найпотужніші майнінгові ферми і добувається майже 60 % біткоїнів [191, с. 37]. Тобто, при відсутності необхідної правової бази у вказаній державі активно використовуються криптовалютні засоби. Попри суперечливість концепції відповідного завдання дисертаційної роботи, досвід Китаю вартий уваги, ураховуючи його частку на світовому ринку криптовалют.

У якості протиставлення окремі суверенні утворення свідомо і цілеспрямовано розбудовують законодавчі бази з центристським орієнтиром навколо саме цифрових активів. Показовими і вартими схвалення, всілякої підтримки та наслідування є підходи, використовувані в рамках реалізації державних правових політик Багамських Островів, Бермудських Островів,

Канади, Китайської Народної Республіки (Китаю) та США.

1. Багамські Острови. На Багамських Островах діє Закон «Про цифрові активи та зареєстровані біржі» (зі змінами) від 2022 року (Digital Assets and Registered Exchanges (Amendment) Act, 2022) [192], яким визначено базові правові основи регламентації відносин щодо цієї предметної сфери. Окрім того, затверджено низку нормативно-правових актів нижчої юридичної сили, покликаних деталізувати певні аспекти у вказаній області (Правила Багамських Островів про індустрію цінних паперів (контракти на різницю) (2020) [98] тощо).

Зазначений нормативно-правовий акт присвячений загальним питанням щодо обороту цифрових активів, у тому числі в ньому окреслена базова компетенція товарних бірж. Водночас самого акценту на загрозливий прояви цифрових засобів ураження не спостерігається, що обумовлено різними факторами. Припускаємо, у першу чергу йдеться саме про законодавчий рівень, де описуються засадничі приписи та власне профілізація такого документу. Слід урахувувати факти очевидної новизни й визнаної малодослідженості предметного феномену. Також не остання роль відведена ініціативі створення додаткових умов для зростання обсягів інвестування в країну й способів досягнення таких цілей. Досвід Багамських Островів наочно показує, що саме посилення інвестиційної компоненти є провідним каталізатором для багатьох змін навіть на законодавчому рівні.

У той же час необхідно слушно зазначити, що їхня національна правова політика вирізняється прогресивністю у частині запровадження нових умов, найсприятливіших для обігу цифрових активів. Свідченням цього є істотно розширений і доопрацьований проєкт Закону «Про цифрові активи та зареєстровані біржі» від 2024 року (Digital Assets and Registered Exchanges Bill, 2024) [193], котрий спрямований на концептуалізацію лівової частки процедур у вказаній сфері й регламентацію багатьох інших фундаментальних аспектів, що не охоплюються чинним документом. Із-поміж іншого йдеться про питання саме протидії кіберзагрозам, які можуть виникати внаслідок операцій із

цифровими активами (пп. «n» п. 7 «Specific matters to be included» Part B (section 39) Contents of an Offering Memorandum) [193, с. 107]. Відповідно, слушно вести мову і про розвиток аналізованого напрямку у контексті цієї країни.

2. Бермудські Острови. Щодо Бермудських Островів, то профільний законодавчий акт – Закон Бермудських Островів «Про комерційні відносини з цифровими активами» від 2018 року (Digital Asset Business Act 2018) [97] охоплює широкий спектр позицій, пов'язаних із оборотом саме цифрових активів. Проте, як і в попередньому випадку, питанням відповідних загроз не приділена увага. Знову ж таки, припускаємо, що це обумовлено перерахованими вище факторами й, імовірно, матиме об'єктивізацію у різних актах (чи змін до них) в осяжному майбутньому. У силу технічного й технологічного розвитку цієї сфери можна очікувати на виникнення колективних запитів відносно механізмів із протидії деструктивним проявам.

В цілому ж державна правова політика Бермудських Островів, як і в випадку з Багамськими Островами, вирізняється прогресивністю зі стійкими прагненнями до розвитку таких ринків. Не публічний, але очевидний намір до зайняття позицій провідних гравців у глобальних масштабах [384] не йде в розріз їх правотворчим підсумкам та іншим санкціонованим крокам.

3. Канада. Відносно Канади, то зазначена країна давно стала на шлях легалізації цифрових активів. Розробка із подальшим прийняттям Закону «Про єдиний доступ до цифрових активів довірених осіб» від 2016 року (Uniform Access to Digital Assets by Fiduciaries Act 2016, UFADAA) [96] є тому наочним підтвердженням. Зокрема, він регламентує ряд засадничих аспектів в аналізованій сфері, що формують основу для володіння, користування й розпорядження вказаними активами, а також охороняє та захищає права учасників ринку та окреслює статус відповідних органів тощо.

Слід відзначити, що на законодавчому рівні питання відповідних загроз також не розкрито. Проте змістовне наповнення нормативних конструкцій дає мотивовані підстави вести мову про наявність так званих «запобіжників» щодо

превенції багатьом руйнівним проявам.

4. Китай. Попри те, що в Китаї офіційно заборонений оборот криптовалют, таке обмеження не поширюється на левову частку форм цифрових активів. Більше того, у жовтні 2023 р. Міністерством фінансових послуг і Бюро казначейства (FSTB) уряду Гонконгу спільно була оприлюднена заява про розвиток віртуальних активів [385]. При цьому слід відмітити, що представники уповноважених інституцій не оминули увагою питання запобігання й протидії відповідним загрозам. Одними із пріоритетних векторів є такі позиції: 1) легалізація (відмивання) доходів, отриманих неправомірними шляхами; 2) маніпулювання та зловживанням ринком; 3) відповідні кіберзагрози; 4) інші чинники, явища та тенденції [182, с. 12-13]. Аналізуючи наявну нормативно-правову базу, що регулює досліджувані нами суспільні відносини, відзначаємо, що, будучи одним із провідних гравців на міжнародній арені, Китай належним чином реагує на нові виклики, продиктовані реаліями цифрового середовища. Його політика хоч і носить консервативний, інколи вийнятковий сталий характер щодо певних цифрових новацій (криптовалюти), проте все ж поступово й планомірно враховує ці видозміни.

5. Сполучені Штати Америки. Зосереджуючи увагу на моделі США, доцільно вказати, що тематика цифрових активів урегульована у значній кількості штатів (Аризона, Вайомінг, Гаваї, Джорджія, Західна Вірджинія, Іллінойс, Колорадо, Коннектикут, Массачусетс, Мічиган, Нью-Джерсі, Огайо, Північна Дакота, Юта та багатьох інших). Попри широке висвітлення різних груп питань у межах цієї сфери власне такий компонент, як загрози, перебуває в процесі тривалого становлення. Поточна модель вирізняється активною увагою до руйнівних чинників, явищ і тенденцій, на кшталт: захист від витоку даних, забезпечення конфіденційності інформації про користувача тощо [194]. У додаток до цього значна увага приділена різним методам протидії легалізації (відмиванню) доходів, отриманих протиправним шляхом, зокрема і за рахунок функціоналу цифрових інструментів. У рамках такого вектору США навіть долучилися до Рекомендацій (звіти, керівництва, рекомендації) згаданої FATF,

котрі формують міжнародні стандарти AML та KYC для VASP [136], [182, с. 24-25]. Тому, порівняно з наведеними вище країнами, маємо визначити, що у США присутній різноплановий поступальний розвиток безпекової складової в окресленій сфері.

Окрім того, у законодавстві країн, попри відсутність прямої вказівки щодо категорії «цифровий актив», публічні політики націлені на комплексні розбудови цифрових середовищ шляхом об'єктивізації юридичного підґрунтя. На нашу думку, до такої умовної групи слід віднести держави, у яких питання цифрових активів і криптовалют урегульовані відносно в рівній мірі. Серед їхнього числа особливої уваги варті правотворчі результати й наміри Великої Британії, ОАЕ, Республіки Сінгапур (Сінгапур), Французької Республіки (Франції), Швейцарської Конфедерації (Швейцарії), Японської Держави (Японії) та інших.

1. Велика Британія. Як відмічалось нами вище, тематиці цифрових активів присвячена неабияка дослідницька увага на рівні офіційних дорадчих установ. Зокрема, у всіх згаданих вище звітах називається й обґрунтовується доцільність існування таких нагальних загроз: 1) шахрайство із певними типами цифрових активів (п. 17.52) [83, с. 371]; 2) волатильність цін і коливання ліквідності (п. 8.22) [84, с. 188]; 3) імовірність втручання у криптографічні методи обчислення (п. 2.58) [85, с. 21]; 4) відсутність ефективної правової бази (п. 4.9) [85, с. 58]; 4) інші.

Щодо самої нормативно-правової бази, то вона фокусується на побудові стабільних ринкових умов, посиленні захисту інвесторів та стійкому забезпеченні середовища, яке сприяє інноваціям [182, с. 22]. При цьому досить слушним є формування прозорого регулювання для створення цифрових технологій, а також належного захисту прав учасників відповідних відносин [182, с. 23]. Отже, можемо стверджувати, що управлінська діяльність Великої Британії у сфері забезпечення економічної безпеки держави щодо реагування на загрози цифрового середовища із-поміж іншого передбачає поступову розбудову відповідних механізмів реагування (на різних стадіях)

щодо однойменних подразників.

2. Об'єднані Арабські Емірати. Відповідні правові механізми, які існують в ОАЕ щодо ринку цифрових активів, за окремими аспектами набули вагомого розвитку. Більше того, присутність високого ступеня зацікавленості представників різних соціальних груп навіть зумовила необхідність трансформації деяких механізмів. Прийнятий у 2024 р. Закон «Про цифрові активи» – Закон DIFC № 2 від 2024 року (Digital Assets Law DIFC Law No. 2 of 2024) [195] врегульовує статус таких активів, окреслює засади охорони майнових прав щодо останніх, їх контролю, обороту тощо. Слід також звернути увагу на висловлювання J. Visser, який зазначив, що цифрові активи являють собою «... клас активів на трильйони доларів, і в них є значні можливості для майбутніх інновацій і ринкових можливостей» [196]. Тобто, укотре доводиться одна з фундаментальних авторських тез про винятково важливу й прогресивну їх роль для багатьох економічних процесів.

Законодавство ОАЕ пішло далі щодо регулювання суспільних відносин у цій сфері. У рамках цих новацій також було прийнято Закон безпеки – Закон DIFC № 4 від 2024 року (Law of Security – DIFC Law No. 4 of 2024) [197], котрий якраз покликаний убезпечити процеси, похідні від цифрових активів. Як відмічає згаданий J. Visser, він передбачає легалізацію юридичних осіб і платформ, що забезпечать надання кредитів під покриття чи заставу цифрових активів, посилення оцифрування міжнародних відносин та багато іншого [196]. Для нас, на цьому етапі дослідження, має значення те, що предметними питаннями опікуються саме з точки зору безпеки. Майже синхронне прийняття названих законодавчих актів свідчить про високу ступінь суверенних намірів щодо різновекторної розбудови цифрового середовища.

3. Сінгапур. Помітний інтерес до цифрових активів давно має місце в зазначеній країні. Основний регулятор цифрових активів – Грошово-кредитне управління Сінгапуру (MAS) стійко й активно удосконалює правову базу з метою формування найсприятливішого середовища для розвитку однойменної сфери. Активна правотворча діяльність є однією з похідних у контексті

публічних намірів щодо розвитку цього вектору в країні. У результаті чого пільгові ставки оподаткування, потужна фінансова інфраструктура і високе сприйняття багатьох форм таких активів [198] помітно посилюють вплив Сінгапуру в міжнародних масштабах.

Есебічна розбудова цифрової індустрії не оминула й коло питань щодо безпекової компоненти. Зокрема, держава тривалий час є активним учасником міжнародного діалогу щодо протидії легалізації (відмиванню) доходів, отриманих протиправним шляхом. Системно взаємодіючи з FATF, вона у різні способи реалізує відповідні міри реагування. Це дає вагомі підстави вести мову про поступальний розвиток безпекових засад відносно цифрового середовища.

4. Франція. Правова політика цієї країни за останні роки продемонструвала всіляку прихильність аналізованим суспільним здобуткам, вирізняючись також прогресивністю. Зокрема, не чекаючи набрання чинності Регламенту MiCA [189], керівництвом країни було приведено у відповідність ряд національних нормативно-правових актів [199], оперативно сприяючи уніфікації відповідних стандартів.

У той же час слід відзначити, що питання безпекового напрямку поки перебувають на початкових етапах. Безумовно, вагомі кроки було здійснено в частині контролю й нагляду за роботою постачальників послуг із цифрових активів. Ідеться про їх ідентифікацію та неухильне дотримання встановленого правопорядку. Також слід виділити питання страхування професійної цивільної відповідальності чи капіталу, власну систему безпеки і контролю, належне управління конфліктами інтересів тощо (ст. L54-10-5 Валютного фінансового кодексу Франції (Code monétaire et financier)) [200]. Можемо констатувати, що в цій країні зазначені проблеми поступово потрапляють у поле зору й вивчаються відповідними інституціями. Зазначене свідчить про позитивну динаміку з позиції розвитку безпекового напрямку, але все ж перебуває на ранніх стадіях.

5. Швейцарія. У цілому національне законодавство цієї країни орієнтовано на віртуальні активи й криптовалюти як пріоритетні одиниці цифрового виміру. Однак така стратегія не залише поза увагою й цифрових

активів, різні аспекти котрих мають інтерес, у тому числі із безпекової позиції.

Ідеться про долучення до колективних (у світових масштабах) заходів щодо запобігання й протидії легалізації (відмиванню) доходів, отриманих неправомірним шляхом із закономірною консолідацією зусиль із FATF [182, с. 23]. Політика Швейцарії вирізняється застосуванням превентивних заходів, покликаних мінімізувати можливі ризики й загрози від операцій із цифровими активами. Національним законодавством передбачена всіляка підтримка та контроль середовища, в якому учасники ринку вивчають пропозиції на основі блокчейну, зокрема – стартапи, та можуть тестувати продукти і послуги, взаємодіючи з регулюючими органами для забезпечення відповідності, зниження ризиків та забезпечення захисту споживачів [182, с. 23]. Значений аспект також має перспективне значення для розвитку безпекової інфраструктури на різних рівнях, у тому числі – міжнародному й міждержавному.

6. Японія. Країна є першою державою у світі, що запустила в обіг цифрові активи та давно усвідомила потребу регулювання останніх. Злам найбільшої у 2014 р. криптобіржі MtGox [386] відобразився на законодавчому розвитку їхньої безпекової компоненти. Відповідно, у цьому аспекті законодавство Японії є одним із найпрогресивніших у глобальних масштабах. До основних напрямів із протидії деструктивним чинникам і явищам слід віднести такі питання: 1) безпечність кіберпростору; 2) ефективна регуляторна політика; 3) запобігання легалізації (відмиванню) доходів, отриманих злочинним шляхом; 4) захист прав та інтересів учасників ринків цифрових активів; 5) підтримка стабільності криптовалют; 6) інші аспекти [182, с. 14-15]. Щодо конкретизації загроз, то вони будуть релевантними окресленим векторам роботи уповноважених суб'єктів.

Зважаючи на це, пропонується відмітити, що серед наявних підходів найпрогресивнішими слід вважати моделі Багамських Островів, Бермудських Островів, Великої Британії, Канади, Китаю, ОАЕ, Сінгапуру, США, Франції, Швейцарії та Японії. Перераховані держави ціленаправлено стали на шлях

стійкої комплексної правової, організаційної і технологічної розбудов національних цифрових середовищ. Результати їхньої правотворчої діяльності, стратегічні цілі й окремі проєктні роботи засвідчують безальтернативність подальшого руху в межах цього вектору розвитку. Проблематика безпекового спрямування у більшості з зазначених країн поки перебуває на стадії становлення, що зумовлено різними факторами.

Додатково порівнюючи розглянуті моделі, можемо відмітити, що лівова частка цих країн фундаментальні засади відповідних політик закріпила на законодавчому рівні (Багамські Острови, Бермудські Острови, Канада, ОАЕ, США та Франція). Окремі закріплюють стратегічні вектори відповідного руху (Китай, Швейцарія). Велика Британія детально опрацьовує такий напрям на рівні законодавчих комісій та інших авторитетних дорадчих органів.

Тематиці безпекової складової присвячена епізодична увага, як правило, в контексті інших, уже відомих і визнаних загроз (часто деякі форми цифрових активів породжують нові способи і засоби скоєння вже відомих суспільно-небезпечних діянь). Помітною прогресивністю, з позицій усвідомлення реалістичності й широкого спектра, за цим компонентом вирізняються (Велика Британія, ОАЕ, Сінгапур, США та Японія). Відносно персоналізації таких явищ і чинників, то зазвичай мовиться про питання легалізації (відмивання) протиправних доходів, кіберзлочинності, шахрайства й іншого. Законодавча база ОАЕ у цьому аспекті містить позиції відносно певних діянь міжнародного масштабу та супутніх питань.

3.2. Окреслення першочергових векторів для розбудови комплексного адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами

Стойка і всебічна розбудова цифрового середовища з мінімізацією

загрозливого ефекту для перебігу економічних процесів передбачає чітку, збалансовану, а також обов'язково послідовну державну правову політику щодо всіх предметних питань. Досвід неефективного державного управління осяжного минулого, в умовах обмеженого за кількістю та якістю ресурсного забезпечення, спонукає до результативних кроків, уникаючи точкових прорахунків і не допускаючи руху за хибними траєкторіями. Окрім цього, необхідно враховувати вагому роль темпоральної складової, зважаючи на потенціал лишень відомих людству цифрових засобів. Ураховуючи явні можливості для подальшого розвитку технологій блокчейну, токенизації, штучного інтелекту й решти (у тому числі маловідомих) інструментів такої природи, вказане має надважливе значення навіть уже в нинішніх умовах. Попри те, що Рекомендації Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року [122] і Регламент MiCA [189] оцінюють фінансову обстановку як помірковану з позиції впливу таких засобів (пункти 5 вступних частин), факти, наведені у підрозділі 1.3 із високим ступенем імовірності дають підстави стверджувати протилежне. До того ж Регламент MiCA [189] охоплює не всі форми цифрових активів, а також містить певні застереження, при настанні яких можливе погіршення фінансової ситуації під дією таких чинників, явищ і тенденцій.

Зазначене дає вагомі мотивовані підстави для провадження системної політики щодо розбудови цифрової складової. Це забезпечить належний базис для формування відповідних ефективних механізмів, покликаних приводити в дію необхідні заходи. Лише в такому випадку слушно розраховувати на адміністративно-правове регулювання, яке здатне відчутно посилити наявний безпековий потенціал, гармонійно синхронізуючись із рештою безпекових основ.

Реалізація кроків у наведеній послідовності безальтернативно має на увазі формування дорожньої карти для поступального розвитку зазначеного вектора. Зважаючи на невідворотність інтеграції цифрових інструментів у різні сфери суспільного життя та широке сприйняття останніх суспільством застосування

саме пропонованого підходу є найперспективнішим кроком.

Під цим кутом зору своєчасно, слушно і виправдано вести мову про розробку й визнання стратегічного (керуючись наявними національними правотворчими реаліями) акту із предметних питань чи доповнення і корегування існуючих документів такого типу. Загальновідомим є той факт, що Розпорядженням КМ України від 17 січня 2018 року [329] було схвалено Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки (далі – Концепція), а також затверджено План заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки (далі – План заходів щодо реалізації Концепції). Зазначені документи передбачали цілі, принципи, напрями та інші аспекти цифрового економічного розвитку України, у тому числі її гармонізацію з цифровими ініціативами, цифровий порядок денний для Європи (Digital Agenda for Europe) та єдиний цифровий простір (Digital Single Market) [329]. Іншими словами, передбачалася поступальна економічна цифровізація держави із активним долученням до провідних світових процесів, зокрема і країн ЄС.

З-поміж таких позицій прослідковується питання уникнення ризиків, що можуть виявлятися в рамках реалізації відповідних заходів Концепції [329], попри те, що ми у своєму дослідженні довели, що не доцільно ототожнювати ризики із загрозами, тому що перші можуть перекваліфікуватися в другі, формуючи несприятливі чинники та явища економічній складовій. Відповідно, слушно вести мову про побічне підтвердження загрозовості окремих проявів цифровізації щодо стійкого перебігу низки економічних процесів і появи тенденцій. Більше того, одним із принципів цифровізації визнається підвищенням рівня довіри і безпеки [329], що, знову ж таки, передбачає дієву протидію саме загрозам, якщо виходити з логіки Закону України «Про національну безпеку України» [1]. Тому вбачаємо хибним підхід не врахування загроз від операцій із цифровими активами як таких, що можуть впливати на відповідні індикатори й показники системи економічної безпеки України.

Вочевидь, успішність реалізації стратегічних намірів вимірюється

різними оцінюваннями, зазвичай – співставленням усіх отриманих підсумків очікуваним запитам. Одними із авторитетних і неупереджених мірил ефективності й результативності здійснення певних кроків є світові рейтинги, на які особливу увагу звертає спільнота. Таким шляхом пішли й автори Концепції [329], ініціювавши необхідність досягнення Україною показників у профільних міжнародних оцінюваннях (див табл 3.1)

Таблиця 3.1 Оцінки рівня ефективності реалізації Концепції [329] на основі провідних світових рейтингових організацій

Рейтинг	На 2016 р.	Наміри на 2020 р.	Результати у 2020 р.	Станом на 2023/24 р. (поточна ситуація)
Networked Readiness Index (WEF)	64	30	64	43
Global Innovation Index (INSEAD, WIPO)	56	40	45	60
ICT Development Index (ITU)	79	50	79 (на 2017 р.)*	–
Global Competitiveness Index (WEF)	85	60	104 (на 2019 р.)*	–

* рейтинги «ICT Development Index (ITU)» і «Global Competitiveness Index (WEF)» формувались до 2017 і 2019 рр., відповідно

Сформовано автором на основі [330], [331], [332], [333]

Як бачимо, очікувані наміри від реалізації аналізованих документів не були досягнуті за жодною з рейтингових позицій. Попри припинення оцінювання в рамках програм «ICT Development Index (ITU)» [332] і «Global Competitiveness Index (WEF)» [333] тогочасні тенденції не засвідчували факти саме руху за конструктивною траєкторією. До того ж за більшістю позицій спостерігається істотне розходження із показниками минулого, що явно вказує на складні проблеми, зокрема й безпекового плану.

Такі аргументи дають мотивовані підстави визнати, що лєвова частка цілей Концепції [329] не була досягнута, а інші – не виконані у повній мірі. Зважаючи на вплив строку для її реалізації, а також враховуючи відсутність альтернативних документів щодо цих питань, виникає об'єктивна необхідність переосмислення потреби розробки концептуального акту.

