

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА**

Кваліфікаційна наукова праця
на правах рукопису
УДК 343.3/.7:[336.74:004](477)

НОГІН ВОЛОДИМИР ВОЛОДИМИРОВИЧ

**ДИСЕРТАЦІЯ
КРИМІНАЛЬНО-ПРАВОВА ПОЛІТИКА У СФЕРІ ЗАБЕЗПЕЧЕННЯ
ОХОРОНИ ВІРТУАЛЬНИХ АКТИВІВ**

Спеціальність 081 «Право»
Галузь знань 08 «Право»

Подається на здобуття ступеня доктора філософії

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

_____ В. В. Ногін

Науковий керівник: Козич Ігор Васильович, доктор юридичних наук,
професор

Івано-Франківськ - 2026

АНОТАЦІЯ

Ногін В. В. Кримінально-правова політика у сфері забезпечення охорони віртуальних активів. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право» (галузь знань 08 «Право»). - Карпатський національний університет імені Василя Стефаника Міністерства освіти і науки України, Івано-Франківськ, 2026.

Дисертація є комплексним монографічним дослідженням кримінально-правової політики у сфері забезпечення охорони віртуальних активів, виконаним з урахуванням права Європейського Союзу (насамперед Регламенту (ЄС) 2023/1114 (MiCA)), міжнародних стандартів (Групи з розробки фінансових заходів боротьби з відмиванням грошей (ФАТФ), Ради з фінансової стабільності, Міжнародного валютного фонду) та перехідного стану національного регулювання, за якого профільний Закон України «Про віртуальні активи» № 2074-IX залишається ухваленим, але не введеним у дію, унаслідок чого чинна легальна дефініція віртуального активу *de jure* виводиться із Закону України № 361-IX. Актуальність роботи зумовлена стрімким поширенням віртуальних активів, їх транскордонною та технологічно складною природою, дедалі ширшим використанням у механізмі вчинення та приховування кримінальних правопорушень, а також незавершеністю національної реформи регулювання їх обігу, реформаторська траєкторія якої пролягає через проєкт Закону № 10225-д та модель MiCA, що потребує науково обґрунтованого визначення меж і змісту кримінально-правової охорони цієї сфери.

Об'єктом дослідження є суспільні відносини, що складаються у сфері формування та реалізації кримінально-правової політики щодо забезпечення охорони віртуальних активів; предметом — кримінально-правова політика у цій сфері, її поняття, зміст, принципи, засоби та механізми реалізації у взаємозв'язку з регулятивним, кримінальним процесуальним і кримінально-виконавчим законодавством України та правом Європейського Союзу. Мета

роботи полягає у формуванні цілісної наукової концепції кримінально-правової політики у сфері забезпечення охорони віртуальних активів і в розробленні на її основі науково обґрунтованих пропозицій щодо вдосконалення національного законодавства та практики його застосування. Методологічну основу дослідження становить система загальнонаукових і спеціально-юридичних методів — діалектичного, історико-правового, порівняльно-правового, формально-юридичного, системно-структурного, статистичного й методу моделювання, застосованих у їх поєднанні; окремі допоміжні операції з опрацювання та систематизації масиву джерел виконано із залученням інструментів штучного інтелекту з подальшою авторською верифікацією результатів.

У першому розділі досліджено теоретико-методологічні та понятійні засади вивчення віртуальних активів як об'єкта кримінально-правової охорони: з'ясовано генезу, економіко-технологічні передумови та міждисциплінарний зміст поняття «віртуальні активи»; простежено еволюцію національного правового статусу — від кваліфікації криптовалюти як «грошового сурогату» до її визнання «цифровим вираженням вартості». Сформульовано визначення віртуального активу як майна особливого роду (*suī generis*), субстратом якого є сама інформація, а не носій права вимоги; вибудовано понятійний ланцюг «цифрові речі (цифрові активи) — віртуальні активи — криптоактиви — криптовалюта» з послідовним розмежуванням віртуальних активів від суміжних категорій — нематеріальних благ та інформації, грошей і засобів платежу, цінних паперів і фінансових інструментів, робіт і послуг. Систематизовано класифікації віртуальних активів за законодавством України та Європейського Союзу й доктриною (зокрема трикомпонентну модель MiCA: токени, забезпечені активами, токени електронних грошей та інші криптоактиви) й обґрунтовано самостійне кримінально-правове значення такої класифікації для встановлення предмета посягання та правильної кваліфікації.

Другий розділ присвячено питанням формування та реалізації кримінально-правової політики у досліджуваній сфері. Проаналізовано стан наукової розробленості проблеми й визначено методологічні засади

дослідження; сформульовано авторське поняття кримінально-правової політики у сфері забезпечення охорони віртуальних активів як самостійного сегмента політики у сфері протидії злочинності та розкрито її структуру через об'єкт, суб'єктів формування і реалізації, систему принципів та засоби. Виокремлено основні ознаки цієї політики — подвійну родову належність, похідний (субсидіарний) характер щодо регулятивного законодавства з переважно бланкетною природою заборон, міжнародну та європейську зумовленість, технологічну складність об'єкта й динамічність. Окремо обґрунтовано співвідношення кримінально-правової політики з адміністративно- та фінансово-правовим забезпеченням обігу віртуальних активів і доведено, що належна криміналізація посягань у цій сфері є можливою лише за умови попереднього або одночасного впорядкування регулятивної основи їх обігу. Охарактеризовано міжнародні стандарти, право Європейського Союзу та досвід окремих держав як орієнтири національної політики, оцінено чинний стан національного регулювання й окреслено напрями його реформування з урахуванням МіСА, а також визначено місце кримінально-правових засобів у механізмі охорони обігу віртуальних активів і ризик-орієнтовані засади запобігання відповідним правопорушенням.

У третьому розділі встановлено місце віртуальних активів у системі складу кримінального правопорушення, здійснено загальну характеристику й запропоновано багатовимірну типологію кримінальних правопорушень у цій сфері — за роллю активу у складі (предмет; засіб або знаряддя вчинення; об'єкт протиправного впливу; предмет незаконного збагачення та об'єкт фінансового моніторингу), за технологічним критерієм (кіберуможливлені та кіберзалежні посягання) і за безпосереднім об'єктом охорони з прив'язкою до відповідних статей Кримінального кодексу України. Доведено практичне значення розмежування предмета і засобу вчинення, помилкове ототожнення яких спотворює юридичну оцінку діяння. Розкрито особливості кваліфікації типових правопорушень, що вчиняються щодо віртуальних активів або з їх використанням: легалізації (відмивання) майна, одержаного злочинним шляхом, фінансування тероризму та обходу санкцій, шахрайства й інших

кримінальних правопорушень проти власності, корупційних правопорушень, а також правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

Четвертий розділ присвячено взаємозв'язку кримінально-правової політики у сфері забезпечення охорони віртуальних активів із кримінально-процесуальною та кримінально-виконавчою політикою. Виявлено особливості кримінального процесуального доказування, досудового розслідування та укладення угод у відповідних провадженнях, зокрема щодо стандарту встановлення належності активу певній особі. Досліджено матеріально-технічні та правові механізми арешту, спеціальної конфіскації та звернення стягнення на віртуальні активи, а також виконання судових рішень щодо їх конфіскації у кримінально-виконавчому та виконавчому провадженні. Обґрунтовано положення про нерозривний взаємозв'язок матеріальної, процесуальної та кримінально-виконавчої складових: матеріальна заборона, не забезпечена дієвими інструментами виявлення, фіксації, доказування, конфіскації й реалізації активу, залишається декларативною, а технічні прогалини, що паралізують звернення стягнення на віртуальні активи у виконавчому провадженні, тотожно паралізують і кримінально-виконавчу реалізацію їх конфіскації.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших у вітчизняній науці комплексних досліджень кримінально-правової політики у сфері забезпечення охорони віртуальних активів, здійснених із системним урахуванням права Європейського Союзу та перехідного стану національного регулювання. Уперше сформульовано авторську концепцію кримінально-правової політики у цій сфері як самостійного сегмента політики у сфері протидії злочинності з подвійною родовою належністю; запропоновано визначення віртуального активу як майна особливого роду (*sui generis*), основою якого є інформація; розроблено багатовимірну типологію кримінальних правопорушень у сфері обігу віртуальних активів; обґрунтовано тезу про нерозривний взаємозв'язок матеріальної, процесуальної та кримінально-виконавчої складових охорони.

Удосконалено наукові підходи до класифікації віртуальних активів для потреб кримінально-правової кваліфікації, до розуміння бланкетної природи відповідних заборон та до розмежування віртуального активу як предмета і як засобу вчинення кримінального правопорушення. Дістали подальшого розвитку положення щодо адаптації матеріального, процесуального та кримінально-виконавчого законодавства до природи віртуальних активів, зокрема щодо тлумачення поняття «майно» у статті 59 Кримінального кодексу України в контексті їх конфіскації, стандарту доведення належності активу через публічну адресу (відкритий ключ) і переходу до критерію фактичного контролю.

Практичне значення одержаних результатів полягає в можливості їх використання у законопроектній роботі (під час доопрацювання профільної реформи за моделлю MiCA), у правозастосовній діяльності органів досудового розслідування, прокуратури й суду, а також у навчальному процесі під час викладання кримінального права, кримінального процесу та спеціальних дисциплін. За результатами дослідження сформульовано науково обґрунтовані пропозиції щодо адаптації матеріального, процесуального та кримінально-виконавчого законодавства до природи віртуальних активів, а також щодо запровадження технічно спроможної процедури ідентифікації, арешту, оцінки й реалізації віртуальних активів через авторизованих посередників, синхронізованої з профільною реформою за моделлю MiCA та стандартами ФАТФ.

Ключові слова: кримінально-правова політика, віртуальні активи, кримінальна відповідальність, криміналізація, кваліфікація кримінального правопорушення, предмет кримінального правопорушення, знаряддя і засоби вчинення кримінального правопорушення, кримінальні правопорушення проти власності, кримінальні правопорушення у сфері господарської діяльності, комп'ютерні кримінальні правопорушення, корупційні правопорушення, покарання та його види, спеціальна конфіскація, законодавство Європейського Союзу, гармонізація законодавства.

SUMMARY

Nohin V. V. Criminal-Law Policy in the Sphere of Ensuring the Protection of Virtual Assets. - Qualifying scientific work on the rights of a manuscript.

Dissertation for the Doctor of Philosophy degree in specialty 081 “Law”. - Vasyl Stefanyk Carpathian National University of the Ministry of Education and Science of Ukraine, Ivano-Frankivsk, 2026.

The dissertation is a comprehensive monographic study of criminal-law policy in the sphere of ensuring the protection of virtual assets, carried out with regard to the law of the European Union (primarily Regulation (EU) 2023/1114 (MiCA)), international standards (the Financial Action Task Force (FATF), the Financial Stability Board, the International Monetary Fund) and the transitional state of national regulation, under which the specialized Law of Ukraine “On Virtual Assets” No. 2074-IX remains adopted but has not entered into force, with the result that the operative legal definition of a virtual asset is de jure derived from Law of Ukraine No. 361-IX. The relevance of the study is determined by the rapid spread of virtual assets, their cross-border and technologically complex nature, their increasing use in the mechanism of committing and concealing criminal offences, and the incompleteness of the national reform of their circulation — whose reform trajectory runs through draft Law No. 10225-d and the MiCA model — which calls for a scientifically grounded determination of the limits and content of criminal-law protection in this sphere.

The object of the study is the social relations arising in the sphere of formation and implementation of criminal-law policy regarding the protection of virtual assets; the subject is criminal-law policy in this sphere — its concept, content, principles, means and mechanisms of implementation in their interrelation with the regulatory, criminal procedural and penal (criminal-executive) legislation of Ukraine and EU law. The aim of the work is to form a coherent scientific conception of criminal-law policy in the sphere of ensuring the protection of virtual assets and, on its basis, to develop scientifically grounded proposals for improving national legislation and the practice of its application. The methodological basis of the study comprises a system of general scientific and special legal methods — dialectical, historical-legal,

comparative-legal, formal-legal, systemic-structural, statistical and modelling — applied in combination; certain auxiliary operations for processing and systematizing the body of sources were performed using artificial-intelligence tools, with subsequent verification of the results by the author.

The first chapter examines the theoretical-methodological and conceptual foundations of studying virtual assets as an object of criminal-law protection: it clarifies the genesis, the economic and technological preconditions and the interdisciplinary content of the concept of “virtual assets”, and traces the evolution of the national legal status — from qualifying cryptocurrency as a “monetary surrogate” to recognizing it as a “digital expression of value”. A definition of a virtual asset as property of a special kind (*sui generis*) is formulated, the substrate of which is information itself rather than a carrier of a claim right; a conceptual chain “digital things (digital assets) — virtual assets — crypto-assets — cryptocurrency” is built, with a consistent delimitation of virtual assets from adjacent categories — intangible goods and information, money and means of payment, securities and financial instruments, works and services. The classifications of virtual assets under the legislation of Ukraine and the European Union and under doctrine are systematized (in particular, the three-component MiCA model: asset-referenced tokens, e-money tokens and other crypto-assets), and the independent criminal-law significance of such classification for establishing the object of an offence and its correct qualification is substantiated.

The second chapter is devoted to the formation and implementation of criminal-law policy in the sphere under study. The state of scholarly development of the problem is analyzed and the methodological foundations of the research are determined; the author’s concept of criminal-law policy in the sphere of ensuring the protection of virtual assets is formulated as an independent segment of policy in the sphere of combating crime, and its structure is disclosed through its object, the subjects of its formation and implementation, the system of principles and the means employed. The principal features of this policy are identified — its dual generic affiliation, its derivative (subsidiary) character with respect to regulatory legislation with the predominantly blanket nature of its prohibitions, its international and

European conditioning, the technological complexity of its object and its dynamism. The correlation of criminal-law policy with the administrative-law and financial-law support of the circulation of virtual assets is separately substantiated, and it is shown that the proper criminalization of offences in this sphere is possible only on condition of prior or simultaneous ordering of the regulatory basis of their circulation. International standards, EU law and the experience of individual states are characterized as benchmarks for national policy; the current state of national regulation is assessed and directions for its reform with regard to MiCA are outlined; and the place of criminal-law means within the mechanism of protecting the circulation of virtual assets and the risk-oriented foundations of preventing the relevant offences are determined.

The third chapter establishes the place of virtual assets within the system of the elements of a criminal offence, provides a general characterization and proposes a multidimensional typology of criminal offences in this sphere — by the role of the asset within the *corpus delicti* (object of the offence; means or instrument of its commission; object of unlawful influence; object of illicit enrichment and of financial monitoring), by a technological criterion (cyber-enabled and cyber-dependent attacks) and by the immediate object of protection, tied to the relevant articles of the Criminal Code of Ukraine. The practical significance of distinguishing the object of an offence from the means of its commission — whose erroneous conflation distorts the legal assessment of the act — is demonstrated. The peculiarities of qualifying typical offences committed in respect of virtual assets or with their use are disclosed: legalization (laundering) of property obtained through crime, financing of terrorism and circumvention of sanctions, fraud and other criminal offences against property, corruption-related offences, and offences in the sphere of the use of electronic computers (computers), systems and computer networks.

The fourth chapter is devoted to the interconnection of criminal-law policy in the sphere of ensuring the protection of virtual assets with criminal procedural and penal (criminal-executive) policy. The peculiarities of criminal procedural proof, pre-trial investigation and the conclusion of agreements in the relevant proceedings are revealed, in particular as regards the standard for establishing the attribution of an

asset to a particular person. The material-technical and legal mechanisms of seizure, special confiscation and enforcement against virtual assets, as well as the execution of court decisions on their confiscation in penal and enforcement proceedings, are studied. The proposition concerning the indissoluble interconnection of the substantive, procedural and penal components is substantiated: a substantive prohibition that is not backed by effective instruments for detecting, recording, proving, confiscating and realizing an asset remains declarative, while the technical gaps that paralyze enforcement against virtual assets in enforcement proceedings equally paralyze the penal realization of their confiscation.

The scientific novelty of the obtained results lies in the fact that the dissertation is one of the first comprehensive studies in domestic scholarship of criminal-law policy in the sphere of ensuring the protection of virtual assets, carried out with systematic regard to EU law and the transitional state of national regulation. For the first time, the author's conception of criminal-law policy in this sphere is formulated as an independent segment of policy in the sphere of combating crime with a dual generic affiliation; a definition of a virtual asset as property of a special kind (*sui generis*), the substrate of which is information, is proposed; a multidimensional typology of criminal offences in the sphere of the circulation of virtual assets is developed; and the thesis of the indissoluble interconnection of the substantive, procedural and penal components of protection is substantiated. Scholarly approaches have been improved with respect to the classification of virtual assets for the purposes of criminal-law qualification, to understanding the blanket nature of the relevant prohibitions, and to distinguishing a virtual asset as the object and as the means of committing a criminal offence. Provisions have received further development concerning the adaptation of substantive, procedural and penal legislation to the nature of virtual assets — in particular, regarding the interpretation of the concept of “property” in Article 59 of the Criminal Code of Ukraine in the context of their confiscation, the standard of proving the attribution of an asset through a public address (public key) and the transition to the criterion of actual control.

The practical significance of the obtained results lies in the possibility of their use in legislative drafting (in the course of finalizing the specialized reform along the MiCA model), in the law-enforcement activity of pre-trial investigation bodies, the prosecution and the court, and in the educational process in teaching criminal law, criminal procedure and special disciplines. On the basis of the study, scientifically grounded proposals are formulated for adapting substantive, procedural and penal legislation to the nature of virtual assets, as well as for introducing a technically capable procedure for the identification, seizure, valuation and realization of virtual assets through authorized intermediaries, synchronized with the specialized reform along the MiCA model and the FATF standards.

Keywords: criminal-law policy, virtual assets, criminal liability, criminalization, qualification of a criminal offence, object of a criminal offence, instruments and means of committing a criminal offence, criminal offences against property, criminal offences in the sphere of economic activity, computer criminal offences, corruption-related offences, punishment and its types, special confiscation, legislation of the European Union, harmonization of legislation.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України (категорія «Б»):

1. Ногін В.В. Генеза поняття віртуальних активів та предмет кримінально-правової охорони. *Актуальні проблеми вдосконалення чинного законодавства України. Випуск 60, 2022. С.293-301*

DOI: <https://doi.org/10.15330/apiclu.60.293-301>

URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10750/10367>

2. Ногін В.В. Легальні дефініції віртуального актива та їх значення для кримінально-правової охорони. *Актуальні проблеми вдосконалення чинного законодавства України. Випуск 61, 2023. С.1.72-1.79*

DOI: <https://doi.org/10.15330/apiclu.61.1.72-1.79>

URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10751/10368>

3. Ногін В.В. Зарубіжний досвід правового регулювання віртуальних активів у сфері протидії відмиванню коштів і фінансуванню тероризму та орієнтири для кримінально-правової політики України. *Актуальні проблеми вдосконалення чинного законодавства України. Випуск 65, 2024. С.1.149-1.158*

DOI: <https://doi.org/10.15330/apiclu.65.1.149-1.158>

URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10752/10369>

Праці, що засвідчують апробацію матеріалів дисертації:

4. Ногін В.В. Кримінально-правова політика у сфері захисту віртуальних активів: виклики та перспективи. *Вдосконалення правового регулювання: погляд молодих науковців [Текст] : Матеріали щорічної Всеукраїнської науково-практичної конференції здобувачів освіти та молодих вчених (9 травня 2025 року). Івано-Франківськ, 2025.с. 319-321.*

URL:

<https://law.cnu.edu.ua/wp-content/uploads/sites/100/2025/12/youth2025.pdf>

5. Ногін В.В. Цивільно-правовий договір щодо віртуальних активів у механізмі кримінально-правової охорони. *Договір як універсальна форма правового регулювання: Матеріали Всеукраїнської науково-практичної конференції, присвяченої пам'яті академіка Національної академії правових наук України, заслуженого діяча науки і техніки України, доктора юридичних наук, професора Володимира Васильовича Луця (1933-2021) (м. Івано-Франківськ, 17 квітня 2026р.). Івано-Франківськ: Карпатський національний університет імені Василя Стефаника, 2026. Івано-Франківськ, 2025.с. 268-271.*

URL:

https://kcp.cnu.edu.ua/wp-content/uploads/sites/82/2026/06/zbirnyk_dohovir_2026-2.pdf

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ.....	16
РОЗДІЛ 1.....	29
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПОНЯТІЙНІ ЗАСАДИ ДОСЛІДЖЕННЯ ВІРТУАЛЬНИХ АКТИВІВ ЯК ОБ’ЄКТА КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ	29
1.1. ГЕНЕЗА ТА МІЖДИСЦИПЛІНАРНІ АСПЕКТИ ПОНЯТТЯ «ВІРТУАЛЬНІ АКТИВИ» ...	29
1.2. Розмежування віртуальних активів із суміжними поняттями.....	40
1.3. Класифікація віртуальних активів та її кримінально-правове значення.....	47
Висновки до розділу 1.....	53
РОЗДІЛ 2.....	56
ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ВІРТУАЛЬНИХ АКТИВІВ.....	56
2.1. Стан наукової розробки проблеми та методологія дослідження кримінально-правової політики у сфері забезпечення охорони віртуальних активів.....	56
2.2. Поняття, ознаки та структура кримінально-правової політики у сфері забезпечення охорони віртуальних активів.....	62
2.3. Міжнародні стандарти та зарубіжний досвід як орієнтири кримінально-правової політики у сфері забезпечення охорони віртуальних активів.....	73
2.3.1. Міжнародні стандарти регулювання та охорони віртуальних активів.....	73
2.3.2. Законодавство і досвід Європейського Союзу та держав-членів Європейського Союзу.....	79
2.3.3. Досвід окремих держав, які не є членами ЄС.....	89
2.4. Національне регулювання обігу віртуальних активів як нормативна основа кримінально-правової політики: чинний стан і напрями реформування	100
2.5. Місце кримінально-правових засобів у механізмі охорони обігу віртуальних активів та ризик-орієнтовані засади запобігання кримінальним правопорушенням	108
Висновки до розділу 2.....	113
РОЗДІЛ 3. КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ, ЩО ВЧИНЯЮТЬСЯ ЩОДО ВІРТУАЛЬНИХ АКТИВІВ АБО З ЇХ ВИКОРИСТАННЯМ.....	116
3.1. Віртуальні активи в системі об’єктів та предметів кримінальних правопорушень	116
3.2. Загальна характеристика та типологія кримінальних правопорушень у сфері віртуальних активів.....	123

3.3. ТИПОВІ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ, ЩО ПОВ'ЯЗАНІ З ВІРТУАЛЬНИМИ АКТИВАМИ.....	129
3.3.1. Легалізація (відмивання) майна, одержаного злочинним шляхом, із використанням віртуальних активів.....	129
3.3.2. Фінансування тероризму із використанням віртуальних активів...	135
3.3.3. Шахрайство та кримінальні правопорушення проти власності, предметом або засобом яких є віртуальні активи	138
3.3.4. Незаконне збагачення та корупційні правопорушення, пов'язані з віртуальними активами	143
3.3.5. Кіберкримінальні правопорушення (Розділ XVI КК України) та кримінально-правова охорона безпеки інфраструктури ринку віртуальних активів.....	149
3.3.6. Використання віртуальних активів в організації азартних та онлайн-ігор	154
Висновки до розділу 3.....	159
РОЗДІЛ 4. ВЗАЄМОЗВ'ЯЗОК КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ВІРТУАЛЬНИХ АКТИВІВ З КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОЮ ТА КРИМІНАЛЬНО-ВИКОНАВЧОЮ ПОЛІТИКОЮ.....	162
4.1. Особливості кримінального процесуального доказування, досудового розслідування та укладення угод у провадженнях, пов'язаних з віртуальними активами.....	162
4.2. Арешт, спеціальна конфіскація та звернення стягнення на віртуальні активи; виконання судових рішень щодо їх конфіскації.....	176
Висновки до розділу 4.....	189
ВИСНОВКИ	192
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	198
ДОДАТКИ.....	226

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АРМА - Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів

БЕБ - Бюро економічної безпеки України

ВА - віртуальні активи

ВАКС - Вищий антикорупційний суд

ДБР - Державне бюро розслідувань

Держфінмоніторинг - Державна служба фінансового моніторингу України

ДПС - Державна податкова служба України

Європол - Європейське поліцейське управління (Europol)

ЄДРСР - Єдиний державний реєстр судових рішень

ЄС - Європейський Союз

ЄЦБ - Європейський центральний банк

ЗВА(ВЦ) - забезпечений віртуальний актив, забезпечений валютними цінностями (за Законом України № 2074-IX)

ЗВА(ФІ) - забезпечений віртуальний актив, забезпечений цінним папером або деривативним фінансовим інструментом (за Законом України № 2074-IX)

Інтерпол - Міжнародна організація кримінальної поліції (INTERPOL)

КК України - Кримінальний кодекс України

КПК України - Кримінальний процесуальний кодекс України

КПП - кримінально-правова політика

МВС - Міністерство внутрішніх справ України

НАБУ - Національне антикорупційне бюро України

НАЗК - Національне агентство з питань запобігання корупції

НБУ - Національний банк України

НКЦПФР - Національна комісія з цінних паперів та фондового ринку

нмдг - неоподатковуваний мінімум доходів громадян

НС(Р)Д - негласні слідчі (розшукові) дії

ОБСЄ - Організація з безпеки і співробітництва в Європі

ОГП - Офіс Генерального прокурора

ОРД - оперативно-розшукова діяльність

ОРЗ - оперативно-розшукові заходи

ПВК/ФТ - протидія відмиванню коштів та фінансуванню тероризму

ПКУ - Податковий кодекс України

ППВА - постачальники послуг, пов'язаних з оборотом віртуальних активів (за Законом України № 2074-IX; відповідник VASP за термінологією ФАТФ)

ПФР - підрозділ фінансової розвідки (financial intelligence unit, FIU)

САП - Спеціалізована антикорупційна прокуратура

СБУ - Служба безпеки України

СРД - слідчі (розшукові) дії

СРО - саморегулювальна організація (з протидії відмиванню коштів)

США - Сполучені Штати Америки

ФАТФ - Група з розроблення фінансових заходів боротьби з відмиванням коштів (FATF)

ЦК України - Цивільний кодекс України

4AMLD - Fourth Anti-Money Laundering Directive - Четверта директива ЄС про запобігання відмиванню коштів (Директива (ЄС) 2015/849)

5AMLD - Fifth Anti-Money Laundering Directive - П'ята директива ЄС про запобігання відмиванню коштів (Директива (ЄС) 2018/843)

AMF - Autorité des marchés financiers - Управління фінансових ринків (Франція)

AMLA - Authority for Anti-Money Laundering and Countering the Financing of Terrorism - Орган ЄС з протидії відмиванню коштів та фінансуванню тероризму (Регламент (ЄС) 2024/1620)

AMLD6 - Sixth Anti-Money Laundering Directive - Шоста директива ЄС про запобігання відмиванню коштів (Директива (ЄС) 2024/1640)

AMLR - Anti-Money Laundering Regulation - Регламент ЄС про запобігання відмиванню коштів (Регламент (ЄС) 2024/1624)

ART - asset-referenced token - токен, прив'язаний до активів (за Регламентом MiCA)

BaFin - Bundesanstalt für Finanzdienstleistungsaufsicht - Федеральне управління фінансового нагляду ФРН

CASP - crypto-asset service provider - постачальник послуг, пов'язаних з обігом криптоактивів (за Регламентом MiCA)

CBDC - central bank digital currency - цифрова валюта центрального банку

CEX - centralized exchange - централізована криптобіржа

CSMAD - Criminal Sanctions for Market Abuse Directive - Директива ЄС про кримінальні санкції за зловживання на ринку (Директива 2014/57/ЄС)

DASP - digital asset service provider - постачальник послуг, пов'язаних з цифровими активами (Франція, Закон RASTE)

DeFi - decentralized finance - децентралізовані фінанси

DEX - decentralized exchange - децентралізована криптобіржа

DLT - distributed ledger technology - технологія розподіленого реєстру

DORA - Digital Operational Resilience Act - Регламент ЄС про цифрову операційну стійкість фінансового сектору (Регламент (ЄС) 2022/2554)

EBA - European Banking Authority - Європейське банківське управління

EIOPA - European Insurance and Occupational Pensions Authority - Європейське управління з питань страхування та професійних пенсій

EMD2 - Second Electronic Money Directive - Друга директива ЄС про електронні гроші (Директива 2009/110/ЄС)

EMT - e-money token - токен електронних грошей (за Регламентом MiCA)

ESA - European Supervisory Authorities - європейські наглядові органи (EBA, ESMA, EIOPA)

ESMA - European Securities and Markets Authority - Європейське управління з цінних паперів та ринків

EULA - End User License Agreement - ліцензійна угода з кінцевим користувачем

Europol - European Union Agency for Law Enforcement Cooperation - Агентство Європейського Союзу зі співробітництва правоохоронних органів

FATF - Financial Action Task Force - див. ФАТФ

FCA - Financial Conduct Authority - Управління з фінансового регулювання та контролю (Велика Британія)

FinCEN - Financial Crimes Enforcement Network - Мережа боротьби з фінансовими злочинами (США)

FINMA - Swiss Financial Market Supervisory Authority - Швейцарська служба нагляду за фінансовими ринками

FINTRAC - Financial Transactions and Reports Analysis Centre of Canada - Центр аналізу фінансових операцій та звітів (Канада)

FSB - Financial Stability Board - Рада з фінансової стабільності

ICO - initial coin offering - первинна пропозиція (розміщення) монет

IFRIC - International Financial Reporting Interpretations Committee - Комітет з тлумачень міжнародних стандартів фінансової звітності