Варто зазначити, що Розпорядженням КМ України від 3 березня 2021 року [334] було схвалено Концепцію розвитку цифрових компетентностей і затверджено План заходів з реалізації Концепції розвитку цифрових компетентностей. Проте виходячи зі змісту останніх, йдеться не про зміну попереднього документа, а деталізацію положень саме щодо розвитку цифрових компетентностей. Можна також згадати Стратегію кібербезпеки України. «Безпечний кіберпростір – запорука успішного розвитку країни» від 26 серпня 2021 року (абз. 13 п. 1) [163], в якій частина здобутків цифрового світу розглядається як загроза кібербезпеці. Проте документ не містить конкретизації останніх, оперуючи загальними термінами. Що більш важливо, пропонуване бачення оминає економічний блок, з огляду на профілізацію вказаного документа.

Тому на сучасному етапі функціонування держави в Україні відсутній стратегічний документ із питань подальшого належного цифрового розвитку, що релевантний осучасненим суспільним запитам. Аналогічна ситуація стосується й відповідних безпекових орієнтирів і пріоритетів, котрі варті уваги під зазначеним та вище розкритим кутом зору.

У контексті безпекових векторів слід звернути увагу на Стратегію національної безпеки України [2], котра є системоутворюючим стратегічним документом в однойменній сфері. П. 9, що присвячений важливим аспектам поточних і прогнозованих загроз національній безпеці України й відповідним національним загрозам, серед таких чинників і явищ виділяє наступні підпитання, дотичні репрезентованій проблематиці: 1) стрімкі технологічні зміни; 2) розробки у сфері штучного інтелекту, зокрема й ті, що докорінно трансформують економіку; 3) інші фактори [2]. Наведені елементи можуть мати

прямий та опосередкований стосунки до цифрових засобів і відповідно це вкотре доводить загрозливість окремих проявів останніх.

У той же час слушним буде приведення до відповідності цих категорій задля окреслення чітких контурів потенційних безпекових мір. У абз. 4 пп. 14 п. 4 Положення про Міністерство цифрової трансформації України від 18 вересня 2019 року одразу використовуються такі одиниці, як блокчейн, віртуальні активи, токени і штучний інтелект [270]. На наше переконання, варто проаналізувати питання щодо кореляції всіх названих правоположень під егідою цифрових засобів.

Існуюча стратегічна вказівка відносно потенційної докорінної зміни структури чи порядку перебігу економічних процесів зумовлює думку про можливе доповнення Стратегії економічної безпеки України [3] як загального плану дій щодо відповідного безпекового напрямку функціонування держави і діяльності суспільства. Абз. 3 п. 18 документа визначено, що одним із завдань у сфері забезпечення економічної безпеки є гарантування національної економічної незалежності, а також здатності до захисту національних економічних інтересів, зокрема і у високотехнологічній сфері [3]. Виходячи із відомих іноземних досліджень [335], [336], [337], можна зробити точковий висновок про приналежність цифрових активів якраз до такої групи. При цьому, зважаючи на швидкий вплив строку дії такого документа, пропонований вектор має бути врахований під час розробки наступного акту. Отже, навіть при нинішній парадигмі існує зобов'язання забезпечення саме економічної безпекової складової від руйнівного впливу цифрових засобів ураження.

Попри такі приписи їх дійсна ефективна та результативна реалізація можлива винятково при наявності відповідного адміністративно-правового забезпечення. У розділі 2 нашого дисертаційного дослідження було розкрито питання специфіки такого регулювання крізь призму наступних провідних атрибутів: 1) адміністративно-правові засади; 2) суб'єкти; 3) взаємодія цих суб'єктів; 4) контроль та нагляд у предметній сфері. За результатами аналізу відповідних нормативно-правових конструкцій та беручи до уваги

правозастосовні практики, було аргументовано встановлено, що наявні відповідні механізми лишень фрагментарно охоплюють безпекові питання такого спрямування. Існуючі прогалини обмежують функціонал публічних інституцій (Мінцифри, Держфінмоніторинг, НКЦПФР, НБУ, БЕБ, ДБР, НАБУ, НП, СБУ та інших суб'єктів і громадян), формуючи вузьке й хитке підґрунтя для реалізації власної компетенції у зазначеній сфері.

Ураховуючи результати нашого дисертаційного дослідження, ми вважаємо, що найпершим стратегічним завданням є розробка сприятливого теоретико-методологічного та методичного підґрунтя для майбутньої розбудови комплексного й збалансованого адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Наступним фундаментальним кроком має бути утворення юридичного підґрунтя для подальшої розбудови системи економічної безпеки України і формування необхідних реагувань на відповідні подразники, у тому числі загрозливого характеру.

При цьому вагомою є уніфікація таких підходів із міжнародними стандартами за для впровадження наднаціональних дієвих форм, методів, способів і засобів запобігання й протидії відповідним загрозам. У такому контексті мова повинна йти про найскорішу імплементацію Регламенту МіСА [189], котрому не відповідає зміст ряду норм Закону України «Про віртуальні активи» та інших вітчизняних джерел права. Наведений варіант розвитку подій не містить альтернатив із огляду на стійкі проєвропейські прагнення українського народу та численні вже реалізовані заходи за вказаним вектором.

Наступним кроком має стати вирішення питання щодо розмежування та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів) шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу. З точки зору наявних здобутків цивілізаційного суспільства першочергово належної уваги мають заслуговувати

питання розробки загальних комплексних адміністративно-правових засад, із особливим акцентом на питання рівнів і напрямів функціонального впливу, взаємодії, контролю і нагляду, а також запобігання та протидії проявам економічної злочинності. У контексті злочинності йдеться саме про діяння, вчинювані за допомогою різних форм цифрових засобів ураження економічних процесів.

Такі питання, з одного боку, якраз є першочерговими і базовими напрямами для розбудови комплексного та збалансованого адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, котрі можуть виникати внаслідок операцій із цифровими активами, що відповідає концепту завдання нашого дослідження. З іншої сторони, їх поступове вирішення має вагомое значення для окремих безпекових сфер в умовах сьогодення. Оскільки ті ж самі прояви економічної злочинності істотно послаблюють і так виснажений війною економічний потенціал держави [6, с. 172, 299-300], [338, с. 8-9], [339, с. 251-252], що не допустимо на третій рік повномасштабного вторгнення. Різні їхні прояви, на кшталт: кіберзлочини [340], [341, с. 60-61], правопорушення проти власності, шахрайство, у тому числі в корпоративному управлінні [339, с. 250] та інші діяння деструктивного спрямування [342, с. 97-98] посилюють відповідний вплив на весь безпековий сектор.

Закладення основ для вирішення такого спектра проблем має виняткове значення для України під різними кутами зору. Стабільне отримання міжнародної технічної та гуманітарної допомог передбачає впевненість партнерів у стійкості безпекового середовища та руху за визнаними демократичними орієнтирами. Одним із напрямів такої політики є системне удосконалення законодавства у безпековій сфері як свідчення гарантування належного використання ресурсів та послуг на колективні суспільні блага та недопущення різних маніпуляцій із неправомірних мотивів.

Україна, будучи тривалий час активним бенефіціаром міжнародної технічної [343, с. 691-692], [344, с. 3-4], [345, с. 4-5] та з недавніх пір

вимушеним реципієнтом значних обсягів гуманітарної допомоги, потребує належних законодавчих основ і стратегічних намірів щодо розвитку безпекового сектора. На відміну від багатьох провідних іноземних держав [346, с. 122-123], на національних теренах гострою є проблема ефективного контролю за розподілом і використанням міжнародної технічної [344, с. 4], [345, с. 5], [347, с. 151] та гуманітарної [348, с. 45-46, 54-55] допомог, її стійке надходження є важливим із позиції життєздатності країни загалом.

Розглянута й численна когорта інших прикладів із урахуванням аргументів у вступній частині дисертаційної роботи спонукає до думки про безальтернативність у частині розбудови безпекового вектору. Зважаючи на визнані економічні безпекові прагнення (абз. 3 п. 18 [3]), це має пряме відношення і до цифрових активів, які, окрім низки істотних переваг, мають і негативні сторони.

Ініційоване коло проблемних позицій вартує уваги якраз із точки зору про окреслення першочергових векторів розбудови адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Поточний ступінь наукової розробки проблематики та наявні масштаби закріпленості санкціонованих механізмів дають підстави вести мову саме про таку стадію. Розуміння ключових векторів забезпечить розбудову оптимальних траєкторій розвитку законодавства та мінімізує застосування неперспективних тактик. Оскільки затвердження (схвалення) ризикових концептуальних документів (стратегій, концепцій, програм, планів тощо) в сучасних умовах є несвоєчасним та фінансово обтяжливим для української держави. Тому слід підготувати до реалізації певних векторів лишень із позиції реалістичності, себто реальної здатності виконати всі поставлені завдання. У зворотному випадку можна очікувати розбалансування державного управління та ускладнення суміжних управлінських процесів.

3.3. Шляхи реалізації напрямів формування комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами з урахуванням досвіду іноземних країн

Окреслені й мотивовані першочергові кроки розбудови відповідного адміністративно-правового забезпечення проваюють на представлення і обґрунтування доцільності дзеркальних шляхів їхньої юридичної реалізації. Такі ініціативи сформовані на основі результатів, отриманих під час вирішення попередніх завдань дисертації, і покликані забезпечити досягнення мети роботи. З-поміж іншого наведені підсумки є завершальними у частині аналізу об'єктів наукового пізнання і мають утворити цілісний спектр перспективних варіантів вирішення найнагальніших проблем цієї тематики. Маємо сподівання, що наведені нижче та решта результатів стануть у нагоді під час подальших розвідок указаних і суміжних питань.

Відносно прикладних аспектів, то слід укотре зауважити, що Законом України «Про національну безпеку України» визначено контури однойменної політики, у межах яких провадяться похідні заходи різного характеру. Однак нормативна логіка побудови такого документа не передбачає конкретизацію і класифікацію загроз для безпекового сектора, будучи націленою на інші засадничі організаційні основи.

Більше того, ч. 1 ст. 26 зазначеного законодавчого акту визначено, що основні напрями державної політики з питань національної безпеки визначаються саме у Стратегії національної безпеки України, яка становить ключовий документ довгострокового планування [1]. Не суперечачи правотворчій логіці, сфокусуємо увагу саме на стратегічних положеннях, що також відповідає висвітленому концепту в попередньому підрозділі.

Названий стратегічний акт, окрім інших закономірних атрибутів містить самостійну позицію щодо поточних та прогнозованих загроз однойменній безпеці та національним інтересам України із урахуванням

зовнішньополітичних та внутрішніх умов [2]. Як уже зазначалося, п. 9 документа присвячений питанням загроз, що дотичні (розробки у сфері штучного інтелекту) або похідні саме від операцій із формами цифрових активів (стрімкі технологічні зміни та інші фактори), тим самим несвідомо підкреслюючи руйнівну значущість останніх. У цьому абзаці міститься вказівка про докорінну трансформацію економіки від окермих проявів таких здобутків цивілізаційного соціуму.

Ми хочемо відмітити наступне: семантично такі формулювання у повному обсязі не охоплюють орієнтовну типологізацію аналізованих активів, що може призвести до колізій та інших невизначеностей на практиці. Усвідомлюючи реалістичність цієї ситуації та зважаючи на термінологічну неусталеність, пропонується **уточнити відповідну позицію стратегічного акту**, доповнивши новими категоріальними одиницями.

Зокрема, перше речення п. 9 Стратегії національної безпеки України, варто викласти у наступній редакції: *«Стрімкі технологічні зміни, насамперед в енергетиці, біотехнологіях та цифровій сфері, розробки у сфері штучного інтелекту тощо докорінно трансформують економіку і суспільство в цілому»*. Фактично, ми змістовно докорінно не змінили представлену стратегічну позицію, а лише сформулювали умови для розширеної градації відповідних загроз. Іншими словами, мову доцільно вести про формування поля для розробки такої тематики, не обмежуючись вузьким колом форм прояву аналізованих вище чинників, явищ і тенденцій.

При цьому свідомо було ініційовано обіг категорії цифрове середовище і відхилено термін «цифрові активи». Такий підхід пояснюється наданням переваги з боку законодавця категорії «цифрові речі» і залишенням поза визнанням аналізованої нами дефініції. Попередньо ми, з урахуванням думок В. Бацуци [100, с. 34-35; 93, с. 33-34, 61], О. Даниленко [101, с. 150-151, 152-153] й О. Кудь [78, с. 2-3, 6, 7-8] та інших видатних науковців, прийшли до висновку про доцільність і методологічну обґрунтованість офіційного вжитку саме терміна «цифрові активи». На користь представлені логіки виступають і

законодавчі акти іноземних держав (Багамські Острови (Закон «Про цифрові активи та зареєстровані біржі» (зі змінами) від 2022 року (Digital Assets and Registered Exchanges (Amendment) Act, 2022)) [192], Бермудські Острови (Закон Бермудських Островів про комерційні відносини з цифровими активами 2018 року (Digital Asset Business Act 2018)) [97], Канада («Закон про єдиний доступ до цифрових активів довірених осіб» від 2016 року (Uniform Access to Digital Assets by Fiduciaries Act 2016, UFADAA)) [96], ОАЕ (Закон про цифрові активи – Закон DIFC № 2 від 2024 року (Digital Assets Law DIFC Law No. 2 of 2024)) [195], США (Закон «Digital assets-existing law» [87] (штат Вайомінг), Закон про довірений (фідучіарний) доступ до цифрових активів від 2015 року (Revised Uniform Fiduciary Access to Digital Assets Act 2015, RUFADAA) [91], Закон штату Массачусетс про доступ до облікових записів електронної пошти спадкодавця (Massachusetts Law on Access to Decedent Email Accounts) [94], Закон штату Іллінойс стосовно цифрових активів (Illinois Digital Asset Law)) [95]), Франція (Валютний фінансовий кодекс Франції (Code monétaire et financier)) [200]) та інших). Проте питання визначення доцільності вжитку тієї чи іншої категорії на законодавчому рівні перебуває поза нашою увагою. Це обмежує аргументацію у пріоритетності згаданих одиниць, що робить недоцільним такого змісту корективи до наведеної позиції стратегічного документа. Натомість пропонуване словосполучення релевантне відповідним характеристикам цифрових активів і може бути використане під наведеним кутом зору, не суперечачи легалізованій дефініції.

Похідним актом, вартим предметної уваги, є Стратегія економічної безпеки України [3]. В дослідженні ми неодноразово загострювали увагу на тому, що одним із завдань відносно забезпечення такої безпеки (відповідно і системи економічної безпеки України) є гарантування національної економічної незалежності та здатності щодо захисту національних економічних інтересів, зокрема і у високотехнологічній сфері [3]. У відомих наукових джерелах іноземного походження чітко й неодноразово прослідковується теза щодо включення до такої категорії багатьох визнаних типових форм цифрових

активів [335], [336], [337]. Водночас беззаперечною є обставина, що в рамках здійснення правозастосовних заходів безумовним залишається слідування чітким приписам нормативно-правових актів [371]. У зворотному випадку можна зіткнутися з успішним оскарженням відповідних дій суб'єкта реалізації таких заходів, знівелювавши власні зусилля та неефективно використавши своє ресурсне забезпечення, сформоване за рахунок коштів платників податків, міжнародної технічної і гуманітарної допомог.

Такий підхід передбачає конкретизацію юридичних приписів задля чіткого розуміння предметних питань, постановки цілей і визначення завдань у рамках реалізації певних заходів. Усвідомлюючи ту вагому обставину, що термін «високотехнологічна сфера» не знайшов свого відображення у чинних нормативно-правових актах, у тому числі проєкті Розпорядження КМ України «Про схвалення Стратегії розвитку високотехнологічних галузей до 2025 року та затвердження плану заходів щодо її реалізації» від 2016 р. [349], виникає потреба уточнення відповідних положень. З огляду на широку полівекторну змістовну охопленість такого поняття, а саме включення до нього інших об'єктів матеріального й нематеріального світу, які не доцільно розцінювати в статусі цифрових активів, слід піти шляхом, обраним і для Стратегії національної безпеки України [2], а саме доповнивши предметну позицію.

Виходячи з цього, пропонується абз. 3 п. 18 Стратегії економічної безпеки України [3] **викласти у такому змісті:** *«Основними завданнями у сфері забезпечення економічної безпеки є: ...»*

«... гарантування національної економічної незалежності та здатності до захисту національних економічних інтересів, зокрема у високотехнологічній сфері, у тому числі з питань цифрового розвитку, цифрової економіки, цифрових інновацій та технологій». Пропоноване уодноманітнення з нормами Положення про Міністерство цифрової трансформації України від 18 вересня 2019 року [270] із одного боку має посилити синхронізацію управлінських заходів щодо різних граней цифрових засобів, а з іншого – охопити максимальну кількість предметних позицій.

Заключним комплексним підпитанням є **окреслення дорожньої карти** для ефективної й результативної, у тому числі послідовної і, водночас, адаптивної державної правової політики за предметним напрямом. Іншими словами, йдеться про шляхи пріоритетної розбудови адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Вони мають стати гармонійним доповненням пропонованих намірів у Стратегії національної безпеки України [2] та Стратегії економічної безпеки України [3], фактично втілюючи в життя окреслені безпекові орієнтири.

Із огляду на недосягнення цілей Концепції [329], а також ураховуючи вузький предметний орієнтир суміжних документів (Концепція розвитку цифрових компетентностей від 3 березня 2021 року [334], Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року від 17 листопада 2021 року [350] та ін.), **окремо слід розглянути питання відносно пролонгації дії такого документа**. Відмінною рисою зазначеного акта мають стати чіткі й виважені темпоральні строки і терміни досягнення поставлених цілей, а також залучення представників фахової міжнародної та вітчизняної спільнот для ефективного моніторингу власне її реалізації. Переконані, це має запобігти появі прорахунків минулого та наростити можливості цифрової економіки за різними напрямками.

При цьому увагу необхідно присвятити багатьом безпековим векторам, про які йшлося вище. Слідуючи орієнтирам попереднього підрозділу дисертації та враховуючи надскладний характер дискусійних питань, на нашу думку, увагу слід звернути **на наступні позиції**:

1) активне виконання комплексних типологічних досліджень Мінцифри, Держфінмоніторингу, НКЦПФР, НБУ, БЕБ, ДБР, НАБУ, НП, СБУ, а також Міністерством фінансів України (далі – Мінфін), зацікавлених закладів вищої освіти (далі – ЗВО), насамперед наукових установ, що досліджують вплив цифрових засобів ураження на підвідомчі сфери (за прикладами FATF і

ESMA, а також Великої Британії, Німеччини, Сінгапуру, США, Франції, Швейцарії й інших країн). Належна теоретико-методологічна основа забезпечить формування й стійку реалізацію збалансованої державної правової політики;

2) розроблення Міністерством фінансів України відповідного правового забезпечення для здійснення аудиту ефективності національної фінансової системи на предмет оцінки руйнівного впливу цифрових засобів та безпосередня такого аудиту із можливим залученням закордонних партнерів. Вітчизняні й іноземні практики засвідчили: на сучасному етапі найуразливішими є саме фінансові системи, що спонукає до відповідного аналізу певних індикаторів і показників;

3) створення робочих груп (за прикладом Китаю, Швейцарії, Японії та інших країн) за участі представників Мінцифри, Мінфіну, FATF, Держфінмоніторингу, НКЦПФР, НБУ, БЕБ, ДБР, НАБУ, НП, СБУ, а також ESMA, зацікавлених ЗВО, насамперед наукових установ і представників вітчизняної й іноземної фахової громадськості для висвітлення та аналізу проблемних питань у цій сфері. Обмін результатами ініційованих вище типологічних досліджень забезпечить напрацювання шляхів для вирішення низки організаційних та інших проблем на методичному рівні;

4) проведення спільних засідань учасників Комітету з питань економічного розвитку, Комітету з питань національної безпеки, оборони та розвідки, Комітету з питань правоохоронної діяльності, Комітету з питань цифрової трансформації щодо загроз для економіки, продиктованих цифровим розвитком, а також цифровими інноваціями і технологіями для ініціювання змін до чинного законодавства. Також важливим є питання адаптації норм чинного профільного правового забезпечення (Закону України «Про віртуальні активи» та інших нормативно-правових актів) у відповідність до Рекомендацій Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року [122], Керівництва FATF [136] та Регламенту MiCA [189] та інших документів, зважаючи на міжнародні зобов'язання України;

5) активізація правоохоронного напрямку в сфері обігу цифрових активів для протидії та запобіганню фактам стійкого обходу санкційних обмежень країною агресором [166, с. 43] і застосунку різних методів гібридної війни для впливу на стійкий перебіг вітчизняних економічних процесів шляхом використання різних форм цифрових активів. Такі засоби продукують нові способи проявів економічної злочинності, що є несвоєчасним для виснаженою війною й похідними викликами країни.

Складність зазначених явищ і специфіка національної підслідності [246] зумовлюють потребу консолідації зусиль суб'єктів правоохоронної діяльності БЕБ, ДБР, НАБУ, НП, СБУ. Не останню роль у цьому аспекті має відігравати поглиблення взаємодії з FATF, Держфінмоніторингом та компетентними органами іноземних держав (Багамські Острови, Бермудські Острови, Велика Британія, ОАЕ, Канада, Сінгапур, США, Франція, Швейцарія, Японія та ін.), котрі посилять відповідні заходи. Зважаючи на прогресивний потенціал указаних активів [355, с. 76; 139, с. 511-512; 140], [356, с. 163-164; 357], консолідація зусиль є своєчасним і виправданим кроком у складних реаліях дійсності [358, с. 448-449; 359, с. 381-382]. Тому намір щодо поглиблення взаємодії безпосередньо як практичних заходів у сучасних умовах займає особливе місце, зважаючи на наявний руйнівний і наростаючий тиск у різних економічних галузях.

Виходячи з цього, у разі пролонгації строку реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки від 17 січня 2018 року [329], її варто доповнити позиціями щодо розвитку безпекового напрямку із предметних питань:

1. Розділ *«Основні цілі цифрового розвитку»* доповнити наступними положеннями:

«... дотримання балансу між цифровим розвитком та стійкістю національних економічних інтересів від можливого руйнівного впливу цифрових інновацій та технологій ...».

2. Принцип 7. Розділу *«Принципи цифровізації»* викласти у наступній

редакції:

«Принцип 7. Цифровізація повинна супроводжуватися підвищенням рівня довіри і безпеки.