I-GRIP - INTERPOL Global Rapid Intervention of Payments - механізм Інтерполу швидкого реагування на платежі

INTERPOL - International Criminal Police Organization - Міжнародна організація кримінальної поліції

IOSCO - International Organization of Securities Commissions - Міжнародна організація комісій з цінних паперів

IP - Internet Protocol (address) - (мережева) адреса за інтернет-протоколом

KWG - Kreditwesengesetz - Закон ФРН про банківську діяльність

KYC - know your customer - «знай свого клієнта» (ідентифікація та верифікація клієнта)

MAR - Market Abuse Regulation - Регламент ЄС про зловживання на ринку (Регламент (ЄС) № 596/2014)

MiCA - Markets in Crypto-Assets Regulation - Регламент ЄС про ринки криптоактивів (Регламент (ЄС) 2023/1114)

MiFID II - Markets in Financial Instruments Directive II - Директива ЄС про ринки фінансових інструментів (Директива 2014/65/ЄС)

MMORPG - massively multiplayer online role-playing game - масова багатокористувацька рольова онлайн-гра

MONEYVAL - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - Комітет експертів Ради Європи з оцінки заходів протидії відмиванню коштів

NCA - National Crime Agency - Національне агентство з боротьби зі злочинністю (Велика Британія)

NFT - non-fungible token - невзаємозамінний токен

OFAC - Office of Foreign Assets Control - Управління контролю за іноземними активами Міністерства фінансів США

OSINT - open-source intelligence - розвідка на основі відкритих джерел

OTC - over-the-counter - позабіржовий (провайдер послуг з обміну криптоактивів)

P2P - peer-to-peer - одноранговий (прямий) обмін між користувачами

PRISMA - Preferred Reporting Items for Systematic Reviews and Meta-Analyses - стандарт звітування систематичних оглядів та метааналізів

PSD2 - Second Payment Services Directive - Друга платіжна директива ЄС (Директива (ЄС) 2015/2366)

RegTech - regulatory technology - регуляторні технології

RMT - real money trading - торгівля (внутрішньоігровими цінностями) за реальні гроші

SDN - Specially Designated Nationals and Blocked Persons - список спеціально позначених і заблокованих осіб (ведеться OFAC, США)

SupTech - supervisory technology - наглядові технології

ToS - Terms of Service - умови обслуговування (онлайн-сервісу)

Travel Rule - «правило подорожі» - вимога супроводження переказів коштів і криптоактивів інформацією про сторони (Регламент (ЄС) 2023/1113)

TXID - transaction identifier - ідентифікатор транзакції

UNODC - United Nations Office on Drugs and Crime - Управління ООН з наркотиків і злочинності

VASP - virtual asset service provider - постачальник послуг, пов'язаних з обігом віртуальних активів

VFA - Virtual Financial Assets - віртуальні фінансові активи (Республіка Мальта)

ВСТУП

Обґрунтування вибору теми дослідження. Поява та стрімке поширення віртуальних активів стали одним із найпомітніших проявів цифрової трансформації економічних відносин. Побудовані на технології розподіленого реєстру, такі активи забезпечують швидкий, транскордонний і значною мірою анонімний обіг цінностей поза традиційною банківською інфраструктурою, що зумовлює як їх економічну привабливість, так і підвищену кримінологічну вразливість. Віртуальні активи дедалі частіше виступають предметом, знаряддям чи засобом протиправного впливу у механізмі вчинення різноманітних кримінальних правопорушень (від легалізації (відмивання) доходів та фінансування тероризму до шахрайства, незаконного збагачення й комп'ютерних кримінальних правопорушень).

Транснаціональна і технологічно складна природа віртуальних активів зумовлює те, що національна кримінально-правова політика у відповідній сфері не може формуватися ізольовано. На рівні Європейського Союзу створено комплексний регуляторний каркас, насамперед, Регламент (ЄС) 2023/1114 (MiCA), а також пов'язані акти у сфері протидії відмиванню коштів і забезпечення цифрової операційної стійкості; на міжнародному рівні діють стандарти Групи з розроблення фінансових заходів боротьби з відмиванням коштів (ФАТФ), Ради з фінансової стабільності та Міжнародного валютного фонду. Ці наднаціональні орієнтири задають зміст бланкетних заборон і визначають межі допустимої криміналізації, що актуалізує потребу їх системного врахування у вітчизняній доктрині та законодавстві.

Україна перебуває у стані незавершеної реформи регулювання обігу віртуальних активів. Профільний Закон України «Про віртуальні активи» № 2074-IX ухвалено, проте він не набрав чинності, а його запровадження пов'язується з оновленням податкового законодавства та адаптацією регуляторної моделі до Регламенту MiCA. За таких умов кримінально-правова охорона відповідних відносин спирається переважно на загальні норми Кримінального кодексу України та на регулятивне законодавство у сфері запобігання та протидії легалізації (відмиванню) доходів, що породжує суттєві

проблеми кваліфікації, доказування та виконання судових рішень. Це робить актуальним наукове осмислення кримінально-правової політики у сфері забезпечення охорони віртуальних активів як цілісного явища, що поєднує матеріальну, процесуальну та кримінально-виконавчу складові.

Загальнотеоретичні питання кримінально-правової політики розроблялися у працях таких вітчизняних учених, як П. Л. Фріс, В.І.Борисов, І. В. Козич, Ю. В. Кернякевич-Танасійчук та інших. Водночас комплексні дослідження кримінально-правової політики саме у сфері забезпечення охорони віртуальних активів, які системно враховували б право Європейського Союзу, міжнародні стандарти та перехідний стан національного регулювання, на сьогодні відсутні.

Зв'язок роботи з науковими програмами, планами, темами. Тему дисертації затверджено Вченою радою Прикарпатського національного університету імені Василя Стефаника (протокол № 9 від 01 листопада 2022 року). Дисертацію виконано в межах науково-дослідної теми «Політика у сфері боротьби зі злочинністю в умовах євроінтеграції» (державний реєстраційний номер 0125U000669) на кафедрі політики у сфері боротьби зі злочинністю та кримінального права Навчально-наукового юридичного інституту Карпатського національного університету імені Василя Стефаника.

Мета і завдання дослідження. Метою дослідження є комплексне визначення засад формування та реалізації кримінально-правової політики у сфері забезпечення охорони віртуальних.

Для досягнення поставленої мети визначено такі завдання:

- з'ясувати генезу, економіко-технологічні передумови та міждисциплінарний зміст поняття «віртуальні активи» й сформулювати визначення віртуального активу для цілей кримінально-правового дослідження;
- розмежувати віртуальні активи із суміжними поняттями (цифрові речі, цифрові активи, криптоактиви, криптовалюта, віртуальні валюти, гроші, цінні папери, фінансові інструменти) та визначити їх правову природу як предмета кримінально-правової охорони;

- систематизувати класифікації віртуальних активів за законодавством України і Європейського Союзу та доктриною й розкрити самостійне кримінально-правове значення такої класифікації;
- проаналізувати стан наукової розробленості проблеми та визначити методологічні засади дослідження кримінально-правової політики у сфері забезпечення охорони віртуальних активів;
- сформулювати поняття, виокремити ознаки й розкрити структуру кримінально-правової політики у сфері забезпечення охорони віртуальних активів та встановити її джерела;
- охарактеризувати міжнародні стандарти регулювання й охорони віртуальних активів, право Європейського Союзу та досвід окремих держав як орієнтири національної кримінально-правової політики;
- оцінити чинний стан національного регулювання обігу віртуальних активів як нормативну основу кримінально-правової політики й окреслити напрями його реформування з урахуванням Регламенту (ЄС) 2023/1114 (MiCA);
- визначити місце кримінально-правових засобів у механізмі охорони обігу віртуальних активів та розкрити ризик-орієнтовані засади запобігання відповідним кримінальним правопорушенням;
- встановити місце віртуальних активів у системі об'єктів та предметів кримінальних правопорушень;
- здійснити загальну характеристику та запропонувати типологію кримінальних правопорушень, що вчиняються щодо віртуальних активів або з їх використанням (легалізація (відмивання) доходів, фінансування тероризму та обхід санкцій, шахрайство, незаконне збагачення, кіберправопорушення, незаконні азартні ігри тощо);
- виявити взаємозв'язки між кримінально-правовою, кримінально-процесуальною та кримінально-виконавчою політикою в сфері забезпечення охорони віртуальних активів.

Об'єкт дослідження - суспільні відносини, що виникають у сфері формування та реалізації кримінально-правової політики щодо забезпечення

охорони правомірного створення, обігу й використання віртуальних активів та охорони майнових прав учасників відповідного ринку.

Предмет дослідження - кримінально-правова політика у сфері забезпечення охорони віртуальних активів.

Методи дослідження. Методологічний інструментарій дослідження визначено його об'єктом, метою та завданнями. Основою виступає діалектичний метод, застосований у дослідженні наскрізно для розкриття різноманітного й динамічного характеру віртуальних активів як об'єкта кримінально-правової охорони та для дослідження кримінально-правової політики в її розвитку й внутрішніх зв'язках. Онтологічний підхід використано при з'ясуванні природи віртуального активу, субстратом якого є інформація, при розмежуванні його із суміжними поняттями (підрозділи 1.1, 1.2) та встановленні місця активу в системі предметів кримінальних правопорушень (підрозділ 3.1). Історико-правовий метод застосовано для відтворення генези поняття та правового статусу віртуальних активів (підрозділ 1.1). Системно-структурний метод використано при розкритті структури кримінально-правової політики (підрозділ 2.2) і побудові багатовимірної типології кримінальних правопорушень (підрозділ 3.2), а метод класифікації (групування) - для систематизації віртуальних активів та з'ясування її кримінально-правового значення (підрозділ 1.3). Порівняльно-правовий (компаративістський) метод став основним при дослідженні міжнародних стандартів, права Європейського Союзу й досвіду окремих держав та при оцінці напрямів національного реформування (підрозділи 2.3, 2.4). Формально-юридичний (догматичний) метод і метод юридичного тлумачення використано при аналізі чинного й перспективного законодавства, кваліфікації конкретних складів кримінальних правопорушень (розділ 3) та дослідженні процесуальних і кримінально-виконавчих механізмів (розділ 4). Методи аналізу й синтезу, індукції та дедукції, а також узагальнення наукових джерел застосовано для оцінки стану наукової розробленості проблеми (підрозділ 2.1) і формулювання загальних висновків.

Застереження щодо використання допоміжних цифрових інструментів. Під час підготовки дисертації як допоміжний засіб використано інструмент штучного інтелекту (Claude, розробник — компанія Anthropic) для редагування граматики та стилю, а також опрацювання джерел іноземними мовами. Зазначений інструмент не використовувався для генерування наукових результатів чи висновків.

Наукова новизна одержаних результатів полягає в тому, що дисертація є комплексним монографічним дослідженням кримінально-правової політики у сфері забезпечення охорони віртуальних активів, виконаним з урахуванням права Європейського Союзу (насамперед Регламенту (ЄС) 2023/1114 (MiCA)), міжнародних стандартів (ФАТФ, FSB, МВФ) та перехідного стану національного регулювання, за якого профільний Закон України «Про віртуальні активи» № 2074-IX залишається ухваленим, але не введеним у дію. До положень, що мають наукову новизну, зокрема, належать такі:

уперше:

- сформульовано авторське поняття кримінально-правової політики у сфері забезпечення охорони віртуальних активів як самостійного сегмента політики у сфері боротьби зі злочинністю та розкрито її структуру через об'єкт (суспільні відносини правомірного створення, обігу й використання віртуальних активів і охорони майнових прав учасників ринку), суб'єктів формування і реалізації, систему принципів та засоби; визначено її основні ознаки - подвійну родову належність, похідний (субсидіарний) характер щодо регулятивного законодавства з переважно бланкетною природою заборон, міжнародну та європейську зумовленість, технологічну складність об'єкта й динамічність;

- обґрунтовано, що, на відміну від традиційних сфер кримінально-правової охорони, де визначальними джерелами політики виступають внутрішні соціально-економічні чинники й національна правова традиція, у сфері віртуальних активів первинним джерелом є зовнішній - наднаціональний - нормативний і досвідний масив (право Європейського Союзу та міжнародні стандарти), що зумовлено транскордонною природою самих активів;

- обґрунтовано самостійне кримінально-правове значення класифікації віртуальних активів: доведено, що вид активу безпосередньо впливає на встановлення предмета та кваліфікацію відповідних правопорушень - забезпечений актив тяжіє до предмета злочинів проти власності; незабезпечений породжує проблему визначення предмета й доказування вартості; фінансові активи окреслюють сферу посягань, пов'язаних із ринками капіталу; платіжні та анонімні активи становлять підвищений ризик використання як засобу легалізації (відмивання) доходів і фінансування тероризму; поділ на централізовані та децентралізовані активи визначає коло суб'єктів фінансового моніторингу й реальні межі охорони;

- комплексно обґрунтовано положення про нерозривний взаємозв'язок матеріальної, процесуальної та кримінально-виконавчої складових кримінально-правової політики у досліджуваній сфері: доведено, що матеріальна заборона, не забезпечена дієвими процесуальними та виконавчими інструментами виявлення, фіксації, доказування, конфіскації й реалізації активу, залишається декларативною, а технічні прогалини, що паралізують звернення стягнення на віртуальні активи у виконавчому провадженні, тотожно паралізують і кримінально-виконавчу реалізацію їх конфіскації;

удосконалено:

- понятійний апарат щодо віртуальних активів в контексті об'єкта кримінально-правової охорони в рамках функціонування кримінально-правової політики. Відтак, запропоновано визначення віртуального активу (для потреб дослідження кримінально-правової політики) та підтримано пропонування в літературі ланцюг «цифрові речі (цифрові активи) - віртуальні активи - криптоактиви - криптовалюта» з розмежуванням віртуальних активів від нематеріальних благ та інформації, грошей і засобів платежу, цінних паперів і фінансових інструментів, робіт і послуг;

- систематизацію кримінальних правопорушень, що вчиняються щодо віртуальних активів або з їх використанням, і внаслідок цього запропоновано їх поділ на види за різними критеріями;

дістали подальшого розвитку:

- положення про гармонізацію національної моделі регулювання й охорони віртуальних активів із правом Європейського Союзу - щодо дефініції, видової типології та режиму постачальників послуг - як необхідну передумову коректної кримінально-правової кваліфікації за умов незавершеності профільної реформи;

- пропозиції щодо адаптації матеріального, процесуального та кримінально-виконавчого законодавства до природи віртуальних активів, зокрема, щодо матеріально-правових підстав конфіскації віртуальних активів (поняття «майно» у статті 59 Кримінального кодексу України).

Практичне значення одержаних результатів полягає в можливості їх використання: у нормотворчій діяльності - під час доопрацювання профільного законодавства про віртуальні активи та його синхронізації з Регламентом MiCA, а також удосконалення матеріальних, процесуальних і кримінально-виконавчих норм щодо охорони віртуальних активів, їх арешту, спеціальної конфіскації та реалізації; у правозастосовній діяльності - для коректної кваліфікації кримінальних правопорушень, що вчиняються щодо віртуальних активів або з їх використанням, та для вдосконалення практики доказування й виконання судових рішень; у науково-дослідній сфері - як підґрунтя для подальших досліджень кримінально-правової політики у відповідній сфері; в освітньому процесі - під час викладання навчальних дисциплін кримінально-правового циклу та спеціальних курсів, присвячених протидії злочинності.

Апробація результатів дослідження. Основні положення, висновки та рекомендації дисертації оприлюднено на науково-практичних конференціях: щорічній Всеукраїнській науково-практичній конференції здобувачів освіти та молодих вчених «Вдосконалення правового регулювання: погляд молодих науковців» (м. Івано-Франківськ, 9 травня 2025 року) та Всеукраїнській науково-практичній конференції «Договір як універсальна форма правового регулювання», присвяченій пам'яті академіка Національної академії правових наук України, доктора юридичних наук, професора В. В. Луця (м. Івано-Франківськ, 17 квітня 2026 року).

Публікації. Результати дисертації відображено у 5 наукових публікаціях, з яких 3 - статті у наукових фахових виданнях України з юридичних наук (категорія «Б»), 2 - тези доповідей на всеукраїнських науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з анотації, переліку умовних позначень і скорочень, вступу, чотирьох розділів, що об'єднують тринадцять підрозділів (окремі з яких поділено на пункти), висновків, списку використаних джерел і додатку. Загальний обсяг дисертації становить 227 сторінок, з них основного тексту - 182 сторінки. Список використаних джерел налічує 220 найменувань.

РОЗДІЛ 1.

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПОНЯТІЙНІ ЗАСАДИ ДОСЛІДЖЕННЯ ВІРТУАЛЬНИХ АКТИВІВ ЯК ОБ'ЄКТА КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ

1.1. Генеза та міждисциплінарні аспекти поняття «віртуальні активи»

Дослідження кримінально-правової політики у сфері забезпечення охорони віртуальних активів неможливе без попереднього з'ясування того, що саме охороняється, тобто без встановлення сутності, генези та правової природи самого феномену віртуальних активів. Точність предмета кримінально-правової охорони безпосередньо залежить від точності вихідного поняття: помилка чи невизначеність на рівні дефініції неминуче відтворюється на рівні кваліфікації відповідних кримінальних правопорушень, оцінки розміру шкоди та доказування.

Методологічно необхідно одразу зробити наскрізне застереження щодо стану нормативної бази, у межах якої провадиться дослідження. Закон України «Про віртуальні активи» № 2074-IX, попри ухвалення 17 лютого 2022 року, не набрав чинності, оскільки його введення в дію прив'язане до прийняття змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами [1]; де-юре статус віртуальних активів наразі визначається функціональною дефініцією Закону № 361-IX і статтею 179-1 ЦК України, а перспективна модель регулювання вибудовується за зразком Регламенту МіСА та законопроекту № 10225-д. З огляду на це далі за текстом цей акт іменується нечинним Законом № 2074-IX, а його положення розглядаються як перспективна (*de lege ferenda*) модель - окрім випадків, коли нечинність акта має самостійне кваліфікаційне значення. Це означає, що станом на період дослідження чинне національне регулювання обігу віртуальних активів залишається фрагментарним, а єдина легальна дефініція віртуального активу, що має юридичну силу, міститься в законодавстві про фінансовий моніторинг. Водночас на рівні Європейського Союзу з 30 грудня 2024 р. набув

повного застосування Регламент (ЄС) 2023/1114 про ринки криптоактивів (MiCA) [2], який задає орієнтир для майбутньої національної моделі регулювання. Ці обставини обумовлюють дослідницьку рамку кримінально-правової політики в умовах переходу до європейської моделі регулювання і вимагають чіткого розмежування того, що в опрацьованих джерелах подається як чинне право, і того, що насправді є аналізом тексту нечинного закону або пропозицією *de lege ferenda*.