Інформаційна безпека, кібербезпека, стійке функціонування системи економічної безпеки України, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками».

3. Розділ *«Напрями цифрового розвитку»* доповнити рубрикою *«Система економічної безпеки України»*, представивши її зміст у такому вигляді:

«Система економічної безпеки України

Стійкість національної економіки під впливом чинників, явищ і тенденцій різного походження є одним із провідних завдань, визнаних на конституційному рівні. Зниження відповідних індикаторів і показників, невідповідність визнаним критеріям недопустимі в умовах тривалого ведення й прогресування методів гібридної війни.

Запобігання й протидія будь-яким загрозам і ризикам для економіки має особливе значення, зважаючи на її роль у структурі національної безпеки України. Цифрові інновації та технології, окрім значної кількості переваг, характеризуються і руйнівними проявами. Використання їхнього функціоналу в протиправних цілях може позначитися на багатьох економічних процесах, підриваючи виснажений економічний потенціал держави.

Відносна новизна і недостатня розробка численних форм цифрових засобів зумовлюють потребу під різними кутами оцінювати такі інновації й технології. Світові практики показують, що деякі цифрові інструменти успішно використовуються в якості засобів і способів руйнування елементів економічних систем, знищуючи або викривлюючи усталені конклюдентні алгоритми й практики перебігу відповідних процесів.

Поточні умови зумовлюють виникнення потреби визначення основних напрямів для розбудови механізмів належного реагування на такі подразники. У подальшому це має забезпечити створення ефективної системи запобігання їй протидії багатьом чинникам, явищам і тенденціям цифрового походження, що можуть впливати на різні складові національної економічної системи.

Серед першочергових ініціатив є:

виконання комплексних типологічних досліджень Міністерством цифрової трансформації України, Міністерством фінансів України, Державною службою фінансового моніторингу України, Національною комісією з цінних паперів та фондового ринку, Національного банку України, Бюро економічної безпеки України, Державним бюро розслідувань, Національним антикорупційним бюро України, Національною поліцією, Службою безпеки України, присвячених впливу цифрових засобів ураження на підвідомчі сфери, а також зацікавленими закладами вищої освіти;

Міністерству фінансів України розробити механізм здійснення аудиту ефективності національної фінансової системи на предмет оцінки руйнівного впливу цифрових засобів, а також провести однойменні заходи;

створення робочих груп за участі представників Міністерства цифрової трансформації України, Міністерства фінансів України, FATF, Державної службою фінансового моніторингу України, Національної комісії з цінних паперів та фондового ринку, Національного банку України, Бюро економічної безпеки України, Державного бюро розслідувань, Національного антикорупційного бюро України, Національної поліції, Служби безпеки України, а також ESMA, зацікавлених закладів вищої освіти, представників вітчизняної й іноземної фахової громадськості для висвітлення та аналізу проблемних питань у цій сфері;

проведення спільних засідань учасників Комітету з питань економічного розвитку, Комітету з питань національної безпеки, оборони та розвідки, Комітету з питань правоохоронної діяльності, Комітету з питань цифрової трансформації щодо загроз для економіки, продиктованих цифровим

розвитком, а також цифровими інноваціями і технологіями та за необхідності ініціювати зміни до чинного законодавства, а також щодо адаптації норм у відповідність до міжнародних стандартів;

посилення взаємодії у рамках правоохоронної діяльності щодо відповідних протиправних діянь».

Перераховані кроки спрямовані на реалізацію першого напрямку, що запропонований у підрозділі 3.2 дисертаційного дослідження. Усі результати таких заходів матимуть вагоме значення для досягнення цілей наступного вектора, а саме – формування юридичних основ для подальшої розбудови системи економічної безпеки України і утворення механізмів реагування на відповідні подразники, у тому числі загрозового характеру.

Підсумки виконаних комплексних типологічних досліджень під егідою попереднього вектора ляжуть в основу вже розробки юридичного підґрунтя із розбудови згаданої системи й механізмів. Результати аудиту ефективності національної фінансової системи на предмет оцінки руйнівного впливу цифрових засобів будуть додатковим вагомими і наочно доведеними аргументами щодо нагальної та дійсної потреб удосконалення існуючих адміністративно-правових засад. До того ж вони покажуть найуразливіші місця фінансової системи, тим самим надаючи змогу зосередитися щодо найскладніших питань.

Наведені вище переваги також можна буде отримати в рамках висвітлення та аналізу проблемних питань у цій сфері за підсумками спільних обговорень представниками Міністерства цифрової трансформації України, Міністерства фінансів України, FATF, Державної служби фінансового моніторингу України, Національної комісії з цінних паперів та фондового ринку, Національного банку України, Бюро економічної безпеки України, Державного бюро розслідувань, Національного антикорупційного бюро України, Національної поліції, Служби безпеки України, а також ESMA, зацікавлених ЗВО, представників вітчизняної й іноземної фахової громадськості. Відповідно, уже ініційовані рішення суб'єктів правотворчості

будуть обґрунтованими, маючи належну теоретико-методологічну й методичну розробки.

У межах хронологічно першого вектора роль Комітету з питань економічного розвитку, Комітету з питань національної безпеки, оборони та розвідки, Комітету з питань правоохоронної діяльності та Комітету з питань цифрової трансформації зводилась до наступних проявів законопроектної функції: 1) попередній розгляд та підготовка висновків і пропозицій щодо законопроектів, унесених суб'єктами законодавчої ініціативи на розгляд відповідному органу; 2) попередній розгляд та підготовка висновків і пропозицій щодо проєктів загальнодержавних програм економічного та науково-технічного розвитку (п. п. 2, 4 ч. 1 ст. 12 Закону України «Про комітети Верховної Ради України» [354]). Натомість у рамках цього напрямку мову слід вести про практичну реалізацію інших проявів згаданої функції. Мова, зокрема, йде про питання розробки проєктів законів, інших актів Верховної Ради України (п. 1 ч. 1 ст. 12 [354]), тобто формування правового інструментарію для відповідної сфери суспільних відносин. Така ж логіка має місце і у випадку функціональної діяльності решти згаданих міністерств та центральних органів виконавчої влади, одним із завдань яких є розробка проєктів законів та інших нормативно-правових актів з питань, що належать до їхньої компетенції чи внесення на розгляд відповідних пропозицій (абз. 3 ст. 9 [361], пп. 2 п. 4 [270], пп. 2 п. 1 [273], пп. 2 п. 4 [360]). Це стосується й питання поглиблення взаємодії у рамках правоохоронної діяльності, підсумки якої також мають вагомим значенням для досліджуваної сфери особливо в нинішній період.

Формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів реагування на відповідні подразники має продовжитися під егідою такого вектора, як вирішення питання щодо розмежування компетенції та посилення ролі більшості самих суб'єктів аналізованої системи (персоніфікованих органів), шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу. У

2 розділі дисертації було доведено існування окремих механізмів, які фрагментарно можуть впливати на незначну частку процесів, що становлять дослідницький інтерес. Натомість, сама система економічної безпеки України взагалі не адаптована до таких загроз, про що йшлося у першому розділі роботи. Під час вирішення завдання, якому було присвячене питання 3.2, було встановлено й доведено, що це зумовлено наявними підходами на законодавчому, а також стратегічному рівнях. Тому навіть після реалізації заходів у рамках другого напряму додаткової уваги вартуватиме адміністративно-правове становище суб'єктів зі спеціальною компетенцією й, імовірно, деяких інших установ.

Зважаючи на роль адміністративно-правового статусу [364, с. 207] та його виключних особливостей [362, с. 98-99], [363, с. 37-38], [365, с. 172], [366, с. 30], саме акцент щодо вказаної позиції із похідними підпитаннями є виправданим кроком. До того ж пропоноване нами бачення його структури у підрозділі 2.2 доводить міркування про слушність аналізу відповідних положень. Це позитивно відобразиться на поглибленні взаємодії, оптимізації контролю та нагляду, підвищенні ефективності запобігання й протидії проявам економічної злочинності із використанням функціоналу цифрових засобів ураження. Хоч опосередкований, але важливий стосунок воно матиме й для формування саме комплексних адміністративно-правових засад, чіткого визначення рівнів і напрямів функціонального впливу, а також багатьох інших, у тому числі суміжних критичних питань.

Під час реалізації заходів із удосконалення адміністративно-правового становища, насамперед суб'єктів зі спеціальною компетенцією, уваги варті міжнародні стандарти і відповідні моделі, а також практики іноземних держав. Навіть попри недостатню розробку такої тематики, уваги заслуговують моделі Австралії, Багамських Островів, Бермудських Островів, Великої Британії, Казахстану, Канади, Китаю, Кіпру, Мальти, Молдови, Німеччини, ОАЕ, Сінгапуру, США, Філіппін, Франції, Швейцарії, Швеції, Японії та ін. Як було з'ясовано у підрозділі 3.1, державні правові політики окремих цих країн

переважно орієнтовані на регулювання відносин із питань обороту криптовалют. Незважаючи на такий підхід, загальне розуміння тамтешніх основ справить позитивний ефект на вітчизняні правотворчі процеси. Тим паче криптовалюти, будучи формами цифрових активів, також потребують уваги як самостійних засобів, так і з позиції приналежності й зв'язків з функціонально ширшими явищами.

Якщо безпосередньо фокусуватись на розкритих у розділі 2 аспектах адміністративно-правового регулювання, то з позиції проведення спільних заходів на поточному етапі також уваги вартий досвід усіх перерахованих держав. Окрім того, варто сфокусуватись на різних формах і похідних від загального питання (обіг цифрових активів) напрямах міждержавної взаємодії за участі Австралійської комісії з цінних паперів та інвестицій (ASIC), Бюро казначейства (FSTB) (Китай), Грошово-кредитного управління Сінгапуру (MAS), Комісії з цінних паперів та бірж (SEC) (США), Дубайського фінансового центру (DIFC) (ОАЕ), Комісії з цінних паперів і ф'ючерсів Гонконгу (SFC) (Китай), Мальтійської організації з регулювання фінансових послуг (MFSA), Міністерства фінансових послуг (Китай), Податкової служби США (IRS) (США), Регіонального регуляторного органу ADGM (ОАЕ), Управління нагляду за операціями фінансового ринку Швейцарії (FINMA), Фінансового наглядового органу (FCA) (Велика Британія), Фінансової служби протидії фінансовим злочинам (FinCEN) (США), Фінансової служби Японії (FSA) та іншими контролюючими, наглядовими, правоохоронними й іншими органами, а також дорадчими суб'єктами і науково-дослідними установами.

Також слід враховувати діяльність суб'єктів міжнародного права (ESMA, ЄС, ЄЦБ, FATF, OECD та ін.), яка, з огляду на євроінтеграційні прагнення України, носить взірцевий характер. Вона не лише заслуговує дослідницької уваги, а й низка відповідних положень має бути інтегрована до вітчизняної правової площини. З огляду на це, стійка комунікація із такими інституціями поживить і оптимізує відповідні заходи, відчутно сприяючи посиленню безпековому потенціалу України.

У цьому аспекті слід виділити підпитання посилення правоохоронної діяльності шляхом консолідації зусиль із суб'єктами міжнародного рівня (Європейське поліцейське управління (Європол), FATF, Міжнародна організація кримінальної поліції (Інтерпол) та ін.). Це ж стосується і міждержавної взаємодії у виконанні правоохоронних органів із уповноваженими інституціями іноземних держав. Така діяльність має виключне значення навіть у нинішніх умовах, зважаючи на прогресування власне явища економічної злочинності [339, с. 251-252]. До того ж факти скоєння правопорушень, у тому числі проти основ національної безпеки, свідчать про нагальну потребу розвитку таких мір.

Із приводу наглядових і контролюючих заходів, то, керуючись нинішніми реаліями, першочергової уваги заслуговують робота Грошово-кредитного управління Сінгапуру (MAS), Комісії з цінних паперів та бірж (SEC) (США), Дубайського фінансового центру (DIFC) (ОАЕ), Податкової служби США (IRS) (США), Регіонального регуляторного органу ADGM (ОАЕ), Управління нагляду за операціями фінансового ринку Швейцарії (FINMA), Фінансового наглядового органу (FCA) (Велика Британія), Фінансової служби Японії (FSA) та ін. Напрацьовані практики останніх матимуть вагоме значення для розбудови комплексного й збалансованого адміністративно-правового забезпечення досліджуваної сфери суспільних відносин.

Пропоновані ініціативи мають забезпечити комплексну розбудову цифрового безпекового середовища на національних теренах, паралельно нарощуючи потенціал цифрової економіки. Окреслені позиції повинні гармонійно доповнити загальну політику розбудови такого типу економічних відносин, убезпечивши багато галузей суспільного виробництв від дії низки нетипових подразників. Стрімкий багатовекторний розвиток цифровізації і значне масштабування сфер її впливу по-новому змушують дивитися на це питання, відносячи його до розряду загальнообов'язкових.

Висновки до розділу 3

1. Міжнародна спільнота вийшла на новий рівень розбудови уніфікованих підходів регламентації відносин, що виникають під час обороту багатьох типів цифрових активів. Починаючи від дійсного усвідомлення руйнівного для економіки й багатьох інших сфер потенціалу цифрових засобів ураження і завершуючи затвердженням Регламенту МіСА, було предметно опрацьовано ряд системоутворюючих питань.

У той же час, проблематика загроз від операцій із цифровими активами поки висвітлена фрагментарно й за рядом позицій перебуває в процесі становлення. Серед розкритих та об'єктивованих у різних нормативно-правових документах виділяються питання відмивання коштів, фінансування розповсюдження зброї масового знищення, спонсорування тероризму, кіберзагроз, технічні аспекти, фінансової стабільності, а також шахрайства. Проте кожна із цих позицій потребує подальшої змістовної розробки з огляду на нетиповий прогресивний і прогресуючий діапазон властивостей цифрових активів.

Провідні іноземні моделі щодо протидії таким загрозам, у переважній більшості, також перебувають на зародкових стадіях. Виняток складають деякі держави (Велика Британія, ОАЕ, Сінгапур, США, Японія та ін.), котрі в силу різних індивідуальних обставин випереджають інших за цим параметром. У той же час спостерігається тенденція до розуміння потреби комплексної розробки саме цього напрямку. Серед найпоширеніших загроз від операцій із цифровими активами виділяються наступні: 1) відсутність комплексного правового забезпечення; 2) кіберзагрози; 3) легалізація (відмивання) доходів, отриманих протиправним шляхом; 4) недостатня дослідженість таких засобів і їхнє стрімке прогресування за різними характеристиками; 5) шахрайство; 6) інші чинники, явища, а також тенденції.

Для України, яка стійко декларує проєвропейські наміри, важливим залишається питання урахування на тероретико-методологічному, методичному

й правотворчому рівнях такого спрямування безпекових новацій. Тим паче, що підсумки від таких операцій із цифровими активами є однотипними і, часто, не мають територіальних обмежень. Відповідно, уваги заслуговують тамтешні підходи й результати відповідних заходів (управлінських, організаційних, правових, економічних, технічних тощо). Тому серед механізмів, вартих уваги з позиції розгляду й аналізу на предмет імплементації, заслуговують такі питання: 1) недостатня дослідженість відповідних засобів; 2) кіберзагрози; 3) легалізація (відмивання) доходів, отриманих протиправним шляхом; 4) розробка комплексного правового забезпечення; 5) шахрайство; 6) інші чинники, явища, у тому числі – дотичні до такої проблематики.

2. Ураховуючи потенціал лише відомих людству цифрових активів та оцінюючи його імовірний реалістичний руйнівний вплив на систему економічної безпеки України, виникає об'єктивна необхідність формування дієвих механізмів реагування на відповідні подразники. Новизна, багатогранність, складність і маловідомість багатьох технічних можливостей цих засобів спонукає першочергово окреслити провідні вектори розбудови комплексного адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами.

Вихідною точкою у пропонованій парадигмі є питання розробки «дорожньої карти» для чіткої, збалансованої та послідовної державної правової політики в цій сфері. Зазначений підхід забезпечить рух по оптимальній траєкторії та мінімізує прийняття стратегічно невиправданих управлінських рішень. На додаток до цього, указане сприятиме розробці дієвих механізмів, що гармонійно доповнять існуючі безпекові засади за такими і суміжними напрямками. До числа пріоритетних напрямів для розбудови комплексного адміністративно-правового регулювання з протидії аналізованим слід віднести такі заходи у відповідній послідовності: 1) розробка сприятливого теоретико-методологічного та методичного підґрунтя; 2) формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів

реагування на чинники, явища та тенденції цифрового походження; 3) вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів) шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу (формування збалансованих адміністративно-правових засад, чіткого визначення рівнів і напрямів функціонального впливу, поглиблення взаємодії, оптимізація контролю та нагляду, підвищення ефективності запобігання й протидії проявам економічної злочинності із використанням функціоналу цифрових засобів ураження).

3. Окреслені шляхи реалізації засадничих напрямів, у рамках ініційованої дорожньої карти, мають забезпечити поміркований перехідний період від дійсного визнання більшістю суспільства загрозовості цифрових інновацій та технологій для економіки, до комплексної розбудови відповідного правового забезпечення. Вони покликані сформувати упорядковану траєкторію розвитку такого перспективного напрямку з подальшою його синхронізацією із наявними безпековими системами і механізмами.

Попри стратегічний рівень, за логікою законодавця, саме на ньому розробляються ключові прагнення щодо поступового і збалансованого посилення безпекового напрямку української держави. З огляду на такий підхід, належне планування й поетапна реалізація намічених цілей – основоположна передумова для розбудови сприятливого правового й організаційного забезпечення та інституційної основи. А враховуючи певні закріплені стратегічні підвалини, слушно розраховувати на конструктивний поступальний розвиток такого напрямку.

Виходячи з представлених і обґрунтованих напрямів, слід запропонувати конкретні шляхи власне їхньої реалізації. Пропонована постановка питання має бути репрезентована у наступному вигляді: 1) розробка сприятливого теоретико-методологічного та методичного підґрунтя: а) виконання комплексних типологічних досліджень суб'єктами, що компетенційно дотичні до аналізованої сфери, а також зацікавленими ЗВО; б) розробка механізмів

аудиту ефективності національної фінансової системи на предмет оцінки руйнівного впливу цифрових засобів та проведення однойменних заходів;

в) створення робочих груп за участю уповноважених суб'єктів публічно-правових відносин, а також представників вітчизняної й іноземної фахової громадськості для висвітлення та аналізу проблемних питань у цій сфері;

г) посилення різних, у тому числі неправових форм взаємодії суб'єктів правоохоронної діяльності;

2) формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів реагування на чинники, явища та тенденції цифрового походження:

а) акумуляція результатів типологічних досліджень, підсумків аудиту ефективності національної фінансової системи, підсумків дискусій, у рамках міжвідомчого аналізу проблемних питань, пропозицій і висновків комітетів Верховної Ради України;

б) формування базису для розробки проєктів законів та інших нормативно-правових актів;

в) прийняття (затвердження) актів законодавства, забезпечуючи подальший розвиток системи економічної безпеки України та розробку нових і удосконалення існуючих механізмів реагування на відповідні подразники;

3) вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів) шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу:

а) на базі сформованого юридичного підґрунтя предметно опрацювати питання щодо посилення адміністративно-правового становища суб'єктів зі спеціальною компетенцією та деяких інших установ з метою приведення у чітку відповідність завдань і функцій таких органів орієнтирам системі економічної безпеки України;

б) всебічне і повне вивчення міжнародних стандартів та моделей, а також практик іноземних держав;

в) розробка пропозицій і рекомендацій щодо внесення змін до чинного законодавства, формуючи комплексне і збалансоване адміністративно-правове забезпечення вказаної сфери.

ВИСНОВКИ

У представленій широкому загалу дисертації на основі узагальнення досліджень провідних іноземних і вітчизняних учених, норм міжнародного права, національного й іноземного законодавств, документів рекомендаційного характеру, практик їх застосування, проєктів, а також різного типу аналітичних матеріалів (звітів, інформаційних довідок, пояснювальних записок, роз'яснень, тлумачень тощо) розроблено наукові положення, орієнтовані на розв'язання перспективної наукової проблеми – формування сприятливого теоретико-методологічного, методичного та правового підґрунтя для розбудови комплексного й збалансованого адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами.

За результатами проведеного дисертаційного дослідження було сформовано й обґрунтовано низку фундаментальних положень у формі пропозицій та рекомендацій. До основних із їхнього числа слушно віднести наступні.

1. Досліджено категорію «система економічної безпеки України» крізь призму об'єкта публічно-правового забезпечення. Установлено, що, будучи приналежною до системи вищого рівня (національна безпека України), вона потребує стійкої й ефективної підтримки з боку держави і суспільства. Це пояснюється її винятковою роллю у воєнний період, а також прогресуючим діапазоном викликів, загроз і ризиків елементам останній, у тому числі цифрового походження.

Точка зору про важливість підтверджується тим, що на сучасному етапі її слід розглядати як багатоаспектну складну соціальну систему, яка включає в себе численний неоднорідний елементний склад, сполучений широким спектром зв'язків та орієнтовану на постійну ефективну й результативну реалізацію заходів за такими напрямками: 1) збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з

боку більшості викликів, загроз та ризиків останній; 2) забезпечення здатності конкурентоспроможності лівової частки вітчизняних економічних галузей у світі; 3) сприяння поступальному розвитку всього економічного сектора. Її властивий наступний спектр характеристик: 1) взаємозалежність із багатьма іншими системами, насамперед безпековими (вищого, рівнозначного і нижчого рівнів); 2) взаємозалежність із навколишнім середовищем, політичною кон'юнктурою, геополітичними і геоекономічними процесами й іншими факторами; 4) динамічність функціонування; 5) емерджентність; 6) ієрархічність; 7) синергетичність; 8) сталість базових мети і завдань; 9) функціональність; 10) цілісність. До числа ознак слід віднести такі позиції: 1) багатоаспектність; 2) наявність структури з численним неоднорідним елементним складом, сполученим широким спектром зв'язків; 3) підпорядкованість системі вищого рівня (національній безпеці України); 4) предметний орієнтир на: а) збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній; б) забезпечення здатності конкурентоспроможності лівової частки вітчизняних економічних галузей у світі; в) сприяння поступальному розвитку всього економічного сектора; 5) соціальна система; 6) спрямованість на ефективне й результативне функціонування.

Метою функціонування системи економічної безпеки України є перелік офіційно закріплених орієнтирів щодо збереження стійкості національної економіки відносно поточного або перспективного деструктивного впливу з боку більшості викликів, загроз та ризиків останній, забезпечення здатності до конкурентоспроможності вітчизняних економічних галузей у світі, а також сприяння поступальному розвитку всього національного економічного сектору. Її завданнями є спектр об'єктивованих у нормативно-правових актах і стратегічних документах установок, практична реалізація заходів, по яких, має забезпечити досягнення мети.

Структура системи економічної безпеки України є обов'язковим

атрибутом, що передбачає розташування елементів у певному порядку, які діють (функціонують) за встановленими алгоритмами й поєднані спільними зв'язками. Її елементний склад налічує такі позиції: 1) об'єкти безпеки (національні економічні інтереси України); 2) суб'єкти із забезпечення безпеки; 3) правові засади, на основі яких формується відповідна система і функціонують її механізми; 4) елементи суміжних систем вищого рівня, рівнозначних систем, а також підсистеми системи економічної безпеки України (виробнича, енергетична, інвестиційно-інноваційна, продовольча, фінансова та ін.).

2. Здійснено теоретико-правову характеристику цифрових активів, зокрема сформульовано поняття останніх під декількома кутами зору, а саме: 1) блага з унікальними ідентифікаційними (буквено-числовими) кодами, що існують у цифровій формі й перебувають в обороті виключно у цифровому середовищі, мають цінність і вартісну визначеність у платіжній, інших матеріальних і нематеріальних формах та можуть використовуватися необмежним колом осіб; 2) широкий, непрогнозовано змінний спектр типів об'єктів нематеріального змісту, що існують у цифровій формі й обертаються в цифровому середовищі; 3) прояв прав власності (володіння, користування, розпорядження), що передбачають оперування об'єктами нематеріального змісту в цифровому середовищі, у тому числі – переважно безперешкодного доступу до них, незалежно від волі інших учасників відносин, зокрема й держави та суб'єктів міжнародного права; 4) у залежності від намірів, різновидів засобів і способів підвищення або зниження рівня ефективності функціонування установ, підприємств, організацій та діяльності суспільства.

Також визначено властивості цих активів, запропоновано наступний перелік: 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 деяких існуючих активів, генеруючи нові способи їх застосування та

засоби реалізації; 6) конкурентоздатність; 7) подекуди радикальний вплив на характер і темпи перебігу багатьох економічних процесів; 8) схильність до непрогнозованих радикальних трансформацій деяких форм. Ознаками такої категорії слід вважати наступні: 1) використання необмеженим колом осіб; 2) вираз майнових прав; 3) існування у цифровій формі та обертання в цифровому середовищі; 4) засоби і способи обороту, у тому числі – фактично шляхом здійснення платежів на території України, обміну на майно (товари), роботи (послуги) тощо; 5) наявність унікального ідентифікаційного (буквено-числового) коду; 6) незалежність від наслідків впливу лівової частки заходів під егідою процесів різного рівня (міжнародного, міждержавного, національного, регіонального, місцевого, локального) та характеру (геополітичних, гео економічних, економічних, політичних, правових, соціальних, технічних, технологічних та ін.); 7) об'єкти права власності; 8) сукупність благ.

Проблематика форм цифрових активів перебуває в процесі активного розвитку, що зумовлено новизною, складністю і малодослідженістю цього явища, а також різними підходами правових політик у іноземних країнах. Ураховуючи безпрецедентний потенціал таких засобів на тлі появи багатьох інновацій і технологій, а також спроб представників світової спільності упорядкувати окреслену сферу, варто розраховувати на швидку появу нових класифікацій та критеріїв градації відповідних типів (форм прояву).

На основі цього також доведено, що їхній подальший розвиток і активне масштабування є безальтернативним із огляду на потенціал цифрових технологій та інновацій. Їх прогресування матиме різний ефект для багатьох сфер і ланок вітчизняної економіки, При цьому ігнорування таких здобутків є хибною стратегією з огляду й на істотні функціональні переваги багатьох цифрових інструментів. Тому, попри певні ризики, упровадження частини з їх числа – необхідність, продиктована складними конкурентними умовами сьогодення.

3. Визначено поняття загроз системі економічної безпеки України як

тенденцій, чинників і явищ, котрі як індивідуально, так і сукупно унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію основних національних економічних інтересів України. До властивостей таких загроз доцільно віднести наступні позиції: 1) адаптивність (трансформація) до різних змін; 2) активна й, подекуди, стрімко прогресуюча конгломерація з іншими чинниками та явищами; 3) висока ймовірність ураження об'єктів деструктивного впливу; 4) істотний вплив на формування багатьох тенденцій у цій сфері; 5) залежність від супутніх факторів (геополітичних, геоekonomічних, політичних, правових, економічних, соціальних, технічних, технологічних тощо); 6) один із вагомих каталізаторів для появи нових і посилення дії існуючих викликів, загроз та ризиків для суміжних підсистем національної безпеки України; 7) різні темпи стійкої реалізації руйнівних намірів; 8) спрямованість на ключові національні економічні інтереси України; 9) часта латентність; 10) шкідливість. Ознаками загроз системі економічної безпеки України є: 1) визнання на офіційному рівні; 2) конституційне закріплення таких загроз як одних із пріоритетних, що впливає із ролі економічної безпеки; 3) спектр тенденцій, чинників і явищ, котрі, здебільшого, орієнтовані на одне коло типів національних інтересів України з подальшою диференціацією щодо похідних безпекових систем (виробничої, демографічної, енергетичної, зовнішньоекономічної, інвестиційно-інноваційної, макроекономічної, продовольчої, соціальної та фінансової); 4) участь держави, суспільства й кожної людини в запобіганні та протидії різним їх проявам.

У питанні класифікації загроз за основу взято існуючий державницький підхід, об'єктивований у стратегічних засадах економічної безпекової політики. Водночас доведено необхідність перегляду визнаного спектра тенденцій, чинників та явищ у зв'язку появою й стійким прогресуванням деяких загроз економічній складовій.

Із-поміж числа таких факторів виділяється цифрова складова, деструктивна роль якої невпинно зростає. На сучасному етапі узагальнено їх

варто розцінювати як чинники та явища цифрового походження, котрі унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію основних національних економічних інтересів України, таких, як сталість розвитку національної економіки, інтеграцію країни в європейський економічний простір, поглиблення рівноправного взаємовигідного економічного співробітництва з іншими державами. Загального розуміння останніх достатньо для усвідомлення істотного впливу на різні сфери економічної діяльності у середньо- та довгостроковій перспективах із позицій форм прояву, ступеня складності, потенційної міри ураження, взаємозв'язків із іншими методами економічної деструкції тощо.

Відповідно, окрім істотних переваг, такі засоби можуть деструктивно відобразитися на багатьох економічних аспектах, у різні способи руйнуючи структури останніх та продукуючи багато несприятливих тенденцій. Тому виникає потреба дотримання балансу між необхідністю упровадженням цифрових технологій й інновацій та уникнення ризикових інструментів відповідного спрямування. Окрім того, не втрачає гостроти питання мимовільної інтеграції вказаних засобів, а також неконтрольованого руйнівного впливу в різних сферах економічних відносин. Попри їх недостатню розробленість на теоретико-методологічному рівні окремі прецедентні й інші випадки засвідчують факти руйнівного впливу на процеси з виробництва, розподілу, перерозподілу, обміну товарів і послуг.

4. Розкрито тематику виняткової важливості міжнародних та іноземних стандартів і правових механізмів із протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами та оцінено їх вплив на результати національної правотворчості. Зокрема, підкреслено й доведено визначальну роль таких вихідних положень у питаннях розбудови цифрових середовищ та закладенні підвалин із протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами, та оцінено їхній вплив на результати національної правотворчості. З'ясовано, що деякі засадничі підходи й практики були імplementовані до вітчизняної законодавчої бази відносно

питань обороту окремих форм цифрових, запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення тощо.

Наголошено й аргументовано необхідність подальшого врахування таких цілей і орієнтирів із огляду на євроінтеграційні прагнення українського народу, усвідомлення потреби стійкої консолідації зусиль у міжнародному та міждержавному вимірах, а також ураховуючи нетипову природу цифрових активів. Винятковість цієї позиції обумовлена затвердженням Керівництва FATF з ризик-орієнтованого підходу віртуальні активи та постачальники послуг із переказу віртуальних активів від 2019 року, Регламенту MiCA й деяких інших документів, котрі носять наднаціональний характер і покликані стандартизувати відповідні механізми та практики. Відповідно, гармонізація із такими механізмами має позитивно відобразитися на поступовій розбудові ефективного комплексного адміністративно-правового забезпечення з протидії відповідним загрозам в Україні.

Виходячи із розуміння складності такої проблематики, стандарти суб'єктів міжнародного права й деяких іноземних держав варті уваги з позиції закладення сприятливих основ для розбудови цієї сфери. Урахування тамтешніх підходів до засад відповідних систем і механізмів – запорука формування ефективного національного правового забезпечення. Це матиме вагоме значення із точки зору консолідації зусиль у питанні результативного реагування на такі й суміжні чинники, явища і тенденції. Мова йде не лише про сформовані цифрові засоби ураження, а й первинні інструменти та процеси, що спонукають та (або) сприяють відповідним проявам деструкції.

5. Окреслено й класифіковано адміністративно-правові засади з протидії загрозам системі економічної безпеки України, що виникають при проведенні операцій із цифровими активами. Установлено, що такі основи являють собою сукупність норм адміністративного права, об'єктивованих у нормативно-правових актах різної юридичної сили, які визначають мету, завдання, принципи, функції й інші адміністративно-правові способи та засоби,

за допомогою яких здійснюється регулювання предметної сфери відносин.

Зважаючи на те, що всі такі засади закріплюються актами законодавства, їх окреслення має відбуватися шляхом визначення відповідних джерел права з наступною класифікацією. Відповідно, названа градація має такий вигляд: 1) Конституція України; 2) міжнародні договори України (Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом від 8 листопада 1990 року, Угода про асоціацію між Україною та ЄС від 27 червня 2014 року, Рекомендації Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року, Керівництво FATF, Регламент МіСА та інші акти); 3) закони («Про національну безпеку України», «Про віртуальні активи», «Про цифровий контент та цифрові послуги», «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про оперативно-розшукову діяльність», «Про стимулювання розвитку цифрової економіки в Україні», а також Кримінальний кодекс України, Кримінальний процесуальний кодекс України та ін.); 3) підзаконні нормативно-правові акти (Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» від 14 вересня 2020 року, Указ Президента України «Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року» від 11 серпня 2021 року, Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 14 травня 2021 року та ін.).

Зауважено й доведено, що такі засади на сучасному етапі державотворення не забезпечують комплексну протидію відповідним проявам деструкції, що, окрім загроз, породжує і певні ризики для всього безпекового сектора. Їхня епізодичність і обмеженість формує сприятливе підґрунтя для

появи й розвитку відповідних способів деструкції економічних відносин. Ті можуть запустити ланцюгові реакції для продукування нових шляхів і засобів цифрового руйнування економіки. У результаті чого слушно розраховувати на появу нових маловідомих загрозованих трансформацій із непрогнозованими траєкторіями розвитку та ступенем складності наслідків.

6. Проаналізовано адміністративно-правовий статус суб'єктів системи економічної безпеки України зі спеціальною компетенцією, що протидіють загрозам, які виникають при здійсненні операцій із цифровими активами. З'ясовано й доведено, що під таким статусом слід розуміти компетенцію (повноваження, права, обов'язки) та інші атрибути, визначені нормами адміністративного права, що сукупно окреслюють їхнє місце й визначають роль на всіх рівнях та за напрямками функціонального впливу.

Запропоновано класифікацію таких суб'єктів із градацією на дві групи на основі критерію меж компетенції установ (загальна та спеціальна). До носіїв загальної компетенції віднесено наступні суб'єкти: 1) Верховна Рада України; 2) Президент України та Рада національної безпеки і оборони України; 3) Кабінет Міністрів України, Міністерство економіки України, Міністерство фінансів України та інші центральні органи виконавчої влади; 4) суди (місцеві загальні суди, відповідні апеляційні суди, Верховний Суд (Касаційний кримінальний суд, Велика Палата Верховного Суду); 5) та ін. Перелік суб'єктів зі спеціальною компетенцією запропоновано представити у такому складі: 1) Міністерство цифрової трансформації України; 2) Міжнародна група з протидії відмивання брудних грошей; 3) Державна служба фінансового моніторингу України; 4) Національна комісія з цінних паперів та фондового ринку; 5) Національний банк України; 6) правоохоронні органи (Бюро економічної безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України, Національна поліція, Служба безпеки України).

Окреслено поточне адміністративно-правове становище суб'єктів зі спеціальною компетенцією крізь призму рівнів і напрямів функціонального впливу. Встановлено і доведено, що функціонування таких установ особливо

вирізняється на міжнародному і міждержавному, а також національному рівнях. У той же час для Міжнародної групи з протидії відмивання брудних грошей переважає міжнародний і міждержавний рівні. Тоді, як для решти суб'єктів зі спеціальною компетенцією, має перевагу національний рівень.

Визначено та охарактеризовано напрями роботи таких інституцій щодо предметної сфери. Перспективною бачиться наступна диференціація:

- 1) Міністерство цифрової трансформації України: а) формування та реалізація державної політики у сферах цифровізації, цифрових інновацій і технологій, цифрової економіки й цифрового розвитку; б) здійснення державного регулювання і нагляду у сфері запобігання та протидії легалізації (відмиванню) злочинних доходів, одержаних шляхом фінансування тероризму та фінансування розповсюдження зброї масового знищення відносно постачальників послуг, пов'язаних з оборотом віртуальних активів (форм цифрових активів);
- 2) Міжнародна група з протидії відмивання брудних грошей: а) поширення відомостей стосовно заходів боротьби з відмиванням коштів у світі; б) моніторинг за неухильною реалізацією базових рекомендацій установи; в) огляд тенденцій, присвячених питанням відмивання коштів і реалізації відповідних контрзаходів (типологічні дослідження);
- 3) Державна служба фінансового моніторингу України – реалізація державної політики з питань запобігання і протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення за допомогою окремих форм цифрових активів;
- 4) Національна комісія з цінних паперів та фондового ринку – формування й забезпечення реалізації державної політики відносно: а) розвитку і функціонування ринку віртуальних активів; б) сприяння адаптації відповідного законодавства до міжнародних стандартів;
- 5) Національний банк України – реалізація державної політики виключно щодо ЗВА (ВЦ); б) правоохоронні органи (Бюро економічної безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України, Національна поліція, Служба безпеки України) – здійснення правоохоронної діяльності стосовно

відповідних протиправних діянь.

Зважаючи на недосконалість адміністративно-правового забезпечення досліджуваної сфери відносин, питання поточного відповідного становища більшості представлених установ також заслуговує уваги. Обмежений, виходячи з цілей і завдань інституцій, функціонал за підвідомчими рівнями та напрямками функціонального впливу спонукає до удосконалення їхнього адміністративно-правового статусу. Наявне юридичне підґрунтя істотно послаблює потенціал таких суб'єктів, адже йдеться про можливість регулювання відносин усіченого кола критичних і приналежних до цієї області процесів. Відповідно, посилення становища установ з урахуванням новітніх управлінських підходів і практик – безумовна і нагальна потреба сьогодення.

7. Розкрито сутність адміністративно-правового механізму взаємодії суб'єктів зі спеціальною компетенцією з протидії загрозам системи економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами. Відповідну діяльність запропоновано розглядати під такими кутами зору: 1) разове, тривале чи системне вжиття спільних заходів відповідними суб'єктами системи економічної безпеки України з метою протидії загрозам, що можуть виникати внаслідок операцій із цифровими активами, шляхом реалізації управлінських форм і методів та у способи, що не суперечать нормам чинного законодавства; 2) санкціонований вплив одного суб'єкта на інший (чи декількох) з ціллю приведення у відповідність нормам законів і підзаконних нормативно-правових актів заходів, у тому числі недопущення зловживань із питань протидії аналізованим чинникам, явищам, а також тенденціям. Ознаками такого механізму слід вважати наступні: 1) важливе значення міжнародних стандартів у цій сфері; 2) сукупність груп регульованих процедур спільного характеру; 3) участь двох і більше суб'єктів; 4) разовість, тривалість або системність ужиття таких мір; 5) спрямованість на розбудову безпечного цифрового середовища з урахуванням технічних і технологічних новацій та орієнтиром на відомі виклики й ризики осяжного майбутнього; 6) провадження спільних заходів, які не суперечать приписам чинного законодавства;

7) існування форм і методів реалізації таких кроків; 8) наявність визначеними нормами адміністративного права спектру засобів та способів здійснення колективних мір.

Установлено, що метою такої взаємодії є своєчасне і повноцінне досягнення задекларованих державою намірів у предметній сфері шляхом оптимальної консолідації наявного інтелектуального, матеріально-технічного й іншого ресурсного забезпечення та раціонального застосування форм і методів діяльності останніх. Доведено, що завданнями висвітлених спільних заходів є спектри самостійних персоналізованих нормативно допустимих настанов, виконання котрих – прерогатива певного кола учасників відповідних спільних заходів.

Стосовно правозастосовного аспекту, то Міністерство цифрової трансформації України здійснює побічний вплив на контури заходів у виконанні Державної служби фінансового моніторингу України та Національної комісії з цінних паперів та фондового ринку. Представники Міжнародної групи з протидії відмивання брудних грошей активно й стійко співпрацюють із Державною службою фінансового моніторингу України і правоохоронними органами. Слушно вести мову про побічний вплив на деякі напрями роботи Міністерства цифрової трансформації України, Національної комісії з цінних паперів та фондового ринку й Національного банку України. При цьому Національна комісія з цінних паперів та фондового ринку і Національний банк України взаємодіють між собою щодо ряду питань, пов'язаних із оборотом певних форм цифрових активів. Суб'єкти правоохоронної діяльності активно співробітничать між собою у рамках досудового розслідування й здійснення оперативно-розшукових заходів та інших, у тому числі неправових, форм діяльності.

Обмеженість компетенції розглянутих установ особливо негативно відображається на питаннях взаємодії щодо аналізованих, вихідних та похідних векторів. Із огляду на транснаціоналізацію, стрімкий розвиток і динамічне масштабування відповідних чинників та явищ, а також тенденцій цей аспект

має надважливе значення. Їх виключна роль пояснюється і можливістю посилення заходів із протидії й запобігання впливу останніх, насамперед із позиції превенції. Ураховуючи беззаперечний істотний потенціал цифрових засобів ураження, саме запобігання останнім є одним і перспективних та виправданих кроків.

8. Опрацьовано питання правової регламентації здійснення державного контролю та нагляду при проведенні операцій із цифровими активами. З'ясовано, що йдеться про не тотожні, але взаємодоповнюючі знакові інструменти адміністративно-правового регулювання предметної сфери. Установлено, що нагляд не передбачає будь-яких форм фізичного втручання у діяльність об'єкта впливу та провадиться на постійній основі для підтримки правопорядку з питань обороту легалізованих типів цифрових активів. Натомість, контроль має на увазі призупинення всіх чи частки процесів із метою виявлення і встановлення порушень законодавства, співставлення очікуваних результатів дійсним підсумкам та з'ясування інших невідповідностей під час реалізації заходів щодо обігу таких активів.

Наголошено, що такі заходи є важливими з точки зору превенції від руйнівного ефекту багатьох загроз системі економічної безпеки України цифрового походження. Підтверджено: належний застосунок відповідних механізмів, окрім профілактичних кроків, може також сприяти виявленню прогалин, колізій й решти недоопрацьовань.

Серед досліджуваних суб'єктів зі спеціальною компетенцією, окрім правоохоронних органів, інші провадять контролюючі й наглядові заходи. Так, зокрема: 1) Міністерство цифрової трансформації України: а) нагляд із питань: запобігання й протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення відносно постачальників послуг, пов'язаних з обігом віртуальних активів; за формуванням та виконанням Національної програми інформатизації; б) контроль із питань: виконання власної державної політики підвідомчими установами; відповідність заявників та резидентів Дія Сіті

законодавчим вимогам для набуття і наявності однойменного правового статусу; формуванням та виконанням Національної програми інформатизації; виконання власних наказів тощо; 2) Міжнародна група з протидії відмивання брудних грошей: нагляд із питань: поширення відомостей стосовно заходів боротьби з відмиванням грошей на всіх континентах і в усіх світових регіонах; моніторинг за неухильною реалізацією рекомендацій установи у країнах-членах FATF; тенденціями, присвяченими питанням відмивання коштів і реалізації відповідних контрзаходів; 3) Державна служба фінансового моніторингу України: контроль із питань: виконанням виданих наказів за діяльністю учасників, суб'єктів фінансового моніторингу; 4) Національна комісія з цінних паперів та фондового ринку й Національний банк України – нагляд і контроль за дотриманням учасниками відповідних ринків законодавства у підвідомчих сферах. Однак, попри таку компетенцію, існуючі законодавчі неврегульованості істотно обмежують відповідний функціонал установ, тим самим формуючи сприятливе підґрунтя для появи й розвитку деструктивних чинників, явищ і тенденцій в економіці.

Із точки зору адміністративно-правового регулювання досліджуваної сфери відносин вагоме значення відведено контрольним і наглядовим заходам. Доповнюючи взаємодію, при належних адміністративно-правових засадах, вони сприяють мінімізації неправомірних діянь, у тому числі – з позиції профілактики та сприяють уникненню багатьох відхилень під час функціонування низки систем.

Однак нинішній стан правового регулювання щодо здійснення вказаних заходів помітно звужує, а також обмежує аналізований функціонал. Із огляду на це виникає нагальна й обґрунтована потреба розробки та впровадження відповідних змін до законодавства.

9. Здійснено огляд та компаративний аналіз міжнародних і провідних закордонних моделей щодо протидії загрозам, які можуть виникати внаслідок операцій із цифровими активами. Наголошено, що міжнародна спільнота вийшла на новий рівень розбудови уніфікованих підходів щодо регламентації

відносин, які виникають під час обороту деяких типів цифрових активів (Керівництво FATF, Регламент MiCA, Рекомендації Європейського управління з цінних паперів і ринків (ESMA) від 9 січня 2019 року та ін.). У той же час проблематика загроз від операцій із цифровими активами поки висвітлена фрагментарно й за рядом позицій перебуває в процесі становлення. Серед розкритих та об'єктивованих у різних документах виділяються наступні питання: 1) відмивання коштів, фінансування розповсюдження зброї масового знищення, спонсорування тероризму; 2) кіберзагрози; 3) технічні аспекти; 4) фінансова стабільність; 5) шахрайство 6) тощо.