Віртуальні активи, передусім криптовалюти, є новітнім явищем, поява якого зумовлена не лише технологічним поступом, а й певними економічними та світоглядними передумовами. Як слушно зауважує В. Школьний, осягнення природи криптовалют потребує аналізу в контексті глобалізації, співвідношення приватних і публічних інтересів, а також тих ідейних течій, що передували появі децентралізованих цифрових грошей [3, с. 58]. Відсутність єдиного розуміння сутності криптовалюти простежується вже на рівні базових підходів: її трактують і як товар, і як платіжний засіб, і як розрахункову одиницю, і як нематеріальний цифровий актив, інвестиційний чи фінансовий актив, ба навіть як цінний папір [3, с. 59]. Ідейне коріння віртуальних активів сягає австрійської школи економіки: концепція денаціоналізації грошей, обґрунтована Ф. Хаєком і Л. фон Мізесом, передбачала можливість конкуренції приватних валют поза монополією держави на емісію, і саме ця ідея заклала світоглядну основу для появи криптовалют [3, с. 61-62]. Не менш важливим джерелом став рух криптоанархізму: «Маніфест криптоанархізму» Т. Мея (1988), а згодом праці П. Ладлоу та А. Нараянана сформулювали ідеали анонімності, децентралізації та публічної верифікованості, які згодом утілилися в архітектурі біткоїна [3, с. 62-63]. Показово, що сама етимологія складника «крипто» походить від давньогрецького *kruptós* - прихований, приватний, - що відображає закладену в основу технології ідею приватності [3, с. 62]. Таким чином, біткоїн увібрав у себе як економічні ідеї австрійської школи у вигляді конкуренції валют та обмеження державного втручання, так і світоглядні засади криптоанархізму - анонімність, децентралізацію та публічність [3, с. 63]. Не варто залишати поза увагою й суто економічний вимір генези: як зазначають

В. Савчук, Т. Собченко та В. Бойченко, віртуальні активи (криптовалюта) як явище з'явилися у 2009 р. - почасти як спроба протистояти негативним наслідкам світової фінансової кризи 2008 р. [4, с. 40]. Криптовалюта при цьому не є радикально новим продуктом: ідеться радше про динамічний розвиток сфери, що змінює фінансово-господарську діяльність і суспільні відносини. Цей економічний контекст пояснює, чому віртуальні активи від самого початку перебували на перетині приватноправового та публічно-правового регулювання, фінансового та технологічного знання.

Поява віртуальних активів була підготовлена тривалою еволюцією технологій цифрових грошей. Д. Погрібний реконструює цей шлях, вказуючи на низку попередників сучасного блокчейну: ще на початку 1980-х рр. Д. Чом запропонував концепцію «цифрової готівки» (digital cash) і технологію «сліпого підпису»; у 1997 р. А. Бек розробив механізм Hashcash; а у 1998 р. Н. Сабо описав bit gold, який нерідко називають безпосереднім попередником архітектури біткоїна [5, с. 3]. Технологія блокчейн уперше була реалізована саме в біткоїні як цифровий код, який неможливо дублювати, що й вирішило фундаментальну проблему подвійного витрачання у децентралізованих системах [5, с. 4]. Логічним завершенням цієї технологічної лінії стала поява власне біткоїна. С. Гончаренко докладно відтворює відповідну хронологію: у 2008 р. С. Накамото оприлюднив працю «Bitcoin: A Peer-to-Peer Electronic Cash System», у якій блокчейн постав як розподілена база даних - ланцюг блоків із криптографічним підтвердженням; 3 січня 2009 р. було згенеровано перший, так званий генезис-блок, а 9 січня 2009 р. оприлюднено відкритий код [6, с. 152-153]. Ключова ідея Накамото полягала в тому, що валюта має регулюватися математичними законами, а не рішеннями урядів [6, с. 153]. Біткоїн виявився першою, але далеко не останньою криптовалютою: невдовзі з'явилися Namecoin, Litecoin, а згодом - Ethereum (2015) з його платформами для первинного розміщення монет, і загальна кількість криптовалют швидко перевищила дві тисячі [6, с. 154]. Технологічна сутність криптовалюти як «коду у великій книзі під назвою “блокчейн”», що за своєю природою подібний до бухгалтерської книги, підкреслюється і в інших джерелах [7, с. 222]. Розуміння

технологічної основи має безпосереднє значення для кримінально-правового дослідження: саме децентралізований і псевдонімний характер обігу, відсутність єдиного емітента та неможливість скасування транзакції визначають специфіку віртуальних активів і як предмета кримінальних правопорушень, і як засобу їх учинення, і як об'єкта доказування.

Центральною для понятійних засад дослідження є еволюція термінологічної тріади, у якій послідовно змінювалися домінантні поняття - «криптовалюта», «віртуальні активи» та «криптоактиви». Як показує Р. Самсін, історія терміна «криптовалюта» бере початок із квітня 2011 р., коли стаття Е. Грінберга у виданні Forbes «Crypto Currency» сприяла поширенню цього найменування [8, с. 214]. Уже у 2012 р. Європейський центральний банк у доповіді «Virtual Currency Schemes» запровадив у науковий обіг поняття «віртуальна валюта», а Звіт ФАТФ того ж року посилив цю термінологію [8, с. 214]. Поява нових криптопродуктів - інвестиційних токенів, стейблкоїнів, цифрових валют центральних банків, так званих квазікриптовалют, - які відрізнялися від класичних криптовалют, але позиціонувалися як такі, загострила потребу в узагальнювальному терміні [8, с. 215]. Поворотним моментом став 2018 рік, коли Група з розроблення фінансових заходів боротьби з відмиванням коштів (ФАТФ) замінила поняття «криптовалюта» на ширше «віртуальний актив» і запровадила супутню категорію постачальника послуг, пов'язаних з обігом віртуальних активів (VASP) [8, с. 215]. У 2019 р. у пояснювальній записці до Рекомендації 15 ФАТФ закріпила визначення віртуального активу як «цифрового вираження вартості, яким можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних або інвестиційних цілей» [9, с. 33]. Р. Самсін підтримує позицію А. Кудя про те, що саме надання Рекомендаціям ФАТФ статусу міжнародного стандарту змістило фокус світового регулювання з «криптовалюти» на «віртуальний актив» [8, с. 215]. Водночас слід урахувати, що Рекомендації ФАТФ належать до «м'якого права» (soft law), а саме визначення віртуального активу в них не охоплює фіатних валют і цінних паперів, через що навіть у межах самих Рекомендацій воно не стало абсолютно універсальним [8, с. 215-]

216]. Третій етап термінологічної еволюції пов'язаний із правом Європейського Союзу: як зазначає Р. Самсін, із прийняттям Регламенту (ЄС) 2023/1114 (MiCA), ухваленого 31 травня 2023 р., відбувся перехід від поняття «віртуальні активи» до поняття «криптоактиви» (crypto-assets) [8, с. 218]. На підставі аналізу трансформації понять автор доходить висновку, що криптовалюта є видом віртуального активу, а поняття «віртуальні активи» і «криптоактиви» в сучасній правовій площині можна вважати фактично тотожними [8, с. 219-220]. Дещо інакше, через субординацію понять, вибудовує співвідношення С. Цукан: «віртуальні активи» та «цифрові активи» вживаються як синоніми; криптоактиви охоплюють криптовалюти; а віртуальні активи, своєю чергою, охоплюють криптоактиви [10, с. 615]. Для цілей цього дослідження прийнято саме таку, диференційовану модель, у якій віртуальні активи виступають родовим поняттям щодо криптоактивів (детальніше - підрозділ 1.2). При цьому еволюція термінології не означала повного витіснення попередніх понять: як підкреслюють В. Савчук, Т. Собченко та В. Бойченко, термін «віртуальні активи» вживають понад двадцять країн і чисельні міжнародні органи, проте поряд із ним зберігають актуальність - хоч і у вузькому значенні - поняття «віртуальна валюта», «криптовалюта», «токен-актив» [4, с. 43]. Перехід від терміна «валюта» до терміна «актив» автори пов'язують із технологічною еволюцією та використанням віртуальних активів для інвестиційних цілей [4, с. 42]. Ці спостереження узгоджуються з висновком про відсутність на міжнародному рівні єдиного, уніфікованого підходу до найменування досліджуваного феномену.

Еволюція національного правового статусу віртуальних активів в Україні відбувалася складно й суперечливо. Найбільш повну реконструкцію цього шляху пропонує Р. Самсін, який простежує генезу від кваліфікації криптовалюти як «грошового сурогату» до її визнання «цифровим вираженням вартості» [11, с. 210]. Вихідною точкою став Лист Національного банку України від 8 грудня 2014 р. № 29-208/72899, у якому Bitcoin було кваліфіковано як грошовий сурогат без забезпечення, обіг якого фактично заборонявся з огляду на положення Закону України «Про Національний банк

України» [11, с. 210]. Уже у 2017 р. спільна заява фінансових регуляторів дещо змінила цю позицію, констатувавши, що криптовалюта не має ознак грошового сурогату, оскільки в неї немає ознак документа, емітента та визначеної мети виготовлення, однак і не вписується в жодну з усталених правових категорій - вона не є ні грошима, ні валютою, ні електронними грошима, ні цінними паперами [11, с. 210-211]. Особливе значення для термінологічної генези має проєкт розпорядження Кабінету Міністрів України від 25 жовтня 2018 р. про схвалення Концепції державної політики у сфері віртуальних активів: за спостереженням Р. Самсіна, саме в цьому документі вперше в українському правовому полі з'явилися терміни «віртуальні валюти» та «віртуальні активи» [11, с. 211]. Подальша невизначеність статусу посилилася після того, як 22 березня 2018 р. НБУ відкликав свій лист 2014 р., унаслідок чого правовий статус криптовалюти знову став незрозумілим, що підтвердила і консультація Державної фіскальної служби від 25 січня 2019 р. [11, с. 212]. Переломним моментом стало ухвалення Закону України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 6 грудня 2019 р. № 361-IX [12], який, за оцінкою Р. Самсіна, став справжнім проривом: у ньому віртуальний актив уперше було визначено на рівні закону як «цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних або інвестиційних цілей», що відповідає визначенню ФАТФ [11, с. 213]. Саме ця дефініція, як зазначає С. Гончаренко, є на сьогодні чинною легальною дефініцією віртуального активу в українському законодавстві, оскільки вона міститься у законі, що набув чинності, на відміну від профільного закону [6, с. 155-156].