Виявлено, що на рівні країн поступово цей вектор предметно опрацьовують Багамські Острови, Бермудські Острови, Велика Британія, Канада, Китай, ОАЕ, Сінгапур, США, Франція, Швейцарія, Японія. Деякі вагомні зрушення з позиції правотворчості і правозастосування можна прослідувати у практиках Великої Британії, ОАЕ, Сінгапуру, США та Японії. Серед найпоширеніших загроз від операцій із цифровими активами виділяються такі: 1) відсутність комплексного правового забезпечення; 2) кіберзагрози; 3) легалізація (відмивання) доходів, отриманих протиправним шляхом; 4) недостатня дослідженість таких засобів і їхнє стрімке прогресування за різними характеристиками; 5) шахрайство; 6) інші чинники, явища, а також тенденції.

Відмічено кореляцію більшості зароджуваних безпекових орієнтирів на міжнародному й національному рівні в розрізі згаданих держав. Підкреслено виключну значимість транснаціональності аналізованих загроз, стійкого масштабування та розширення функціоналу, чим власне і аргументується подібність загрозливих факторів. Акцентується увага на суттєвих правових зрушеннях із позиції безпеки часткою таких країн (Велика Британія, ОАЕ, Сінгапур, США та Японія).

Результати, отримані під час вирішення завдань у попередніх розділах, засвідчили необхідність поступальної й невпинної розбудови відповідного безпекового напрямку. Взірцевими орієнтирами під час таких тривалих і

комплексних трансформацій є міжнародні й іноземні політики з огляду одноманітності потенційних та існуючих питань. Це також пояснюється критичним станом багатьох економічних показників та визнаною потребою консолідації зусиль задля ефективного реагування на деструктивні новації цифрового середовища. Серед механізмів, вартих уваги з позиції розгляду й аналізу на предмет імплементації, доцільно сфокусувати увагу щодо наступних позицій: 1) недостатня дослідженість відповідних засобів; 2) кіберзагрози; 3) легалізація (відмивання) доходів, отриманих протиправним шляхом; 4) розробка комплексного правового забезпечення; 5) шахрайство; 6) інші чинники, явища, у тому числі дотичні до такої проблематики.

10. Окреслено першочергові вектори для розбудови комплексного адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати при проведенні операцій із цифровими активами. Зауважено, що, беручи до уваги ступінь розробки тематики і зважаючи на епізодичність поточного забезпечення, сфокусовано увагу щодо засадничих аспектів, які потребують об'єктивізації у джерелах права.

На основі авторитетних рейтингів оцінено стан реалізації ключового концептуального документа щодо розвитку цифрової економіки. У ході такого відпрацювання, було доведено факт неефективної реалізації більшості намірів чи недосягнення деяких цілей загалом. Висловлено мотивовану гіпотезу, що однією з істотних причин такого стану є ігнорування проблем безпекового спрямування, а також відсутності оптимальної траєкторії для реалізації державної політики в окресленій сфері.

До числа пріоритетних напрямів для розбудови комплексного адміністративно-правового регулювання з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами, слід віднести такі заходи у відповідній послідовності: 1) розробка сприятливого теоретико-методологічного та методичного підґрунтя; 2) формування юридичних основ для подальшої розбудови системи

економічної безпеки України і механізмів реагування на чинники, явища та тенденції цифрового походження; 3) вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів) шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу (формування збалансованих адміністративно-правових засад, чіткого визначення рівнів і напрямів функціонального впливу, поглиблення взаємодії, оптимізація контролю та нагляду, підвищення ефективності запобігання й протидії проявам економічної злочинності із використанням функціоналу цифрових засобів ураження).

Невпинний рух саме за пропонованою траєкторією має забезпечити дійсне вирішення розкритої в дослідженні центральної проблеми, яка схильна до стрімкого прогресування. Особливу важливість вона має для України, яка, із одного боку, вирізняється виснаженою й уразливою економікою, а з іншого – фактично відсутністю ефективного адміністративно-правового забезпечення та слабо розвиненого технічного функціоналу. Ініційована дорожня карта має закласти перспективні основи для нарощування безпекового потенціалу за відповідним напрямом наукового інтересу. До того ж вона покликана акумулювати та скоординувати наявні прагнення й зусилля у питанні розробки та системного удосконалення засад стійкості держави до таких загроз.

11. Запропоновано й обґрунтовано доцільність шляхів реалізації напрямів формування комплексного адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами з урахуванням досвіду іноземних країн. Ураховуючи зміст і характер представлених вище орієнтирів, перспективною бачиться наступний діапазон послідовних кроків: 1) розробка сприятливого теоретико-методологічного та методичного підґрунтя: а) виконання комплексних типологічних досліджень суб'єктами, що компетенційно дотичні до аналізованої сфери, а також зацікавленими ЗВО; б) розробка механізмів аудиту ефективності національної фінансової системи

на предмет оцінки руйнівного впливу цифрових засобів та проведення однойменних заходів; в) створення робочих груп за участю уповноважених суб'єктів публічно-правових відносин, а також представників вітчизняної й іноземної фахової громадськості для висвітлення та аналізу проблемних питань у цій сфері; г) посилення різних, у тому числі неправових форм взаємодії суб'єктів правоохоронної діяльності; 2) формування юридичних основ для подальшої розбудови системи економічної безпеки України і механізмів реагування на чинники, явища та тенденції цифрового походження: а) акумуляція результатів типологічних досліджень, підсумків аудиту ефективності національної фінансової системи, підсумків дискусій, у рамках міжвідомчого аналізу проблемних питань, пропозицій і висновків комітетів Верховної Ради України; б) формування базису для розробки проєктів законів та інших нормативно-правових актів; в) прийняття (затвердження) актів законодавства, забезпечуючи подальший розвиток системи економічної безпеки України та розробку нових і удосконалення існуючих механізмів реагування на відповідні подразники; 3) вирішення питання щодо розмежування компетенції та посилення ролі більшості суб'єктів системи економічної безпеки України (персоніфікованих органів) шляхом окреслення чітких намірів із удосконалення їхнього адміністративно-правового статусу: а) на базі сформованого юридичного підґрунтя предметно опрацювати питання щодо посилення адміністративно-правового становища суб'єктів зі спеціальною компетенцією та деяких інших установ з метою приведення у чітку відповідність завдань і функцій таких органів орієнтирам системі економічної безпеки України; б) усебічне і повне вивчення міжнародних стандартів та моделей, а також практик іноземних держав; в) розробка пропозицій і рекомендацій щодо внесення змін до чинного законодавства, формуючи комплексне і збалансоване адміністративно-правове забезпечення вказаної сфери.

Пропоновані кроки мають забезпечити дійсну ефективну й результативну реалізацію всіх представлених напрямів, не тільки сформувавши, а й закріпивши траєкторію поступального розвитку вказаного напрямку з

подальшою об'єктивізацією відповідних механізмів у нормах законодавства, доповнюючи існуючі інструменти та синхронізуючись із рештою безпекових засад. Намір та ініціативи щодо уникнення декларативності мають спонукати до дійсного неупередженого і послідовного втілення в життя прагнення: утвердження нового безпекового вектору на теоретико-методологічному, методичному та правотворчому рівнях. Послідовний і стійкий рух усіх суб'єктів і учасників за репрезентованою алгоритмікою забезпечить отримання вагомих підсумків, слугуючи імпульсом для наступних розробок тематики під різними кутами зору (геоекономічними, геополітичними, політичними, економічними, правовими, управлінськими, технічними, технологічними та ін.). Відповідно, слушно вести мову про формування змістовного базису для подальших наукових розвідок на різних рівнях із репрезентованого й суміжних питань.

Наведені базові вектори мають закласти перспективні підвалини для подальшої комплексної розбудови відповідних систем і механізмів реагування, у тому числі запобігання й протидії. Адже із позиції конструктивізму так зване «цифрове десятиріччя» зумовлює необхідність істотного корегування багатьох існуючих правових підходів до регламентації суспільних відносин. Консервативність поглядів і статика наявного інструментарію – невідворотна передумова стагнації чи навіть руйнування багатьох економічних процесів, критично важливих для воюючої та фінансово залежної країни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
2. Про Стратегію національної безпеки України : Указ Президента України від 14 вересня 2020 р. № 392/2020 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/n0005525-20#Text>.
3. Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року» : Указ Президента України від 11 серпня 2021 р. № 347/2021 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/347/2021#Text>.
4. Гарькава В. Економічна безпека регіону: сутність поняття. *Східна Європа*. 2019. № 4 (21). С. 370–375.
5. Гарькава В. Стратегія забезпечення економічної безпеки України : дис. ... д-р екон. наук : 08.00.03. Київ. 2023. 489 с.
6. Гаруст Ю., Мельник В. Правоохоронні органи на захисті економічної безпеки України: адміністративно-правовий аспект: монографія. Суми : Видавничо-виробниче підприємство «Мрія». 2019. 256 с.
7. Harust, Yu., Melnyk, V. (2020). Law enforcement agencies on protection of economic security of Ukraine: administrative and legal aspect. Ottawa: *Accent Graphics Communications & Publishing*. 421 p.
8. Колеснікова К., Маліновська І., Чабаров В. Економічна безпека України в контексті глобалізаційних викликів. *Молодий вчений*. 2018. № 3. С. 351–354.
9. Повзун Д. Економічна безпека регіону як складова національної безпеки України. *Економіка та держава*. 2020. № 8. С. 89–94.
10. Утенкова К. Економічна безпека як складова національної безпеки

України. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Міжнародні відносини. Економіка. Країнознавство. Туризм.* 2019. Вип. 9. С. 133–144.

11. Утенкова К. Управління механізмом економічної безпеки аграрного сектора : дис. ... д-р екон. наук : 08.00.03. Київ. 2020. 560 с.

12. Горбулін В. Забезпечення оборони та безпеки України: актуальні проблеми і шляхи їх вирішення. *Вісник Національної академії наук України.* 2019. № 9. С. 3–18.

13. Горбулін В., Даник Ю. Національна безпека України: фокус пріоритетів в умовах пандемії. *Вісник Національної академії наук України.* 2020. № 5. С. 3–18.

14. Пономарьов С. Поняття та сутність сектору безпеки. *Право.ua.* 2015. № 3. С. 69–73.

15. Пономарьов С. Адміністративно-правове забезпечення діяльності сектору безпеки і оборони України : автореф. дис. ... д-р юрид. наук : 12.00.07. Харків. 2018. 34 с.

16. Пономарьов С. Адміністративно-правове забезпечення діяльності сектору безпеки і оборони України : дис. ... д-р юрид. наук : 12.00.07. Харків. 2018. 513 с.

17. Kim, R. Holmes (2015). What Is National Security? *The Heritage Foundation.* P. 17–26. [online] Available at: https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf.

18. Шлемко В., Білько І. Економічна безпека України: сутність і напрямки забезпечення : монографія. Київ : НІСД. 1997. 144 с.

19. Єрмошенко М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення : монографія. Київ : КНТЕУ. 2001. 309 с.

20. Єрмошенко М., Горячева К. Фінансова складова економічної безпеки: держава і підприємство : монографія. Національна академія управління. Київ :

НАУ. 2010. 232 с.

21. Жаліло Я. Стратегія національної безпеки України в контексті досвіду світової спільноти. Київ : Сатсанга. 2001. 224 с.

22. Жаліло Я. Теорія та практика формування ефективної економічної стратегії держави : монографія. Київ : НІСД. 2009. 334 с.

23. Кулінська А. Державне управління фінансовою складовою економічної безпеки національної економіки України : автореф. дис. ... д-р екон. наук : 08.00.03. Одеса. 2017. 44 с.

24. Кулінська А. Державне управління фінансовою складовою економічної безпеки національної економіки України : дис. ... д-р екон. наук : 08.00.03. Одеса. 2017. 531 с.

25. Machovski, H. (1985). Ost-West Handel: Entwicklung, Interessenlagen. Aussichten. *Aus Politik u. Zeitgeschichte*. № 5. P. 39–44.

26. Пастернак-Таранушенко Г. Результати дослідження шляхів забезпечення економічної безпеки України. *Економіка України*. 1999. № 2. С. 21–28.

27. Пастернак-Таранушенко Г. Економічна безпека держави. Київ : Інститут державного управління і самоврядування при Кабінеті Міністрів України. 1994. 140 с.

28. Пастернак-Таранушенко Г. Економічна безпека держави. Статика процесу забезпечення. Київ : Кондор. 2002. 302 с.

29. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.

30. Концепція економічної безпеки споживчої кооперації України : Концепція від 12 листопада 2008 р. // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/rada/show/n0007626-08#Text>.

31. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України : наказ Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 р. № 1277 // База даних «Законодавство

України». URL: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>.

32. Проект Закону про основи запобігання та боротьби з економічними правопорушеннями : Проект Закону України від 8 серпня 2014 р. № 4449а. Веб-портал: *Державна податкова служба України*. 2014. URL: <https://www.tax.gov.ua/diyalnist-/regulyatorna-politika-/regulyatorna-politika/arhiv/2014-rik/63287.html>.

33. Шайдаров О. Економічна безпека в системі національної безпеки. *Університетські наукові записки*. 2011. № 4 (40). С. 395–400.

34. Мамулай О. Основи економічної теорії : підручник. Київ : Юрінком Інтер. 2006. 479 с.

35. Ковч В. Задоволення потреб суспільства, як стратегічна функція держави в умовах формування інноваційної економіки. *Ефективна економіка*. 2014. № 7. URL: <http://www.economy.nayka.com.ua/?op=1&z=3181>.

36. Mochernyi, S. (2008). *Ekonomichna teoriia : navch. posibn. (3-Btie vyd)*. Kyiv : Akademiia. 640 p.

37. Степаненко А., Герасимов М. Оцінка економічної безпеки України та її регіонів. *Регіональна економіка*. 2002. № 2. С. 39–54.

38. Скорук О. Економічна безпека держави: сутність, складові елементи та проблеми забезпечення. *Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство*. 2016. Вип. 6 (3). С. 39–42.

39. Новікова О., Покотиленко Р. Економічна безпека: концептуальне визначення та механізм забезпечення : монографія. НАН України. Інститут економіки та промисловості. Донецьк. 2006. 408 с.

40. Крихтін Є. Соціальна політика та економічна безпека : монографія. Донецьк : Каштан. 2004. 336 с.

41. Пирожков С. Методичні рекомендації щодо оцінки рівня економічної безпеки України. Київ : НІПМБ. 2003. 42 с.

42. Про затвердження Методики розрахунку рівня економічної безпеки України : наказ Міністерства економіки України від 2 березня 2007 р. № 60 //

База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/rada/show/v0060665-07#Text> (втратив чинність).

43. Гуменюк А. Безпека структурно-інституціональної трансформації економіки регіону: теоретичні основи та прикладні аспекти : монографія. Київ : НІСД, 2014. 468 с.

44. Дацко О., Мокій А. Територіальна громада у системі економічної безпеки держави. *Стратегічні пріоритети*. 2015. № 1 (34). С. 83–89.

45. Дацко О. Забезпечення економічної безпеки України: соціально-гуманітарний вимір : дис. ... д-р екон. наук : 08.00.03. Львів. 2021. 636 с.

46. Завгородня С. Система державного управління економічною безпекою як об'єкт самостійних наукових досліджень. *Ефективність державного управління*. 2014. Вип. 41. С. 80–87.

47. Завгородня С. Система державного управління у сфері економічної безпеки України: теоретичний аспект : автореф. дис. ... канд. наук з держ. упр. : 25.00.01. Київ. 2016. 23 с.

48. Завгородня С. Система державного управління у сфері економічної безпеки України: теоретичний аспект : дис. ... канд. наук з держ. упр. : 25.00.01. Київ. 2016. 267 с.

49. Мельник В. Адміністративно-правова характеристика системи економічної безпеки України. *Порівняльно-аналітичне право*. 2020. № 1. С. 360–362.

50. Мельник В. Загальна характеристика структури системи економічної безпеки України. *Вісник Запорізького національного університету. Юридичні науки*. 2020. № 1. С. 155–159.

51. Мельник В. Адміністративно-правові засади організації та функціонування системи економічної безпеки України : монографія. Суми. ВВП «Мрія». 2020. 452 с.

52. Мельник В. Адміністративно-правові засади організації та функціонування системи економічної безпеки України : дис. ... д-р юрид. наук : 12.00.07. Суми. 2021. 485 с.

53. Морозюк Н. Сучасний стан економічної безпеки в кризових умовах. *Ефективна економіка*. 2015. № 3. URL: <http://www.economy.nauka.com.ua/?op=1&z=3884>.
54. Ревак І. Інтелектуальний потенціал у системі економічної безпеки України : автореф. дис. ... д-р екон. наук : 08.00.03 ; 21.04.01. Львів. 2016. 48 с.
55. Ревак І. Інтелектуальний потенціал у системі економічної безпеки України : дис. ... д-р екон. наук : 08.00.03 ; 21.04.01. Львів. 2016. 474 с.
56. Сазонов В. Поняття та система економічної безпеки: кримінологічний вимір. *Вісник Кримінологічної асоціації України*. 2019. Спец. вип. С. 97–105.
57. Сазонов В. Кримінологічне забезпечення економічної безпеки України : автореф. дис. ... д-р юрид. наук : 12.00.08. Харків. 2020. 32 с.
58. Сазонов В. Кримінологічне забезпечення економічної безпеки України : дис. ... д-р юрид. наук : 12.00.08. Харків. 2020. 416 с.
59. Сухонос В., Сухонос В., Сластьоненко О. Система економічної безпеки України: проблеми та перспективи у юридичному вимірі. *Ірпінський юридичний часопис*. 2023. Вип. 2 (11). С. 28–38.
60. Мельник В. Адміністративно-правові засади організації та функціонування системи економічної безпеки України : автореф. дис. ... д-р юрид. наук : 12.00.07. Суми. 2021. 46 с.
61. Кіяшко Ю. Поняття «системи економічної безпеки України»: адміністративно-правовий вимір. *Міжнародний науковий журнал «Інтернаука»*. Серія : «Юридичні науки». 2022. № 1. URL: <https://www.inter-nauka.com/ru/issues/law2022/1/7882>.
62. Додонов О., Путятін В., Куценко С., Ланде Д. Побудова узагальненої структури інформаційної системи організаційного управління. *Математичні машини і системи*. 2017. № 3. С. 6.
63. Заморська Л. Загальнонаукова концепція категорії «система права». *Держава і право*. 2010. Вип. 47. С. 46–50.
64. Делінський О. Проблеми безпеки української держави в сучасному конституціоналізмі. *Сучасний конституціоналізм та конституційна юстиція* :

матеріали Міжнародної науково-практичної конференції / За ред. С. В. Ківалова, М. П. Орзіха. Бібліотека журналу «Юридичний вісник». Одеса : Юридична література. 2001. С. 237–242.

65. Делінський О. Європейська система безпеки: міжнародно-правові аспекти становлення і розвитку : автореф. ... канд. юрид. наук : 12.00.11. Харків. 2003. 21 с.

66. Сухоруков А., Мошенський С., Петрук О. Національна економічна безпека : навч. посібн. Житомир : Рута. 2010. 384 с.

67. Сідлецька В. Економічна безпека як фактор прояву національних економічних інтересів України. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «Економіка»*. 2016. Вип. 16. С. 79–85.

68. Кіяшко Ю. До питання доцільності та методологічної обґрунтованості використання в науковому обігу категорії «система економічної безпеки України». *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : збірник наукових праць з матеріалами III Міжнародної наукової конференції (м. Дніпро, 6 вересня 2024 р.) Міжнародний центр наукових досліджень. Вінниця : ТОВ «УКРЛОГОС Груп. 2024. 180 с.

69. Податковий кодекс України : Закон України від 2 грудня 2010 р. № 2755-VI // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2755-17>.

70. Про віртуальні активи : Закон України від 17 лютого 2022 р. № 2074-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (набрання чинності з дня набрання чинності законом України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами).

71. Про цифровий контент та цифрові послуги : Закон України від 10 серпня 2023 р. № 3321-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3321-20#Text>.

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

73. 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. [online] Available at: https://www.americanbar.org/content/dam/aba/publications/real_property_trust_and_estate_law_journal/v52/01/rpte-journal-2017-52-1-article-new-uniform-digital-assets-law-estate-planning-andadministration-in-information-age%20.authcheckdam.pdf.

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

75. Li, W. S. (2015). On Digital Asset Management Technology. *Computer Programming Skills and Maintenance*. № 24. P. 76–77.

76. Buntinx, J. P. (2017). Digital assets vs cryptocurrencies. The Merkle. [online] Available at: <https://themerke.com>.

77. Кучерявенко Н., Білінський Д., Смичок Є. Науково-правовий висновок «Цифрові активи як об'єкт правового регулювання». Національна академія правових наук України. 2019. 144 с.

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

79. Кудь О., Мащенко М., Пипенко І., Соболева І. Прогнозування впливу цифрових активів на соціально-економічний розвиток підприємства: метод. посібн. Харків: ХОГОКЗ. 2020. 76 с.

80. What are Digital Assets? (2024). Exploring Their Impact on E-Commerce Marketing. *Digital Asset Management*. [online] Available at: <https://www.demoup-cliplister.com/blog/what-are-digital-assets/>.

81. Sjef van Erp, Jos Uitdehaag etc. (2022). ELI Principles on the Use of Digital Assets as Security. Report of the European Law Institute. 36 p.

82. Директива Європейського Парламенту і Ради (ЄС) 2018/843 від 30 травня 2018 року про внесення змін до Директиви (ЄС) 2015/849 про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму та про внесення змін до директив 2009/138/ЄС і 2013/36/ЄС : Директива від 30 травня 2018 р. № 2018/843 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/984_010-18#Text.

83. Digital Assets: Consultation paper (2022). Law Commission. Reforming the law. Law Commission. Reforming the law. № 256. [online] Available at: <https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2022/07/Digital-Assets-Consultation-Paper-Law-Commission-1.pdf>.

84. Digital Assets: Final report (2023). Law Commission. Reforming the law. Law Commission. Reforming the law. № 412. [online] Available at: <https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2023/06/Final-digital-assets-report-FOR-WEBSITE-2.pdf>.

85. Digital assets as personal property: Supplemental report and draft Bill (2024). Law Commission. Reforming the law. Law Commission. Reforming the law. № 416. [online] Available at: <https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/07/Digital-assets-as-personal-property-supplemental-report-and-draft-Bill-web-version.pdf>.