Профільний Закон України «Про віртуальні активи» від 17 лютого 2022 р. № 2074-IX запропонував іншу, цивілістично орієнтовану дефініцію: віртуальний актив визначено як нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі [13, с. 74]. Однак, як наголошує О. Ушинкіна, запропонований у цьому Законі поділ віртуальних активів на забезпечені та незабезпечені є незвичним для світової

практики [13, с. 74]. Нечинність профільного закону прямо й коректно фіксується в спеціалізованій обліково-правовій літературі: Л. Могил прямо зазначає, що прийнятий у 2022 році Закон України «Про віртуальні активи» досі не набрав чинності, а обіг криптовалюти в Україні досі не має належного правового врегулювання [14, с. 168]. Аналогічно Т. Ковальова та І. Хорошилова констатують, що відповідний Закон розроблено і прийнято, але не введено в дію, а його запуск відкладено у зв'язку з необхідністю внесення змін до Податкового кодексу України [15, с. 37]. Така ситуація створює характерну колізію двох легальних визначень, що існують паралельно: «функціонального» визначення Закону № 361-IX, побудованого через здатність до обігу та цілі використання, і «цивільністичного» визначення Закону № 2074-IX, побудованого через категорію нематеріального блага. На цю розбіжність визначень уже на етапі формування нормативної бази звертає увагу С. Цукан [10, с. 614]. Для кримінально-правового дослідження ця двоїстість має принципове значення, оскільки від обраної дефініції залежить, як саме віртуальний актив кваліфікуватиметься у структурі складу кримінального правопорушення.

Питання про правову природу віртуальних активів залишається найбільш дискусійним у доктрині й має пряме значення для встановлення предмета кримінально-правової охорони. В. Мілаш характеризує законодавче визначення віртуального активу як гетерогенне: воно дозволяє розглядати віртуальний актив одночасно як цифровий еквівалент вартості для платіжних цілей, як об'єкт віртуальної торгівлі, тобто товар у цифровому форматі, та як інструмент для інвестиційних цілей [16, с. 10]. При цьому авторка чітко відмежовує криптовалюту від електронних грошей, указуючи, що криптовалюта не є електронними грошима в розумінні відповідного законодавства [16, с. 11]. Доктринальна дискусія загострюється довкола питання, чи є віртуальний актив суто нематеріальним благом, чи його слід визнати особливим видом майна. С. Аксюков критикує кваліфікацію віртуального активу виключно як нематеріального блага, вважаючи її хибною, і обстоює визнання віртуального активу особливим видом майна - цифровим майновим активом [17, с. 261-262]. Свою позицію автор аргументує практичними проблемами правозастосування,

які виникають через немайнову природу: ускладнюється застосування інституту застави та норм про банкрутство [17, с. 262]. Цей погляд резонує з висновком Т. Дмитренко, яка, спираючись на стандарти бухгалтерського обліку, доходить висновку, що криптовалюта як нематеріальний актив водночас визнається майном за цивільним і господарським правом та товаром за податковим правом, а на саму криптовалюту поширюється право власності [18, с. 130-134]. Особливо ґрунтовний аналіз природи віртуальних активів пропонують В. Савенкова та Б. Вихристенко у новітньому дослідженні: автори наголошують, що головною характеристикою віртуального активу є те, що при його переказі не передаються дані про права вимоги - сама інформація і є активом [19, с. 139-140]. Вони фіксують важливу новелу цивільного законодавства - віднесення віртуальних активів до цифрових речей у відповідних положеннях Цивільного кодексу України [19, с. 141-142], - водночас критично оцінюють концепцію цифрових речей і доходять самостійного висновку про необхідність виділення віртуальних активів як майна *sui generis* з власною дефініцією [19, с. 142-143]. Прикметно, що вони розрізняють підвиди віртуальних активів за критерієм наявності прав вимоги: децентралізовані активи без емітента та забезпечення, такі як Bitcoin і Ethereum, протиставляються стейблкоїнам і токенам, прив'язаним до активів, які посвідчують права вимоги до емітента [19, с. 137-138]. Дискусійним залишається і саме найменування феномену. С. Грицай піддає критиці дефініцію «віртуальний актив» у Законі № 2074-IX, указуючи, що вона не виражає галузевої, фінансової належності, не цілком відповідає усталеному розумінню слова «актив» у стандартах фінансової звітності, а за своєю природою описуване явище ближче до технології [20, с. 315-316]. На цій підставі автор пропонує альтернативний термін - «віртуальні фінансові технології» [20, с. 316-317]. В іншій праці той самий автор, аналізуючи цивілістичну природу віртуального активу, доходить висновку, що за чинним станом законодавства віртуальний актив найближче стоїть до категорії «інформація» в розумінні відповідної статті Цивільного кодексу України [21, с. 248]. Хоча пропозиція замінити усталений термін навряд чи може бути

підтримана з огляду на її розбіжність із міжнародною термінологією, вона є важливим свідченням неусталеності понятійного апарату й слугує аргументом на користь обережного, верифікованого використання термінів у дослідженні.

Поняття «віртуальні активи» формується на перетині кількох галузей знання, і його юридичне розуміння не може ігнорувати економічний, обліковий і фінансовий контексти. Водночас слід наголосити, що облікові та фінансово-економічні характеристики віртуальних активів використовуються в цьому дослідженні виключно для з'ясування сутності поняття, а не як підстава для кримінально-правової кваліфікації: економічні судження про вартість, волатильність чи способи обліку не визначають предмет кримінального правопорушення, хоча й допомагають зрозуміти його природу. Найбільш послідовно обліковий вимір розкривається через питання про те, до якого класу активів належить криптовалюта. Л. Могил демонструє, що криптовалюта може проявляти ознаки одразу кількох категорій - товарів, грошових коштів та їх еквівалентів, фінансових інструментів, інвестиційної нерухомості, нематеріальних активів, запасів [14, с. 168, 170]. Послідовно аналізуючи кожен з цих категорій, авторка доходить висновку, що криптовалюта не може бути віднесена до грошових коштів через відсутність фізичної форми, централізованого емітента та неможливість прямої конвертації у готівку, не може вважатися фінансовим інструментом, оскільки не створює зобов'язального права, що підтверджено й позицією Комітету з тлумачень міжнародних стандартів фінансової звітності 2019 р., і найбільш придатно кваліфікується як нематеріальний актив або, за умови утримання для продажу, як запаси - залежно від мети використання [14, с. 170-173]. Підсумковою для авторки є теза про превалювання економічної сутності над юридичною формою [14, с. 173]. Цей висновок поділяється в обліковій літературі майже одностайно. Т. Ковальова та І. Хорошилова зазначають, що більшість науковців розглядають віртуальні активи як нематеріальні активи; криптовалюта відповідає визначенню нематеріального активу, а в разі утримання для продажу обліковується як запаси, при цьому не може належати до грошей та фінансових активів [15, с. 38]. Аналогічно В. Панасюк, Х. Гальчак і В. Босий констатують,

що криптовалюта не підходить під класифікацію фінансових інструментів, оскільки на спотовому ринку відсутня сторона зобов'язання, однак може визнаватися нематеріальним активом або запасами [7, с. 226-227]. Найновіше комплексне дослідження В. Гавриленко, Ю. Крот, А. Ткаченко та А. Міщенка узагальнює, що в різних юрисдикціях віртуальні активи класифікують як цифрові гроші, майно, фінансові інструменти або новий клас нематеріальних ресурсів, а на рівні міжнародних стандартів за позицією 2019 р. вони визнаються нематеріальними активами або запасами залежно від мети утримання [22, с. 156, 162-163]. Ці облікові висновки опосередковано підтверджують доктринальну тезу про майнову природу віртуального активу і його придатність бути предметом злочинів проти власності.

Окремий вимір додає фінансово-правовий аналіз. В. Нікітін висуває важливу для нашого дослідження тезу про подвійність правової природи віртуальних активів: приватноправова оборотоздатність активу має співіснувати з публічно-правовим наглядом, причому ці виміри повинні не конкурувати, а взаємно підсилюватися [23, с. 493, 497-498]. Автор пропонує функціональну типологію ролей віртуальних активів, виокремлюючи інвестиційну, платіжну, інфраструктурну та комплаєнс-модуючу ролі [23, с. 493, 496]. Хоча ця типологія є авторською аналітичною конструкцією, вона має відповідну цінність для кримінально-правового дослідження, оскільки саме на стику приватного інтересу власника активу та публічного інтересу держави у прозорості й доброчесності фінансових потоків і виникає потреба в кримінально-правовій охороні.

Фінансовий контекст увиразнюється і через масштаб явища: за даними, наведеними у дослідженні В. Гавриленко та співавторів із посиланням на аналітичні платформи, станом на травень 2024 р. Україна посідала 18 місце у світі за рівнем володіння криптовалютою - близько 10,2 % населення мали цифрові активи [22, с. 156]. Подібні показники наводять і В. Панасюк, Х. Гальчак та В. Босий, указуючи, що станом на початок 2023 р. близько 10,3 % населення України володіли криптовалютою [7, с. 224-225]. Ці дані, попри те що походять із приватних аналітичних джерел і потребують обережної

інтерпретації, переконливо свідчать про значне поширення віртуальних активів в Україні, а отже - про актуальність забезпечення їх належної кримінально-правової охорони.

Регламент (ЄС) 2023/1114 (MiCA), як це систематизовано у дослідженні В. Гавриленко та співавторів [22, с. 162], запровадив поділ криптоактивів на три основні категорії: токени електронних грошей (EMT), прив'язані до однієї офіційної валюти; токени, прив'язані до активів (ART), вартість яких підтримується через прив'язку до інших активів чи прав; та інші криптоактиви, що не належать до перших двох категорій, зокрема утилітарні токени. Ця класифікація відповідає й висновкам О. Ушинкіної, яка фіксує запроваджений MiCA перехід від «віртуальної валюти» до «криптоактиву» та виокремлює тенденцію класифікації віртуальних активів за функціональним критерієм [13, с. 71-72, 75]. Національний поділ віртуальних активів на забезпечені та незабезпечені, запроваджений Законом № 2074-IX, хоч і відрізняється від моделі MiCA, спирається на близький критерій - наявність прав вимоги. Як пояснюють В. Савчук, Т. Собченко та В. Бойченко, забезпечені віртуальні активи можуть посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав, тоді як незабезпечені активи, до яких належить більшість криптовалют, зокрема Bitcoin та Ethereum, не посвідчують жодних майнових чи немайнових прав [4, с. 43]. Цей поділ має пряме кримінально-правове значення, оскільки від наявності або відсутності прав вимоги залежить кваліфікація віртуального активу як предмета відповідних правопорушень та оцінка завданої шкоди.