86. National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in all The States at its Annual Conference Meeting in its One-Hundred-and-Twenty-Third Year Seattle (2014). Washington. 12 p. [online] Available at: <http://www.digitalpassing.com/wordpress/wp-content/uploads/2014/07/UFADAA-7-17-2014.pdf>.

87. Digital assets-existing law. State of Wyoming Legislature (2019). [online]

Available at: <https://www.wyoleg.gov/Legislation/2019/SF0125>.

88. Волинка К. Теорія держави і права : навч. посібн. Київ : МАУП. 2003. 240 с.

89. Скакун О. Теорія держави і права : підручн. Харків : Консум. 2001. URL: <http://politics.ellib.org.ua/pages-1591.html>.

90. Скакун О. Теорія держави і права : підручн. 2-ге видання. Київ : Алерта ; ЦУЛ. 2011. 520 с.

91. Тополевський Р., Федіна Н. Теорія держави і права : навч. посібн. Львів : ЛьВДУВС. 2020. 268 с.

92. Revised Uniform Fiduciary Access to Digital Assets Act (2015). [online] Available at: <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=112ab648-b257-97f2-48c2-61fe109a0b33&forceDialog=0>.

93. Бацуца В. Охорона прав на цифрові (віртуальні) активи : дис. ... д-р філософ. (081 – Право). Хмельницький. 2024. 195 с.

94. An Act relative to access to a decedent's electronic mail accounts. No. 4365. The Commonwealth of Massachusetts. [online] Available at: <https://malegislature.gov/Bills/193/S930>.

95. Public Act 099-0775 concerning digital assets. Illinois General Assembly. [online] Available at: <https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=099-0775>.

96. Uniform Access to Digital Assets by Fiduciaries Act. Uniform Law Conference of Canada. [online] Available at: [https://www.ulcc-chlc.ca/ULCC/media/EN-Uniform-Acts/Uniform-Access-to-Digital-Assets-by-Fiduciaries-Act-\(2016\).pdf](https://www.ulcc-chlc.ca/ULCC/media/EN-Uniform-Acts/Uniform-Access-to-Digital-Assets-by-Fiduciaries-Act-(2016).pdf).

97. Digital Asset Business Act 2018. BMA. [online] Available at: <https://www.bma.bm/viewPDF/documents/2023-11-14-11-11-48-Digital-Asset-Business-Act-2018.pdf>.

98. The Bahamas Securities Industry (Contracts for Differences) Rules. *Official Gazette the Bahamas*. [online] Available at:

<https://www.scb.gov.bs/wpcontent/uploads/2019/07/Securities-Industry-Contracts-for-Differences-Rules2020.pdf>.

99. Цивільний кодекс України : Закон України від 16 січня 2003 р. № 435-IV // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/435-15#n6917>.

100. Бацуца В. До питання встановлення правової природи цифрових активів у сучасному цивільному праві. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2022. № 55. С. 32–35.

101. Даниленко О. Щодо цифрових речей як нових об'єктів цивільних прав. *Цивільне право: проблеми теорії та правозастосування* : матеріали XXI наук.-практ. конф., присвяч. 101-й річниці з дня народж. д-ра юрид. наук, проф., чл.-кор. АН УРСР, ректора Харків. юрид. ін-ту (1962-1987 рр.) В. П. Маслова (Харків, 17 лютого 2023 р.) / Нац. юрид. ун-т ім. Ярослава Мудрого, Нац. акад. прав. наук України, Від-ня цивільно-прав. дисциплін, Харків. обл. осередок всеукр. громад. орг. «Асоц. цивілістів України». Харків. 2023. С. 148–154.

102. Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав : Закон України від 10 серпня 2023 р. № 3320-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3320-20#n12>.

103. Форос Г., Жогов В. Адміністративно-правові засади забезпечення в Україні захисту об'єктів авторських і суміжних прав, що виражені у цифровій формі. Одеса : РВВ ОДУВС. 2022. 118 с.

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

105. Білодід І., Горецький П. та ін. Словник української мови: в 11 томах. 1970–1980. Т. 1. С. 29; Т. 3. С. 95; Т. 7. С. 533; Т. 3. С. 300; Т. 8. С. 693; Т. 9. С. 671; Т. 1. С. 346; Т. 4. С. 695; Т. 5. С. 49; Т. 4. С. 271.

106. Русанівський В. та ін. Словник української мови у 20 томах (СУМ-20). Київ : Наукова думка. 2010. 913 с.

107. Бусел В. та ін. Великий тлумачний словник сучасної української мови : 250000. Київ ; Ірпінь : Перун. 2005. VIII. 1728 с.
108. Бусел В. та ін. Великий тлумачний словник сучасної української мови (з дод., допов. та CD). Київ ; Ірпінь : ВТФ «Перун». 2009. 1736 с.
109. OED: Oxford English dictionary: the definitive record of the English language (2011). *English language Dictionaries*. [online] Available at: <https://www.oed.com>.
110. ISO 55000:2014 (2014). Asset management – Overview, principles and terminology [online] Available at: <https://www.iso.org/obp/ui#iso:std:iso:55000:ed-1:v2:en>.
111. Гарантійна угода між Україною та Європейським Інвестиційним Банком «Логістична мережа (Модернізація та цифровізація Укрпошти)» : Угода від 6 жовтня 2020 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/971_005-20#Text.
112. Гулейков І. (2024). Співвідношення цифрового та віртуального активу. *ISPC «Modern Knowledge: Research and Discoveries»*. № 209. Р. 210215.
113. Гурін Б. Теоретико-правова характеристика криптовалют як концептуальних засобів обороту та оцінка їх ролі для розвитку криптоіндустрії в Україні. *Академічні візії*. 2023. № 25. С. 1–12. URL: <https://academy-vision.org/index.php/av/article/view/708>.
114. Дмитрик О. Віртуальні активи і цифрові активи: до питання про співвідношення понять. *Право та інноваційне суспільство*. 2021. № 2 (17). С. 248–254.
115. Овчаренко А. Правове регулювання віртуальних активів та криптовалют в Україні: Сучасний стан та перспективи. *Юридичний науковий електронний журнал*. 2020. № 4. С. 200–202.
116. Проценко А. Правовий статус віртуальних валют: світовий досвід та українські реалії. *Право і суспільство*. 2016. № 2. С. 130–134.
117. Вінник О., Попович Т., Деревянко Б. Регулювання відносин цифрової економіки: окремі аспекти. *Вісник Національної академії правових*

наук України. 2022. Т. 29. № 3. С. 181–204.

118. Demystifying cryptocurrency and digital assets (2022). PwC. [online] Available at: <https://www.pwc.com/us/en/techeffect/emerging-tech/understanding-cryptocurrencydigital-assets.html>.

119. Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard (2022). OECD. 10 October. Paris. 104 p. [online] Available at: <https://www.oecd.org/tax/exchange-of-taxinformation/crypto-asset-reporting-framework-andamendments-to-the-common-reporting-standard.pdf>.

120. Types of Digital Assets Explained with Examples and Use Cases (2023). CFTE. [online] Available at: <https://blog.cfte.education/types-of-digital-assets-explained/>.

121. DAM News. (2023). Types of Digital Asset. [online] Available at: <https://digitalassetmanagementnews.org/features/defining-digital-assets/>.

122. Advice. Initial Coin Offerings and Crypto-Assets (2019). 9 January 2019. ESMA50-157-1391. *European Securities and Markets Authority*. [online] Available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

123. Черних О. Класифікація віртуальних активів в Україні. *Веб-портал: HAS*. 2021. URL: <https://www.hsa.org.ua/blog/klasyfikatsiya-virtualnyh-aktyviv-v-ukrayini/>

124. FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) (2018). Published 16 February 2018. [online] Available at: <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1be-willigung/fintech/wegleitungico.pdf?la=en&hash=9CBB35972F3ABCB146FBF7F09C8E88E453CE600C>.

125. Act No. XXX of 2018 – Virtual Financial Assets Act. 20th July, 2018. *Legizlazzjoni Malta*. [online] Available at: <https://legislation.mt/eli/act/2018/30/eng/pdf>.

126. Act Relating to State Affairs and Government – Rhode Island Economic

Growth Blockchain Act. 2022 – H 7254. State of Rhode Island General Assembly. [online] Available at: <http://webserver.rilin.state.ri.us/BillText22/HouseText22/H7254.pdf>.

127. Іванюк В. Фінансово-правове регулювання ринку криптовалют в Україні : дис. ... д-р філософ. (081 – Право). Тернопіль. 2021. 232 с.

128. Логойда В. Перспективи врегулювання правового статусу криптовалюти в Україні. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2021. Вип. 63. С. 152–157.

129. Логойда В. Криптовалюти як об'єкт цивільних прав: порівняльно-правовий аналіз : дис. ... д-р філософ. (081 – Право). Ужгород. 2022. 287 с.

130. Сословський В., Косовський І. Ринок криптовалют як система. Фінансово-кредитна діяльність: проблеми теорії та практики. 2016. Вип. 2. С. 236–246.

131. ЕВА Opinion on «virtual currencies» (2014). [online] Available at: <https://extranet.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>.

132. Virtual currency schemes – a further analysis (2015). [online] Available at: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

133. Бацуца В. Загальні засади типологізації цифрових активів. *Сучасні виклики для приватного права України: європеїзація, диджиталізація, війна* : матеріали Всеукр. наук.-практ. конф. (Київ–Хмельницький, 21 грудня 2023 р.). Київ : НДІ приватного права ім. Ф. Г. Бурчака НАПрН України. 2023. С. 84–88.

134. Lanzolla, G., Lorenz, A., Miron-Spektor, E., Schilling, M., Solinas, G., C. L. Tucci (2020). Digital transformation: What is new if anything? Emerging patterns and management research. *Academy of Management Discoveries*. Т. 3. № 6. Р. 341–350.

135. Catalini, C., J. S. Gans (2019). Some Simple Economics of the Blockchain. *National Bureau of Economic Research*. June. 40 p.

136. FATF (2019). Guidance for a Risk-Based Approach to Virtual Assets

and Virtual Asset Service Providers. FATF. Paris. [online] Available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

137. Böhm, R., Christin, N., Edelman, B., Moore T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*. Vol. 29. № 2. Spring. P. 213–238.

138. Zohar, A., (2015). Bitcoin: Under the Hood. *Communications of the ACM*. Vol. 58. №. 9. P. 104–113.

139. Кіяшко Ю. Пріоритетні загрози системі економічної безпеки України в умовах воєнного часу: концептуальні погляди на характер та їхню типологізація. *Аналітично-порівняльне правознавство*. 2024. № 5. С. 507–513. DOI: <https://doi.org/10.24144/2788-6018.2024.05.80>.

140. Кіяшко Ю. Цифрові інструменти у структурі актуальних загроз системі економічної безпеки України: теоретико-методологічне дослідження. *International Bulletin on Public Administration and Legal Affairs*. 2024. № 2. С. 81–91. DOI: [10.32844/ibpala-2024-2.10](https://doi.org/10.32844/ibpala-2024-2.10).

141. Україна: Запит на закупівлю за інструментом швидкого фінансування – прес-реліз. Звіт персоналу та Заява Виконавчого директора від України. *Веб-портал: International Monetary Fund*. 2022. URL: <https://www.imf.org/en/Publications/CR/Issues/2022/10/19/Ukraine-Request-for-Purchase-Under-the-Rapid-Financing-Instrument-Press-Release-Staff-524913?cid=em-COM-123-45549>.

142. ООН попереджає, що найближчі перспективи для Співдружності Незалежних Держав та Південно-Східної Європи на тлі війни в Україні та високої геополітичної невизначеності залишаються нестійкими. *Веб-портал: United Nations*. 2023. URL: https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESP2023_PR_CIS_SEE_R.pdf.

143. Економіка України адаптувалася до війни, але є дуже велике «але»: з'явився невтішний прогноз. *Веб-портал: Апостроф*. 2024. URL: <https://apostrophe.ua/ua/news/economy/2024-02-26/ekonomika-ukrainyi->

adaptirovalas-k-voyne-no-est-ochen-bolshoe-no-poyavilsya-nelestnyi-prognoz/314989.

144. Калашник В. Тлумачний словник української мови : понад 12 500 статей (близько 40 000 слів) пуг. 2-ге вид., випр. і доп. Харків : Прапор. 2005. С. 337.

145. Горячова К. Фінансова безпека підприємства. Сутність та місце в системі економічної безпеки. *Економіст*. 2003. № 8. С. 65–67.

146. Пекін А. Економічна безпека підприємств як економіко-правова категорія. *Економіст*. 2007. № 8. С. 23–25.

147. Про Бюро економічної безпеки України : Закон України від 28 січня 2021 р. № 1150-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1150-20#Text>.

148. Лук'яненко Д. Економічна інтеграція та глобальні проблеми сучасності : навч.-метод. посібн. Київ : КНЕУ. 2005.

149. Діденко О. Теоретичне дослідження науково-методичних підходів до дослідження сутності поняття «економічний інтерес». *Демократичне врядування*. 2013. Вип. 12. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2022/feb/26830/didenko.pdf>.

150. Єрмошенко М. Національні економічні інтереси: реалізація і захист. *Актуальні проблеми економіки*. 2002. № 1–2. URL: https://nam.kiev.ua/ape/n_01_1-2/yermosh.htm.

151. Завгородня С. Національні інтереси в економічній сфері: сутність та побудова їх ієрархії. *Аспекти публічного управління*. 2015. № 1–2. С. 40–47.

152. Онищенко В., Рева І. Системний підхід у дослідженні національних економічних інтересів як чинника економічної безпеки держави. *Економіка і регіон*. 2013. № 4. С. 3–9.

153. Шевченко Л., Гриценко О., Макуха С. та ін. Економічна безпека держави: сутність та напрями формування : монографія. Харків : Право. 2009. 312 с.

154. Про затвердження Методичних рекомендацій щодо розрахунку

рівня економічної безпеки України : наказ Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 р. № 1277 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>.

155. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964-IV // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/964-15#Text> (*втрапив чинність*).

156. Мазаракі А., Мельник Т. Економічна безпека України в умовах російської агресії. *Scientia Fructuosa*. 2022. № 145 (5). С. 4–28.

157. Мартиненко В. Загрози економічній безпеці України в контексті викликів глобалізації. *Економічний часопис-XXI*. 2011. № 7–8. С. 40–43.

158. Маслій О., Буряк А. Трансформація загроз економічній безпеці та безпеці інформаційного середовища України в умовах повномасштабної війни. *Держава та регіони. Серія: Економіка та підприємництво*. 2023. № 3 (129). С. 28–32.

159. Маслій О., Ківшик О., Котелевець М. Загрози економічній безпеці держави в умовах глобальних перетворень. *Економічний простір*. 2023. № 183. С. 25–30.

160. Приходько В. Система загроз національним економічним інтересам України. *Інвестиції: практика та досвід*. 2013. № 14. С. 13.

161. Пугач О. Класифікація та систематизація загроз економічній безпеці держави в системі національної безпеки. *Економіка і організація управління*. 2014. Вип. 1–2. С. 209–218.

162. Пугач О., Онищенко С. Загрози економічній безпеці України: сутність, оцінювання та механізм упередження : монографія. Полтава : ПолтНТУ. 2015. 337 с.

163. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 14 травня 2021 р. № 447/2021 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.

164. Про основні засади забезпечення кібербезпеки України : Закон

України від 5 жовтня 2017 р. № 2163-VIII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

165. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.

166. Максименко А. Реальні та потенційні загрози цифрової економіки в умовах війни. *Економічний простір*. 2023. № 188. С. 41–49.

167. Muthusamy, S. K., Kannan, R. (2023). Profits crisis: evolving patterns of firm size and performance in traditional U.S. industries. *Economia e Politica Industriale: Journal of Industrial and Business Economics*. Vol. 50. Issue 3. № 5. P. 575–603. [online] Available at: <https://link.springer.com/article/10.1007/s40812-023-00268-y>.

168. Хаустов В. Цифрова економіка: як тобі служиться? *Веб-портал: Національна академія наук України*. 2019. URL: <https://www.nas.gov.ua/UA/Messages/Pages/View.aspx?MessageID=5604>.

169. Маркевич К. Цифровізація: переваги та шляхи подолання викликів. *Веб-портал: Разумков центр*. 2021. URL: <https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv>.

170. Schumpeter, J. A. (1976). *II. Capitalism, Socialism, and Democracy*, 1942 (5th ed.). George Alwin & Unwin (Publishers) Ltd., First published in the UK in 1942. 460 p.

171. Auer, R., Claessens, S. (2020). Cryptocurrency Market Reactions to Regulatory News. Federal Reserve Bank of Dallas. April. 18 p. [online] Available at: <https://www.dallasfed.org/~media/documents/research/international/wpapers/2020/0381.pdf>.

172. Foley, S., K. Jonathan R., P. Talis J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies, Forthcoming*. December. [online] Available at: <https://ssrn.com/abstract=3102645> or <http://dx.doi.org/10.2139/ssrn.3102645>.

173. Федоров М. В Україні щоденний обіг віртуальних активів становить 1 млрд грн. Але все це у тіні, з жодної операції не сплачують податків. *Веб-портал: ГОРДОН*. 2021. URL: <https://gordonua.com/ukr/blogs/mihail-fedorov/v-ukrajini-shchodennij-oborot-virtualnih-aktiviv-stanovit-1-mlrd-grn-ale-vse-tse-v-tini-ni-z-odnijeji-operatsiji-ne-platjatsja-podatki-1571520.html>.

174. Digital Asset Risk Assessment: A New Paradigm in Risk Management (2022). Deloitte. 6 p.

175. Managing Digital Assets: Overcoming Challenges and Risks (2024). AESIRX. [online] Available at: <https://aesirx.io/blog/dam/managing-digital-assets-overcoming-challenges-and-risks>.

176. Cumming, D., Glatzer, Z., Guedhami, O., (2023). Institutions, digital assets, and implications for economic and financial performance. *Journal of Industrial and Business Economics*. Vol. 50. P. 487–513. [online] Available at: <https://link.springer.com/article/10.1007/s40812-023-00276-y>.

177. Mizrach, B. (2021). The Key Risks in the Digital Assets Space. GLG. [online] Available at: <https://glginsights.com/articles/the-key-risks-in-the-digital-assets-space/>.

178. Isogawa, M. (2023). The Top Security Risks to be Aware of When Managing Your Digital Assets. LinkedIn. [online] Available at: <https://www.linkedin.com/pulse/top-security-risks-aware-when-managing-your-digital-assets-isogawa>.

179. General Risks of Digital Assets (2024). Zero Hash. [online] Available at: [General Risks of Digital Assets – Zero Hash | Help Center](#).

180. 14 Digital Asset Risks To Remember (2022). CFTC. [online] Available at: <https://www.cftc.gov/sites/default/files/2022-09/DigitalAssetRisks.pdf>.

181. Soto, C. (2023). How to Overcome Common Challenges in Digital Asset Management. Openasset. [online] Available at: <https://openasset.com/blog/common-challenges-in-dam/>.

182. Digital Assets Regulation: Insights from Jurisdictional Approaches (2024). Insight report. 41 p. [online] Available at:

https://www3.weforum.org/docs/WEF_Digital_Assets_Regulation_2024.pdf.

183. The EU's Cybersecurity Strategy for the Digital Decade (2020). European Commission. 29 p. [online] Available at: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.

184. Про стимулювання розвитку цифрової економіки в Україні : Закон України від 15 липня 2021 р. № 1667-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1667-20>.

185. Проект Закону про обіг криптовалюти в Україні : Проект Закону України № 7183 від 6 жовтня 2017 р. // База даних: «Законодавство України». URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684.

186. Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні : Проект Закону № 7183-1 від 10 жовтня 2017 р. // База даних: «Законодавство України». URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710.

187. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода від 27 червня 2014 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/984_011#n2669.

188. Директива Європейського Парламенту і Ради (ЄС) 2015/849 від 20 травня 2015 року про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, про внесення змін до Регламенту Європейського Парламенту і Ради (ЄС) № 648/2012 та про скасування Директиви Європейського Парламенту і Ради 2005/60/ЄС та Директиви Комісії 2006/70/ЄС : Директива від 20 травня 2015 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/984_037-15#Text.

189. 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. [online] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114&qid=1730100184935>.

190. Демідко Д. Китайці масово обходять заборону на Bitcoin, інвестуючи у криптовалюту під час економічної кризи. *Веб-портал: Brokker*. 2024. URL: <https://brokker.news/kytajczi-masovo-obhodyat-zaboronu-na-bitcoin>.

191. Некіт Г. Напрями змін у правовому регулюванні обігу криптоактивів: аналіз зарубіжного досвіду. *Економіка та право*. 2022. № 1. С. 33–44.

192. Digital Assets and Registered Exchanges (Amendment) Act, 2022 (2022) : Act. Bahams. [online] Available at: <https://www.scb.gov.bs/wp-content/uploads/2022/05/Digital-Assets-and-Registered-Exchanges-Amendment-Act-2022.pdf>.

193. Digital Assets and Registered Exchanges Bill, 2024. Bahams. [online] Available at: <https://www.scb.gov.bs/wp-content/uploads/2024/05/Digital-Assets-and-Registered-Exchanges-Bill-2024-May-2024.pdf>.

194. Framework for “Investment Contract” Analysis of Digital Assets (2024). U.S. Securities and Exchange Commission. [online] Available at: <https://www.sec.gov/about/divisions-offices/division-corporation-finance/framework-investment-contract-analysis-digital-assets>.

195. Digital Assets Law DIFC Law No. 2 of 2024 (2024). DIFC. [online] Available at: <https://www.difc.ae/business/laws-and-regulations/legal-database/difc-laws/digital-assets-law-difc-law-no-2-of-2024>.

196. Visser, J. (2024). DIFC Announces Enactment of New Digital Assets Law, New Law of Security and Related Amendments to Select Legislation. DIFC. [online] Available at: <https://www.difc.ae/whats-on/news/difc-announces-enactment-of-new-digital-assets-law---new-law-of-security-and-related-amendments>.

197. Law of Security DIFC Law No. 4 of 2024 (2024). DIFC. [online] Available at: <https://www.difc.ae/business/laws-and-regulations/legal-database/difc-laws/law-security-difc-law-no-4-2024>.

198. Ahmed, H. (2024). Singaporeans crypto adoption remains high; staking emerges as top use case. Coinbase. [online] Available at: <https://www.coinbase.com/blog/singaporeans-crypto-adoption-remains-high-staking-emerges-as-top-use-case>.

199. The Developing Global Regulatory Landscape for Digital Assets (2024). State Street. [online] Available at: <https://www.statestreet.com/au/en/asset-manager/insights/digital-digest-developing-global-regulations-digital-assets>.

200. Code monétaire et financier. Version en vigueur au 02 avril 2024 (2024). Légifrance. [online] Available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072026/2024-04-02/.

201. Головій Л., Курило В., Курило І. Адміністративно-правове регулювання поводження з побутовими відходами. *Прикарпатський юридичний вісник*. 2021. № 5 (40). С. 119.

202. Желінський В. Реєстраційна діяльність міністерства юстиції України як об'єкт адміністративно-правового регулювання. *Юридичний бюлетень*. 2019. Вип. 11. Ч. 1. С. 278.

203. Князева Ю. Адміністративно-правове регулювання влаштування дітей-сиріт і дітей, позбавлених батьківського піклування, за законодавством України : автореф. дис. ... канд. юрид. наук : 12.00.07. Запоріжжя. 2024. С. 33.

204. Лакійчук Я. Адміністративно-правове регулювання превентивної діяльності поліції. *Журнал «Підприємництво, господарство і право»*. 2021. № 6. С. 119.

205. Стоєва Т. Адміністративно-правове забезпечення громадської безпеки в Україні. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали VI Міжнародної науково-практичної конференції. (м. Дніпро, 11 березня 2022 р.). Дніпро : Дніпропетровський державний університет внутрішніх справ. 2022. 464 с.

206. Бойчук Р. Правові засади державного регулювання підприємницької діяльності: проблеми формування. *Право та інновації*. 2019.

№ 4 (28). С. 22.

207. Горбачевський В., Ліховицький Я. Про деякі організаційно-правові засади запобігання прокуратурою злочинам, що здійснюється у сфері виконання покарань. *Прокуратура України в умовах європейської інтеграції*. Доповнення до матеріалів міжнародної науково-практичної конференції : матеріали Міжнародної науково-практичної конференції (19 травня 2016 р.). Київ : Національна академія прокуратури України. 2016. 334 с.

208. Козьяков Р. Адміністративно-правове регулювання контрольно-наглядової діяльності в національній поліції України. *Правова позиція*. 2021. № 3 (32). С. 141.

209. Кошиков Д. Сутність правових засад реалізації державної політики у сфері забезпечення економічної безпеки держави. *Вісник пенітенціарної асоціації України*. 2020. № 1 (11). С. 168.

210. Кошиков Д. Адміністративно-правові засади реалізації державної політики у сфері забезпечення економічної безпеки держави : дис. ... д-р юрид. наук : 12.00.07. Суми. 2021. 485 с.

211. Меньяйлов О. Особливості діяльності суддів ВАКС: правові засади. *Науковий вісник Ужгородського національного університету*. Вип. 61. 2020. Т 2. С. 13.

212. Птухіна О. Адміністративно-правові засади діяльності Державної служби України з лікарських засобів та контролю за наркотиками : дис ... д-р філософ. (081 – Право). Харків. 2023. 27 с.

213. Староста В. Адміністративно-правові засади юридичного забезпечення діяльності закладів вищої освіти зі специфічними умовами навчання : дис. ... д-р філософ. (081 – Право). Харків. 2023. 29 с.

214. Чанцева А. Адміністративно-правові засади діяльності патрульної поліції із забезпечення безпеки дорожнього руху в Україні : дис ... д-р філософ. (081 – Право). Харків. 2023. 24 с.

215. Залужний В. Адміністративно-правові засади дисциплінарної відповідальності військовослужбовців Збройних Сил України: поняття,

особливості юридичної природи та змісту. *Право та державне управління*. 2022. № 2. С. 95–102.

216. Коваль М. Зміст та сутність адміністративно-правових засад функціонування митниць. *Науковий вісник Ужгородського національного університету*. 2018. Вип. 50. Т 3. С. 159.

217. Коваль М. Адміністративно-правові засади функціонування митниць в умовах євроінтеграційних процесів в Україні : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя. 2019. С. 46.

218. Курява В. Адміністративно-правові засади та передумови утворення в Україні вищого суду з питань інтелектуальної власності. *Науковий вісник Міжнародного гуманітарного університету*. 2018. № 35. Т 1. С. 99.

219. Курява В. Адміністративно-правові концептуальні засади створення та діяльності вищого суду з питань інтелектуальної власності в Україні : дис ... д-р філософ. (081 – Право). Суми. 2021. С. 78–79.

220. Остапенко О., Ковалів М., Єсімов С., Гулак Л. та ін. Адміністративне право України (загальна частина) : навч. посібн. Вид. 2-ге, доп. Львів : СПОЛОМ. 2021. 616 с.

221. Tarasiuk, Yu. (2020). Problem of determining the place of administrative and legal norms in the system of legal bases of housing construction. *European Reforms Bulletin*. № 4. P. 121.

222. Тарасюк Ю. Адміністративно-правове забезпечення житлового будівництва в Україні : дис. ... канд. юрид. наук : 12.00.07. Суми. 2021. С. 74.

223. Авер'янов В. та ін. Адміністративне право України. Академічний курс : підручн. : у 2-х т. Т. 1. Загальна частина. Київ. 2004. 584 с.

224. Костовська К., Назар Ю., Серeda В. Адміністративне право України : навч. посібн. Львів. 2016. 300 с.

225. Мельник Р. Бевзенко В. Загальне адміністративне право : навч. посібн. Київ : Ваіте. 2014. 376 с.

226. Битяк Ю., Гаращук В., Дьяченко О., Писаренко Н. та ін. Адміністративне право України : підручн. Київ : Юрінком Інтер. 2007. 544 с.

227. Хомулянський В. Адміністративно-правова протидія порушенням митних правил : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя. 2021. 242 с.
228. Заброда Д. Адміністративно-правові засади: сутність та зміст категорії. *Адміністративне право і процес*. 2013. № 2 (4). С. 45–51.
229. Литвин І. Об'єкти адміністративно-правових відносин у сфері надання освітніх послуг. *Підприємництво, господарство і право*. 2016. № 6. С. 114–118.
230. Литвин І. Адміністративно-правові відносини у сфері надання освітніх послуг : автореф. дис. ... д-р юрид. наук : 12.00.07. Дніпро. 2016. 42 с.
231. Про правотворчу діяльність : Закон України від 24 серпня 2023 р. № 3354-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3354-20#Text>.
232. Албу А. Договір як особлива конструкція тлумачення. *Юридичний вісник. Серія : «Проблеми та судження»*. 2023. № 3. С. 84.
233. Вернигора М. Міжнародний договір як джерело права. *Актуальні проблеми приватного та публічного права* : матеріали VI Міжнародної науково-практичної конференції присвяченої 95-річчю від дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, Заслуженого діяча науки України, доктора юридичних наук, професора Процевського О. І. (м. Харків, 31 березня 2023 р). Харків. 2024. С. 327.
234. Градова Ю. Міжнародний договір як об'єкт правового моніторингу. *Південноукраїнський правничий часопис. Серія : «Правова система: теорія і практика»*. 2013. № 2. С. 32.
235. Зверев Є. Міжнародний договір як джерело національного права. *Наукові записки. Серія : «Юридичні науки»*. Т. 103. С. 43.
236. Кізлова О. Категорія «договір» як підстава виникнення правової норми. Концептуальні риси. *Юридичний вісник. Серія : «Проблеми та судження»*. 2013. № 1. С. 105.
237. Про міжнародні договори України : Закон України від 29 червня

2004 р. № 1906-IV // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1906-15#Text>.

238. Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом : Конвенція від 8 листопада 1990 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_029#Text.

239. Бочковий О. Правоохоронна система України: охорона прав чи права охорони? *Проблеми формування громадянського суспільства в Україні: доба нестійкої інституційності* : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 5 травня 2023 р.). Дніпро : ДДУВС. 2023. С. 44–47.

240. Доненко В та Кондратьєв А. Закон як джерело адміністративного права: сучасні підходи до розуміння. *Національний юридичний журнал. Серія : «Теорія і практика»*. 2019. С. 43–44.

241. Мельник Н. Спільні та відмінні риси дефініцій «право» та «закон». *Державотворення та правотворення в контексті євроінтеграції* : збірник тез доповідей учасників учасників VIII Всеукраїнського круглого столу (м. Львів, 8 грудня 2022 р.) / Упорядники: Д. Є. Забзалюк, В. О. Кучер. Львів : ЛьвДУВС. 2022. 234 с.

242. Рій М. Мовленнєвий жанр «закон» у німецькій та українській мовах. Тези звітної наукової конференції професорсько-викладацького складу факультету іноземних мов за 2021 рік (3–4 лютого 2022 р.). Львів : ПАІС. 2022. 320 с.

243. Ткачук С., Юринець Ю. Роль закону у житті держави та суспільства та небезпеки абсолютизації верховенства права. *IV Міжнародний молодіжний науковий юридичний форум* : тези доповідей Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених. Національний авіаційний університет. Київ. 2021. Т. 1. С. 150–152.

244. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 6 грудня

2019 р. № 361-IX // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/361-20>.

245. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.

246. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.

247. Стеблянко А. Адміністративно-правові засади взаємодії правоохоронних органів з фінансовими установами щодо протидії легалізації злочинних доходів : дис. ... д-р філософ. (081 – Право). Суми. 2021. 265 с.

248. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30 червня 1993 р. № 3341-XII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3341-12#Text>.

249. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2135-12>.

250. Гетьман Є. Поняття підзаконного нормативно-правового акту та його співвідношення із нормативно-правовим та правовим актами. *Форум права*. 2013. № 3. С. 110.

251. Гетьман Є. Підзаконний нормативно-правовий акт: поняття, ознаки, функції, види. *Вісник Національної академії правових наук України. Серія : «Питання трудового та адміністративного права»*. 2014. № 2 (77). С. 98.

252. Камінський А. Історія та теорія держави та права, філософія права. *Інноваційна парадигма розвитку економіки, фінансів, обліку та права* : збірник тез доповідей міжнародної науково-практичної конференції (м. Полтава, 15 вересня 2021 р.). Полтава : ЦФЕНД. 2021. 71 с.

253. Обушенко Н. Специфіка систематизації підзаконних нормативно-правових актів. *Український правовий вимір: пошук відповідей на глобальні*

міжнародні виклики : матеріали IV міжнародної науково-практичної конференції. Дніпро. 2022. С. 104.

254. Шуберт Е. Функції підзаконних нормативно-правових актів в Україні. *Прикарпатський юридичний вісник*. 2018. Вип. 2 (23). Т. 4. С. 213.

255. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ Президента України від 11 травня 2023 р. № 273/2023 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/273/2023#Text>.

256. Про затвердження Критеріїв ризиків легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення : наказ Міністерства фінансів України від 28 грудня 2022 р. № 465 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/z0258-23#Text>.

257. Порядок інформаційної взаємодії суб'єктів первинного фінансового моніторингу та Державної служби фінансового моніторингу України : наказ Міністерства фінансів України від 4 червня 2021 р. № 322 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/card/z1036-21> (*набирає чинності*).

258. Кіяшко Ю., Шестаєва М. Роль місцевих загальних судів як суб'єктів захисту прав громадян в Україні. *Травневі правові читання*: матеріали Міжвузівської науково-практичної конференції здобувачів та викладачів закладів вищої освіти – Черкаси : ЧПБ імені Героїв Чорнобиля НУЦЗ України. 2019. 268 с.

259. Слабунова Ю., Кіяшко Ю., Глушко М. Значення діяльності місцевих загальних судів щодо захисту прав громадян у контексті протидії економічній злочинності як загрози фінансовій стабільності України. *Правові горизонти*. 2019. Вип. 17 (30). С. 93–97. DOI: <http://www.doi.org/10.21272/legalhorizons.2019.i17.p:93>.

260. Шевчук Н. Адміністративно-правове регулювання організації

охорони здоров'я на регіональному рівні : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ. 2015. 18 с.

261. Жмурко І., Федоришина Л. Соціальна і фіскальна політика держави: вплив на регіональному рівні. *Електронне наукове видання. Глобальні та національні проблеми економіки*. 2016. Вип. 12. С. 469.

262. Курмаєв П. Сутність механізму управління регіональним соціально-економічним розвитком. *Веб-портал: Economics*. 2009. URL: www.rusnauka.com/12_KPSN_2009/Economics/44539.doc.htm.

263. Сава А., Сидорук Б. Шляхи стимулювання екобезпечного аграрного виробництва на регіональному рівні. *Економічний і соціальний розвиток України в XXI столітті : національна ідентичність та тенденції глобалізації* : зб. тез доп. Х Ювіл. Міжнар. наук.-практ. конф. молод. вчен. 2013. Ч. 2. С. 250–251. URL: <http://dspace.tneu.edu.ua/handle/316497/22326>.

264. Бандурка О. та Литвинов О. І знову про напрями реформування пенітенціарної системи. *Кримінально-виконавча система: Вчора. Сьогодні. Завтра*. 2017. № 1 (1). С. 42.

265. Огородник Є. Провідні напрямки реформування сучасної кримінально-виконавчої політики. *Науковий вісник публічного та приватного права*. 2016. Вип. 2. Ч 2. С. 300.

266. Гамалюк Б, Харун Ю. Формування державної інноваційної політики. *Актуальні проблеми правового регулювання економічного відновлення України* : збірник тез доповідей учасників науково-практичного семінару (м. Львів, 20 жовтня 2023 р.). Львів : ЛьвДУВС. 2023. С. 25–29.

267. Одрехівський М., Когут У. Проблеми формування еко-інноваційної політики. *Вісник Національного університету «Львівська політехніка». Серія : Проблеми економіки та управління*. 2022. № 2 (10). С. 80.

268. Хряпінський П. Заохочення суспільно-корисної поведінки в доктрині кримінального права України. *Правова система України в умовах євроінтеграції* : матеріали Міжнародної науково-практичної інтернет-конференції (м. Дніпро, 9 квітня 2020 р.). Дніпро : НТУ «ДП». 2020. 136 с.

269. Черненко А., Шиян А. Про головну функцію державних органів, що здійснюють кримінальне провадження. *Електронне наукове видання «Порівняльно-аналітичне право»*. Ужгород. 2017. № 5. С. 348.

270. Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 29 липня 2015 р. № 537 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/537-2015-п#Text>.

271. Сорок Рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) : Рекомендації FATF від 25 вересня 2003 р. // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/835_001#Text.

272. Група з розробки фінансових заходів боротьби з відмиванням грошей – FATF. *Веб-портал: Державна служба фінансового моніторингу України*. 2023. URL: <https://www.fiu.gov.ua/content/uk/fatf.htm>.

273. Про затвердження Положення про Державну службу фінансового моніторингу України : Постанова Кабінету Міністрів України від 29 липня 2015 р. № 537 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/537-2015-п#Text>.

274. Нетипові операції підприємців та платежі у криптовалюті потраплять під фінмоніторинг. *Веб-портал: ЛІГА:ЗАКОН*. 2020. URL: https://buh.ligazakon.net/news/192598_netipov-operats-pdprimtsv-ta-platezh-u-kriptovalyut-potraplyat-pd-fnmonitoring.

275. Мельник В., Кіяшко Ю., Бондаренко М. Актуальні питання щодо протидії кіберзагрозам у контексті забезпечення фінансової безпеки держави. *Правові горизонти*. 2019. Вип. 16 (29). С. 55–63.

276. Баранова Ю. *Методологічні правила порівняльно-правових досліджень* : автореф. дис. ... канд. юрид. наук : 12.00.01. Одеса. 2015. 28 с.

277. Баранова Ю. *Методологічні правила порівняльно-правових досліджень* : дис. ... канд. юрид. наук : 12.00.01. Одеса. 2015. 193 с.

278. Царьова І. *Мова і термінологія наукових досліджень у*

юриспруденції : навч. посібн. Дніпро : «Інновація». 2019. 114 с.

279. Черней А. Адміністративна відповідальність під час здійснення державних закупівель : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя. 2015. 189 с.

280. Антонова О. Словник базових понять з курсу «Педагогіка»: навч. посібн. Вид. 2-ге, доп. і перероб. Житомир : Вид-во ЖДУ імені Івана Франка. 2014. 100 с.

281. Merriam-Webster's Learner's Dictionary. [online] Available at: <https://learnersdictionary.com/definition/interaction>.

282. Ібрагімова К. Дефініція поняття соціальна взаємодія, її види та основні теорії. *Проблеми інженерно-педагогічної освіти*. 2013. № 40–41. С. 289–293.

283. Кікінчук В. Форми взаємодії Національної поліції з іншими суб'єктами забезпечення публічної безпеки та порядку в державі. *Право.ua*. 2017. № 1. С. 81–86.

284. Кожушко С. Професійна взаємодія та її характеристики. *Проблеми інженерно-педагогічної освіти*. 2013. № 38–39. С. 247–252.

285. Колянко О. Взаємодія органів державного управління і місцевого самоврядування з громадськістю. *Вісник Львівського торговельно-економічного університету. Серія : Економічні науки*. 2021. № 65. С. 119.

286. Косенко Ю. Педагогічна взаємодія у професійній діяльності вихователя. *Актуальні проблеми науки та освіти* : зб. матеріалів XIV підсумкової наук.-практ. конф. Викладачів (м. Маріуполь, 10 січня 2012 р.). Маріуполь. 2019. С. 170.

287. Круглий В. Теоретико-правові засади взаємодії працівників оперативних підрозділів органів внутрішніх справ з населенням. *Науковий вісник Національної академії внутрішніх справ України*. 2002. № 3. Ч. 2. С. 134.

288. Лемещук М. Взаємодія дітей із загальним недорозвиненням мовлення як складова розвитку у єдиному соціально-розвитковому середовищі дошкільного навчального закладу. *Вісник польсько-української науково-*

дослідницької лабораторії психодидактики імені Яна Амоса Коменського. Серія : «Модернізація освітнього середовища: проблеми та перспективи». Умань. 2019. С. 134.

289. Папуча М., Наконечна М. Взаємодія в освітньому середовищі. *Збірник наукових праць. Психологічні виміри особистісної взаємодії суб'єктів освітнього простору в контексті гуманістичної парадигми*. Київ. 2021. С. 309.

290. Патик А. Форми взаємодії слідчих та оперативно-розшукових підрозділів при розслідуванні майнових злочинів. *Економіка, фінанси і право*. 2009. № 6. С. 26–29.

291. Патик А. Взаємодія слідчих та оперативно-розшукових підрозділів при розкритті та розслідуванні майнових злочинів : дис. ... канд. юрид. наук : 12.00.09. Київ, 2010. 233 с.

292. Подберезький М. Характеристика особливостей педагогічної взаємодії. *Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія : «Педагогіка і психологія»*. 2011. № 2. С. 31.

293. Сугакова Л., Копилов Е. Взаємодія підрозділів Національної поліції України при проведенні оперативно-розшукової діяльності. *Сучасні проблеми оперативно-розшукової протидії кримінальним правопорушенням* : матеріали Всеукраїнської науково-практичної конференції. Дніпро. 2023. С. 279.

294. Стеблянко А. Поняття та зміст взаємодії правоохоронних органів з фінансовими установами щодо протидії легалізації злочинних доходів. *Правові горизонти*. 2019. № 14 (27). С. 87–92.

295. Фесюнін В. Організаційно-правові засади взаємодії органів державної податкової служби з населенням : дис. ... канд. юрид. наук : 12.00.07. Харків. 2007. 187 с.

296. Кіяшко Ю. До питання визначення поняття методів взаємодії суб'єктів системи економічної безпеки України. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали V Міжнародної науково-практичної конференції м. Суми, 20–21 травня 2021 р. Суми : СумДУ. 2021. С. 474–478.

297. Кіяшко Ю. До питання визначення поняття «взаємодія суб'єктів системи економічної безпеки України» як об'єкта правового регулювання. *Юридичний науковий електронний журнал*. 2021. № 12. С. 37–40. DOI: <https://doi.org/10.32782/2524-0374/2021-12/5>.

298. Панова О., Щербина М. Взаємодія поліцейського офіцера громади із структурними підрозділами Національної поліції та іншими суб'єктами, що здійснюють заходи із запобігання і протидії домашньому насильству. *Право і безпека*. 2021. № 3 (82). С. 184–191.

299. Полянський А. Адміністративно-правові засади взаємодії судово-експертних установ з правоохоронними органами : дис. ... д-р юрид. наук : 12.00.07. Суми. 2021. 406 с.

300. Сущенко В., Смирнов А., Коваленко О., Смирнов А. Організація управління персоналом в органах внутрішніх справ : монографія. Київ : Національна академія внутрішніх справ України. 1999. 352 с.

301. Тюрін С. Поняття й ознаки взаємодії органів юстиції України. *Право і Безпека*. 2013. № 2. С. 100–105.

302. Кіяшко Ю. Правові засади взаємодії щодо протидії деяким загрозам економіці, які можуть виникати внаслідок операцій із цифровими активами. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2024. № 12. DOI: <https://doi.org/10.25313/2520-2308-2024-12-10540>.

303. Гаруст Ю., Кіяшко Ю. Ціннісний аспект взаємодії суб'єктів забезпечення системи економічної безпеки України. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали IV Міжнародної науково-практичної конференції: у 2-х ч. (м. Суми, 21–22 травня 2020 р.). Суми: СумДУ. 2020. Ч. 1. С. 65–69.

304. Про затвердження Порядку обміну інформацією між Державною службою фінансового моніторингу України і Міністерством цифрової трансформації України для підвищення ефективності здійснення нагляду за додержанням суб'єктами первинного фінансового моніторингу вимог законодавства з питань запобігання та протидії легалізації (відмиванню)

доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : наказ Міністерства фінансів України, Міністерства цифрової трансформації України від 1 вересня 2020 р. № 541/127 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/z0906-20#Text>.

305. Про затвердження Порядку формування та оприлюднення комплексної адміністративної звітності у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Постанова Кабінету Міністрів України від 5 серпня 2020 р. № 692 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/692-2020-%D0%BF#n10>.

306. Про Державне бюро розслідувань : Закон України від 12 листопада 2015 р. № 794-VIII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/794-19#Text>.

307. Про Національне антикорупційне бюро України : Закон України від 14 жовтня 2014 р. № 1698-VII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1698-18#Text>.

308. Про Національну поліцію : Закон України від 2 липня 2015 р. № 580-VIII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>.

309. Про Службу безпеки України : Закон України від 25 березня 1992 р. № 2229-XII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>.

310. Про затвердження Інструкції про взаємодію правоохоронних органів у сфері боротьби з організованою злочинністю : наказ Міністерства внутрішніх справ України і Служби безпеки України від 10 червня 2011 р. № 317/235 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/z0822-11#Text>.

311. FATF (2018). Guidance on Countering the Financing of Proliferation of

mass destruction. FATF. Paris. [online] Available at: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidancecounter-proliferation-financing.html>.

312. Гаращук В. Теоретико-правові проблеми контролю та нагляду у державному управлінні : автореф. дис. ... д-р юрид. наук : 12.00.07. Харків. 2003. 35 с.

313. Гаращук В. Теоретико-правові проблеми контролю та нагляду у державному управлінні : дис. ... д-р юрид. наук : 12.00.07. Харків. 2003. 413 с.

314. Журавель В. Принципи та види колективних форм захисту трудових прав працівників. *Журнал «Підприємництво, господарство і право»*. 2016. № 2. С. 76.

315. Кайло І. Концепції нагляду і контролю за дотриманням трудового законодавства України : автореф. дис. ... д-р юрид. наук : 12.00.05. Київ. 2021. 39 с.

316. Кайло І. Поняття нагляду і контролю за дотриманням трудового законодавства України. *Держава та регіони*. 2020. № 1 (67). Т. 2. С. 25–32.

317. Ківалов С., Біла Л. Навчально-методичний посібник. Адміністративне право України. Вид. друге, перероб. і доп. Одеса. 2002. С. 63.

318. Козьяков Р. Щодо співвідношення дефініцій «контроль» та «нагляд» в контексті здійснення контрольно-наглядової діяльності в Національній Поліції України. *Юридичний науковий електронний журнал*. 2020. № 5. С. 360–363.

319. Колісніченко С. Адміністративно-правові засади здійснення нагляду та контролю за охороною, захистом, використанням та відтворенням лісів в Україні : дис ... д-р філософ. (081 – Право). Харків. 2024. 232 с.

320. Кравченко В. «Контроль» та «нагляд» – основні риси, відмінність та взаємозв'язок у праві. *Веб-портал: Журнал наукових публікацій аспірантів і докторантів*. 2013. URL: <http://jurnal.org/articles/2013/uri75.html>.

321. Мельниченко А. Адміністративні форми та методи протидії організованій злочинності в Україні. *ПРАВО.UA*. 2020. № 3. С. 229.

322. Сорока Л. Державний нагляд і контроль як основа адміністративно-правового забезпечення та реалізації державних гарантій. *Вчені записки ТНУ імені В. І. Вернадського. Серія : «Юридичні науки»*. 2020. Т 31 (70). № 4. С. 173.

323. Філіпенко А. Контроль і суміжні категорії в адміністративному праві. *Юридичний науковий електронний журнал*. 2021. № 12. С. 318.

324. Хайнацький Є. Адміністративно-правове регулювання епідеміологічного контролю та нагляду в Україні : дис. ... канд. юрид. наук : 12.00.07. Суми. 2021. 234 с.

325. Ярошенко О. Укладення трудового договору, всупереч вимогам Закону України «Про запобігання корупції», як самостійна підстава припинення трудового договору. *Вісник Національної академії правових наук України*. 2016. № 1 (84). С. 104.

326. Коломоєць Т., Гулевська Г. Адміністративне право України. Київ : Істина. 2007. 216 с.

327. Кодекс України з процедур банкрутства : Закон України від 18 жовтня 2018 р. № 2597-VIII // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2597-19#n948>.

328. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 5 квітня 2007 р. № 877-V // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/877-16#Text>.

329. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.

330. Networked Readiness Index (WEF) (2024). [online] Available at: <https://networkreadinessindex.org>.

331. Global Innovation Index (INSEAD, WIPO) (2024). [online] Available at: <https://www.wipo.int/web/global-innovation-index>.

332. ICT Development Index (ITU) (2017). [online] Available at: <https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/default.aspx>.

333. Global Competitiveness Index (WEF) (2017). [online] Available at: <https://www.weforum.org/publications/the-global-competitiveness-report-2020>.

334. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : Розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 67-р // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text>.

335. Science & Engineering Indicators (2018). Appendix Table 6–12. [online] Available at: <https://www.nsf.gov/statistics/2018/nsb20181/downloads>.

336. Nardiello, G., Naumik-Gladka, K., Ptashchenko, O., Maliukina, A. (2017). Economic development based on international entrepreneurship and business tourism. *Economic Annals-XXI*. Vol. 165. No. 5–6. P. 104–109.

337. Selected Database: MVA (2017). [online] Available at: <https://stat.unido.org/database/MVA%202018,%20Manufacturing>.

338. Бучко М. Сучасна корислива економічна злочинність та заходи її попередження : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків. 2002. 24 с.

339. Narust, Yu., Melnyk, V., Kiiashko, Yu., Halunko, V. (2019). Economic crime, innovative mechanisms of counteraction by law enforcement agencies. *Asia Life Sciences*. Supplement. № 21 (2). P. 247–263.

340. Боровик А., Клопотун І. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посібн. Луцьк : СПД Гадяк Ж. В. друкарня «Волиньполіграф». 2019. 304 с.

341. Кіяшко Ю. Загальна характеристика кібертероризму як загрози міжнародній безпеці. *Правові засади функціонування публічної влади щодо забезпечення інтелектуального розвитку та безпеки суспільства*: матеріали Міжнародної науково-практичної конференції, м. Суми, 19-20 травня 2016 р. Суми: СумДУ. 2016. С. 59–62.

342. Ілляшенко А., Кіяшко Ю. Інформаційний тероризм як злочинна діяльність міжнародного масштабу. *Журнал східноєвропейського права*. 2016.

№ 27. С. 94–100.

343. Harust, Yu., Myrhorod-Karpova, V., Mel'nyk, V., Maletov, D., Kiiashko, Yu., Pavlenko, B. (2022). Implementation of international technical assistance projects in Ukraine since 1991 and their actual effectiveness for the state. *Astra Salven*. № 1. P. 691–703.

344. Гаруст Ю., Мельник В., Миргород-Карпова В., Павленко Б., Малетов Д., Кіяшко Ю. Анотований звіт про виконану роботу у 2020 році в рамках досліджень реалізації проєкту із виконання наукових досліджень і розробок. Розробка «Концепції запровадження державної системи контролю за залученням та ефективним використанням міжнародної технічної допомоги в Україні на 2021–2025 рр.». Проєкт Національного фонду досліджень України, номер державної реєстрації – 2020.02/0137. 2020. 8 с.

345. Гаруст Ю., Мельник В., Миргород-Карпова В., Павленко Б., Малетов Д., Кіяшко Ю. Анотований звіт про виконану роботу у рамках досліджень реалізації проєкту із виконання наукових досліджень і розробок. Розробка «Концепції запровадження державної системи контролю за залученням та ефективним використанням міжнародної технічної допомоги в Україні на 2021–2025 рр.». Проєкт Національного фонду досліджень України, номер державної реєстрації – 2020.02/0137. 2021. 8 с.

346. Гаруст Ю., Мельник В., Миргород-Карпова В., Павленко Б., Малетов Д., Кіяшко Ю. Функціонування системи оцінювання ефективності міжнародної технічної допомоги: досвід Європейського Союзу та провідних країн світу. *Правові горизонти*. 2021. № 26 (39). С. 117–124.

347. Гаруст Ю., Мельник В., Миргород-Карпова В., Павленко Б., Малетов Д., Кіяшко Ю. Загальні критерії оцінки ефективності реалізації проєктів міжнародної технічної допомоги в Україні через призму оцінки намірів та результативності виконання проєктів. *Юридичний науковий електронний журнал*. 2021. № 7. С. 71–92.

348. Гаруст Ю. Гуманітарна допомога як вид військового майна: адміністративно-правовий аспект. *Науковий вісник публічного та приватного*

права. 2024. Вип. 1. С. 43–58.

349. Проект Розпорядження КМУ «Про схвалення Стратегії розвитку високотехнологічних галузей до 2025 року та затвердження плану заходів щодо її реалізації» від 2016 р. *Веб-портал: LIGA 360*. 2016. URL: <https://ips.ligazakon.net/document/NT2490>.

350. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 листопада 2021 р. № 1467-р // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text>.

351. Про затвердження Положення про Міністерство фінансів України : Постанова Кабінету Міністрів України від 20 серпня 2014 р. № 375 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/375-2014-%D0%BF#Text>.

352. Слабунова Ю., Кіяшко Ю., Картавий Я. Зарубіжний досвід організації аудиту ефективності в аспекті управління фінансовою системою. *Правові горизонти*. 2019. Вип. 18 (31). С. 142–148.

353. Гаруст Ю., Мельник В., Миргород-Карпова В., Павленко Б., Малетов Д., Кіяшко Ю. Діяльність Міністерства фінансів України, США та Італії: порівняльно-правова характеристика. *Правові горизонти*. 2020. Вип. 25 (38). С. 128–129.

354. Про комітети Верховної Ради України : Закон України від 4 квітня 1995 р. № 116/95-ВР // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/116/95-%E2%F0#Text>.

355. Кіяшко Ю. Цифрові інструменти у системі засобів впливу на темпи і характер перебігу економічних безпекових процесів. *Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference, September 20. 2024. Bern, Swiss Confederation: International Center of Scientific*

Research. P. 75–77.

356. Думчиков М. Особливості кваліфікації шахрайства в кіберпросторі, засобом вчинення якого є віртуальні активи. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького : Журнал. Серія Право*. 2022. № 14 (26). С. 159–165.

357. Думчиков М. Концептуальні засади кримінально-правової охорони кіберпростору в Україні : дис. ... д-р юрид наук : 12.00.08. Дніпро. 2024. 501 с.

358. Кіяшко Ю. Роль та значення взаємодії суб'єктів правоохоронної діяльності з питань протидії явищу економічної злочинності. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали V Міжнародної науково-практичної конференції м. Суми, 20–21 травня 2021 р. Суми: СумДУ. 2021. С. 446–450.

359. Nekrasov, V., Mel'nyk, V., Kryvosheiev, K., Kiiashko, Yu., Yemets, O. (2021). Interaction of law enforcement authorities as the basis of effective combating economic crime. *Journal of Law and Political Science*. Volume 29. Issue 4. P. 366–385.

360. Про Національну комісію з цінних паперів та фондового ринку : Указ Президента України від 23 листопада 2011 р. № 1063/2011 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1063/2011#Text>.

361. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/679-14#n167>.

362. Галунько В., Курило В., Короед С., Дрозд О. та ін. Адміністративне право України. Т. 1. Загальне адміністративне право : навч. посібн. Херсон : Грінь Д. С. 2015. 272 с.

363. Коломoeць Т. Адміністративне право України : підручн. Київ : «Истина». 2008. 457 с.

364. Колпаков В., Кузьменко О. Адміністративне право України : підручн. Київ : Юрінком Інтер. 2003. 544 с.

365. Павленко Б., Кіяшко Ю., Левченко В. Шляхи удосконалення механізмі протидії дискримінації та забезпечення гендерної рівності в секторі безпеки й оборони. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2021. № 93. С. 166–175.

366. Мельник В., Павленко Б., Кіяшко Ю., Сніжко В. Правовий статус органів місцевого самоврядування як суб'єктів адміністративно-правових відносин. *Правові горизонти*. 2020. № 24. С. 29–34.

367. United Nations Charter (full text). United Nations. [online] Available at: <https://www.un.org/en/about-us/un-charter/full-text>

368. Власюк В. 10 способів обходу санкцій, до яких вдаються росіяни. *Веб-портал: ЕКОНОМІЧНА ПРАВДА*. 2022. URL: <https://www.epravda.com.ua/columns/2022/05/25/687436/>

369. Онищенко С., Маслій О., Глушко А., Черв'як А. Загрози соціально-економічній безпеці України: монографія. Полтава: Національний університет імені Юрія Кондратюка. 2022. 375 с.

370. Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року»: Указ Президента України від 11 серпня 2021 р. № 347/2021 // База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/347/2021#Text>

371. Щодо застосування окремих норм матеріального права під час розгляду адміністративних справ (абз. 7 пп. 1 п. 1) : Інформаційний лист Вищого адміністративного суду України від 1 червня 2010 р. № 781/11/13-10 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/v781_760-10#Text

372. Мартин О. Економічна безпека як складова національної безпеки. *Наукові записки Національного університету «Острозька академія». Економіка*. 2013. Вип. 22. С. 68-74.

373. Цвігун Т. Економічна безпека в системі національної безпеки України. *Економіка та суспільство*. 2017. Вип. 11. С. 150-156.

374. Роль ефективного управління державною власністю у відновленні економіки України та на її шляху до євроінтеграції: актуальні питання господарської юрисдикції обговорили на міжнародній конференції. *Веб-портал: Верховний Суд*. 2024. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1615040/>.

375. Воронкова В., Беліченк А., Попов О. та ін. Управління людськими ресурсами: філософські засади : навч. посібн. Київ : Професіонал. 2006. 506 с.

376. Кустовська О. Методологія системного підходу та наукових досліджень : Курс лекцій. Тернопіль : Економічна думка. 2005. 124 с.

377. Груша В. Як змінилося сприйняття криптовалюти бізнесом в Україні за останні п'ять років. *Веб-портал: SPEKA*. 2024. URL: <https://speka.media/yak-zminilos-spriinyattya-kriptovalyuti-biznesom-v-ukrayini-za-ostanni-5-rokiv-9wn770>.

378. Коваленко О. Вперше в Україні. В одному з автосалонів продали електрокар за криптовалюту. *Веб-портал: NV БІЗНЕС*. 2024. URL: <https://biz.nv.ua/ukr/markets/polski-kompaniji-vtratili-do-20-kliyentiv-v-ukrajini-cherez-blokadu-polske-agentstvo-investiciy-i-torgivli-50415005.html>.

379. Human Impact Assessment. *Web portal: United Nations Development Programme*. 2023. June. URL: <https://www.undp.org/ukraine/publications/human-impact-assessment>.

380. OECD (2019). *Належне врядування для забезпечення стійкості критичної інфраструктури. Огляди політики управління ризиками OECD*. Публікація OECD. Париж. <https://doi.org/10.1787/02f0e5a0-en>.

381. The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption (2024). Chainalysis. [online] Available at: <https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/>.

382. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin. [online] Available at: <https://bitcoin.org/bitcoin.pdf>.

383. Vozniuk, A., Tytko, A. (2019). Cryptocurrency: present-day challenges and prospects of development. *Economic Annals-XXI*. 176 (3–4). P. 49–55.

384. Бермудські Острови планують стати найбільшим криптовалютним центром у світі. *Веб-портал: no worries*. 2022. URL: <https://noworries.news/bermudski-ostrovy-planuyut-staty-najbilshym-kryptovalyutnym-czentrom-u-sviti/>.

385. Financial Services and the Treasury Bureau of the Government of the Hong Kong Special Administrative Region (2023). Policy Statement on Development of Virtual Assets in Hong Kong. [online] Available at: https://gia.info.gov.hk/general/202210/31/P2022103000454_404805_1_1667173469522.pdf.

386. Башбишева М. Побита, але не зломлена. Чого Японія може навчити США та світ у регулюванні криптовалют. Розбір Forbes. *Веб-портал: Forbes*. 2023. URL: <https://forbes.ua/innovations/uroki-z-regulyuvannya-kripto-vid-yaponii-10052023-13577>.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Слабунова Ю., **Кіяшко Ю.**, Глушко М. Значення діяльності місцевих загальних судів щодо захисту прав громадян у контексті протидії економічній злочинності як загрозі фінансовій стабільності України. *Правові горизонти*. 2019. Вип. 17 (30). С. 93–97.

DOI: <http://www.doi.org/10.21272/legalhorizons.2019.i17.p:81>.

2. Кіяшко Ю. До питання визначення поняття «взаємодія суб'єктів системи економічної безпеки України» як об'єкта правового регулювання. *Юридичний науковий електронний журнал*. 2021. № 12. С. 37–40.

DOI: <https://doi.org/10.32782/2524-0374/2021-12/5>.

3. Nekrasov, V., Mel'nyk, V., Kryvosheiev, K., **Kiiashko, Yu.**, Yemets, O. Interaction of law enforcement authorities as the basis of effective combating economic crime. *Journal of Law and Political Science*. 2021. Vol. 29. Iss. 4. P. 366–385 (*Web of Science*).

4. Кіяшко Ю. Поняття «системи економічної безпеки України»: адміністративно-правовий вимір. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2022. № 1.

DOI: <https://doi.org/10.25313/2520-2308-2022-1-7882>.

5. Кіяшко Ю. Пріоритетні загрози системі економічної безпеки України в умовах воєнного часу: концептуальні погляди на характер та їхню типологізація. *Аналітично-порівняльне правознавство*. 2024. № 5. С. 507–513.

DOI: <https://doi.org/10.24144/2788-6018.2024.05.80>

6. Кіяшко Ю. Правові засади взаємодії щодо протидії деяким загрозам економіці, які можуть виникати внаслідок операцій із цифровими активами. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2024.

№ 12. DOI: <https://doi.org/10.25313/2520-2308-2024-12-10540>.

які засвідчують апробацію матеріалів дисертації:

7. Гаруст Ю., **Кіяшко Ю.** Ціннісний аспект взаємодії суб'єктів забезпечення системи економічної безпеки України. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали IV Міжнародної науково-практичної конференції: у 2-х ч. (Суми, 21–22 трав. 2020 р.). Суми: СумДУ. 2020. Ч. 1. С. 65–69.

8. Кіяшко Ю. Роль та значення взаємодії суб'єктів правоохоронної діяльності з питань протидії явищу економічної злочинності. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали V Міжнародної науково-практичної конференції (Суми, 20–21 трав. 2021 р.). Суми: СумДУ. 2021. С. 446–450.

9. Кіяшко Ю. До питання визначення поняття методів взаємодії суб'єктів системи економічної безпеки України. *Реформування правової системи в контексті євроінтеграційних процесів*: матеріали V Міжнародної науково-практичної конференції (Суми, 20–21 трав. 2021 р.). Суми: СумДУ. 2021. С. 474–478.

10. Кіяшко Ю. До питання доцільності та методологічної обґрунтованості використання в науковому обігу категорії «система економічної безпеки України». *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти*: збірник наукових праць з матеріалами III Міжнародної наукової конференції (Дніпро, 6 верес. 2024 р.). Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп». 2024. С. 69–71.

11. Кіяшко Ю. Цифрові інструменти у системі засобів впливу на темпи і характер перебігу економічних безпекових процесів. *Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference*, (September 20 2024, Bern). Swiss Confederation: International Center of Scientific Research. P. 75–77.

ЗАТВЕРДЖУЮ

В. о. Президента Науково-дослідного
інституту публічного права,
доктор юридичних наук, професор


Сергій КОРОЄД
14. Серпень 2025 р.

АКТ

**упровадження результатів дисертаційного дослідження
Кіяшка Юрія Михайловича «Адміністративно-правове забезпечення
протидії загрозам системі економічної безпеки України, що можуть виникати
внаслідок операцій із цифровими активами», поданого на здобуття ступеня
доктора філософії зі спеціальності 081«Право» в освітній процес Науково-
дослідного інституту публічного права**

Комісія в складі: завідувача відділу проблем публічного права, доктора юридичних наук, професора Овчарука Сергія Станіславовича (голова комісії), головного наукового співробітника Науково-дослідного інституту публічного права, доктора юридичних наук, професора Луценко-Миськів Лесі Ігорівни, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Козіна Сергія Миколайовича складала цей акт про те, що матеріали дисертації Кіяшка Юрія Михайловича «Адміністративно-правове забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами» (на здобуття ступеня доктора філософії зі спеціальності 081«Право») мають необхідний теоретичний, методологічний рівень і практичну значимість та використовуються в освітньому процесі. Під час обговорення наданих матеріалів комісією було констатовано, що окремі положення дослідження було використано при розробленні лекційних курсів з дисципліни, яка викладається у Науково-дослідному інституті публічного права, а саме «Адміністративне право та процес: доктринальні та практичні проблеми», при підготовці відповідних підручників, навчальних посібників, а також у контексті інших дисциплін, які викладаються в Інституті. Лекційний курс окремих тем навчальних дисциплін увібрав положення цього дисертаційного дослідження.

ВИСНОВОК:

результати дисертаційного дослідження на тему: «Адміністративно-правове забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами» Кіяшка Юрія Михайловича вважати впровадженими в освітній процес Науково-дослідного інституту публічного права з дисципліни «Адміністративне право та процес: доктринальні та практичні проблеми».

Голова комісії:

Сергій ОВЧАРУК

Члени комісії:

Леся ЛУЦЕНКО-МИСЬКІВ

Сергій КОЗІН

ЗАТВЕРДЖУЮ

В.о. Президента Науково-дослідного інституту публічного права,
доктор юридичних наук, професор

Сергій КОРОЄД

« 14 » січня 2025 р.

А К Т

**впровадження результатів дисертаційного дослідження
Кіяшка Юрія Михайловича «Адміністративно-правове забезпечення
протидії загрозам системі економічної безпеки України, що можуть
виникати внаслідок операцій із цифровими активами», поданого на
здобуття ступеня доктора філософії зі спеціальності 081«Право» у науково-
дослідну діяльність Науково-дослідного інституту публічного права**

Комісія в складі: завідувача відділу проблем публічного права, доктора юридичних наук, професора Овчарука Сергія Станіславовича (голова комісії), головного наукового співробітника Науково-дослідного інституту публічного права, доктора юридичних наук, професора Луценко-Миськів Лесі Ігорівни, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Козіна Сергія Миколайовича склала цей акт про те, що матеріали дисертації Кіяшка Юрія Михайловича «Адміністративно-правове забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами» (на здобуття ступеня доктора філософії зі спеціальності 081«Право») мають необхідний теоретичний, методологічний рівень і практичну значимість та використовуються у науково-дослідній діяльності наукових відділів Науково-дослідного інституту публічного права під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем адміністративно-правового забезпечення з протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими активами, та використовуються Інститутом в межах реалізації науково-дослідної теми «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації №0120U105390).

Використання результатів дисертації сприятиме активізації та підвищенню ефективності наукової роботи працівників відділів та аспірантів Науково-дослідного інституту публічного права.

ВИСНОВОК

Результати дисертації Кіяшка Юрія Михайловича на тему «Адміністративно-правове забезпечення протидії загрозам системі економічної безпеки України, що можуть виникати внаслідок операцій із цифровими

активами» вважати впровадженими у науково-дослідну діяльність Науково-дослідного інституту публічного права, під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем контрольно-наглядової діяльності у сфері протидії домашньому насильству.

Голова комісії:

Сергій ОВЧАРУК

Члени комісії:

Леся ЛУЦЕНКО-МИСЬКІВ

Сергій КОЗІН