Узагальнення розглянутих підходів дозволяє сформулювати визначення віртуальних активів, придатне для цілей цього кримінально-правового дослідження. При цьому враховано легальну дефініцію чинного Закону № 361-IX, побудовану за функціональним підходом через здатність до обігу та цілі використання; цивілістично орієнтовану дефініцію неінкорпорованого Закону № 2074-IX, побудовану через категорію нематеріального блага як об'єкта цивільних прав, що має вартість; орієнтир MiCA з його поняттям «криптоактив» та класифікацією; а також доктринальні висновки про майнову

природу віртуального активу та про інформацію як його субстрат. Для цілей дослідження кримінально-правової політики у відповідній сфері під **віртуальними активами** розуміється сукупність даних в електронній, цифровій формі, що має самостійну майнову цінність, обіг якої здійснюється в інформаційній системі на основі технології розподіленого реєстру або іншої подібної технології, може передаватися й використовуватися для платіжних або інвестиційних цілей і виступає об'єктом цивільних прав. Таке розуміння охоплює як незабезпечені віртуальні активи на кшталт Bitcoin та Ethereum, що не посвідчують прав вимоги, так і забезпечені віртуальні активи та токени, прив'язані до активів чи електронних грошей, що посвідчують відповідні права. Принциповою для кримінально-правового аналізу є та обставина, що віртуальний актив за своєю природою є майном особливого роду (*sui generis*), субстратом якого є **інформація**, а не носій права вимоги: *при переказі віртуального активу передається сама інформація, що становить актив, а не дані про права на інший об'єкт*.

1.2. Розмежування віртуальних активів із суміжними поняттями

Окреслене в попередньому підрозділі розуміння віртуальних активів (далі також - ВА) є вихідною точкою дослідження. Але для встановлення точного предмета кримінально-правової охорони необхідно відмежувати цей феномен від суміжних правових категорій, з якими його нерідко ототожнюють. Складність полягає в тому, що в нормативному, доктринальному та правозастосовному обігу паралельно функціонує ціла низка близьких, проте нетотожних термінів - «цифрові активи», «цифрові речі», «криптоактиви», «криптовалюти», «цифрові токени», «віртуальні валюти». І. Е. Щеглаков характеризує цей стан як своєрідний «герменевтичний хаос»: Кримінальний кодекс України (далі - КК України) оперує поняттям «криптовалюта», тоді як суміжні галузі вживають «цифрові речі», «віртуальні активи» та «криптоактиви», а судова практика за статтею 190 КК України ототожнює криптоактиви то з «коштами», то з «віртуальними активами», то з «криптовалютою» в межах однієї категорії справ [24, с. 226-230]. Для

кримінального права, що ґрунтується на принципі правової визначеності, така термінологічна неупорядкованість є неприйнятною, адже чіткість дефініцій і пріоритет видових понять над родовими становлять передумову правильної кваліфікації [24, с. 227-228]. Тому розмежування суміжних понять у цьому підрозділі підпорядковане не суто цивілістичному інтересу, а потребам подальшого кримінально-правового дослідження.

Вихідним пунктом розмежування слугує сама дефініція віртуального активу. Як зазначалося вище, чинне позитивне право України закріплює це поняття у пункті 13 частини першої статті 1 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», визначаючи віртуальний актив як цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних або інвестиційних цілей [12]. Натомість Закон України «Про віртуальні активи», який не набрав чинності, пропонує іншу, цивілістично навантажену конструкцію - нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі [1]. Розбіжність цих двох визначень і той факт, що друге залишається нечинним, є першим джерелом термінологічних труднощів: до набрання чинності профільним законом розмежування слід будувати на чинній дефініції, закріпленій у законодавстві про фінансовий моніторинг [24, с. 232-234].

Першим і чи не найважливішим є відмежування віртуальних активів від цифрових активів. О. О. Дмитрик критикує поширену тенденцію ототожнювати «віртуальний актив» і «цифровий актив», беручи синонімом до них «криптовалюту» чи «віртуальну валюту», і вважає такий підхід необ'єктивним, оскільки йдеться про різнопорядкові поняття [25, с. 249]. Дослідниця простежує й еволюцію міжнародної термінології: якщо у 2012 році Європейський центральний банк та Група з розроблення фінансових заходів боротьби з відмиванням коштів (ФАТФ) оперували поняттям «віртуальні валюти», то у 2018 році ФАТФ замінила його на «віртуальні активи», що згодом було

відображено в пояснювальній записці до Рекомендації 15 [25, с. 250]. Як семантичний критерій розмежування пропонується розрізняти значення прикметників: «цифровий» вказує на формат подання та зберігання інформації (код, числа, сигнали), тоді як «віртуальний» позначає імітований, симульований стан, що не належить до реального фізичного світу [25, с. 250-251]. Водночас власна змістова відмінність, яку обстоює О. О. Дмитрик (цифрові активи нібито мають реальну фінансову вартість і обмінюються на реальні гроші, а віртуальні активи відображають об'єкти у віртуальному світі й мають вартість, обмежену правилами платформи), є радше окремою авторською позицією, ніж усталеним підходом [25, с. 251].

Домінуюча в науці логіка співвідношення є, по суті, зворотною: цифровий актив (цифрова річ) розглядається як родове, ширше поняття, а віртуальний актив - як видове щодо нього. Є. Ю. Савченко, узагальнюючи позиції провідних міжнародних інституцій - Банку міжнародних розрахунків, Ради з фінансової стабільності, Європейського банківського органу та Міжнародного валютного фонду, - показує, що криптоактиви послідовно тлумачаться як вид цифрових активів приватного сектора, що ґрунтуються на криптографії та технології розподіленого реєстру [26, с. 92-93]. Цю ж логіку відображає й класифікація Регламенту (ЄС) 2023/1114 (MiCA), за яким криптоактив є цифровим представленням вартості або права, що може передаватися та зберігатися в електронному вигляді за допомогою технології розподіленого реєстру або подібної технології, і поділяється на три типи - токени електронних грошей (ЕМТ), токени з прив'язкою до активів (ART) та інші, зокрема утилітарні, токени; при цьому невзаємозамінні токени та криптоактиви, що є фінансовими інструментами, виведені за межі регламенту, а сам він побудований на принципі технологічної нейтральності [2; 26, с. 90-91]. На цій основі Є. Ю. Савченко доходить підсумкового співвідношення: цифрові речі та цифрові активи є родовими щодо віртуальних активів, віртуальні активи - видовими, а цифрові токени - водночас видовою категорією та формою існування віртуальних активів [26, с. 94-95]. Тотожну ієрархію обґрунтовує й І. Е. Щеглаков, вибудовуючи послідовний ланцюг від найширшого до

найвужчого поняття: цифрові речі - віртуальні активи - криптоактиви - криптовалюта [24, с. 240-241].

Ключовим є й співвідношення віртуальних активів із цивілістичною категорією речей. Перелік об'єктів цивільних прав, наведений у статті 177 Цивільного кодексу України (далі - ЦК України), є невичерпним і допускає існування інших, прямо не названих благ [27]. Законом України «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав», чинним з 3 вересня 2023 року, ЦК України доповнено статтею 179-1, яка визначає цифрову річ як благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність, і прямо відносить до цифрових речей віртуальні активи [27; 28]. Прикметно, що цю норму вміщено в Главі 13 Розділу III ЦК України («Речі. Майно»), а не серед нематеріальних благ, унаслідок чого законодавець фактично прирівняв правовий режим цифрових речей до режиму матеріальних речей, якщо інше не випливає із сутності такої речі [27]. Доктрина випередила це нормативне рішення: ще у 2022 році К. Г. Некіт обґрунтувала визнання віртуальних активів, зокрема криптовалют, різновидом цифрових речей через механізм правової фікції, наголошуючи, що вітчизняна концепція права власності вже допускає «безтілесні» об'єкти - електроенергію, газ, бездокументарні цінні папери, майнові права [29, с. 55]. Запропонована тоді *de lege ferenda* категорія згодом дістала пряме нормативне втілення у статті 179-1 ЦК України.

Особливої уваги потребує відмежування віртуальних активів від нематеріальних благ - тим паче, що саме до них відносить ВА нечинний профільний закон [1]. Є. Ю. Савченко аргументовано доводить, що віртуальні активи не охоплюються жодною з категорій нематеріальних благ, передбачених статтями 199-201 ЦК України [30, с. 303-306]. Вони не є результатом інтелектуальної, творчої діяльності, оскільки їх емісія не передбачає творчого процесу, а перехід права на віртуальний актив означає перехід тріади правомочностей власника на цифрову річ, а не майнових прав інтелектуальної власності [30, с. 304-305; 27]. Вони не є й інформацією у розумінні статті 200 ЦК України та статті 1 Закону України «Про інформацію»: на відміну від

інформації, віртуальні активи відчужувані від попереднього володільця, морально не старіють, існують лише в цифровій формі, не піддаються необмеженому тиражуванню та є вичерпними, будучи однозначно ідентифікованими в системі розподіленого реєстру; цінність інформації полягає в її змісті, тоді як криптовалюта є інформацією лише за формою [30, с. 305-306; 29, с. 54; 31]. Нарешті, віртуальні активи не належать і до особистих немайнових благ, яким властиві невідчужуваність, відсутність майнового характеру та «природне» походження [30, с. 306]. Звідси автор робить висновок про необхідність розглядати віртуальні активи як окремий об'єкт цивільних прав *sui generis* і пропонує *de lege ferenda* виключити з нечинного профільного закону положення про віднесення їх до нематеріальних благ [30, с. 307-308].

Системне зіставлення віртуальних активів із усім спектром об'єктів приватноправових відносин здійснює В. Ю. Легенько. Відштовхуючись від легального поняття «активів» (за статтею 1 Закону про фінансовий моніторинг це кошти, у тому числі електронні гроші, інше майно, майнові та немайнові права), автор послідовно порівнює віртуальні активи з речами, грошима, цінними паперами, роботами і послугами, нематеріальними благами та інформацією [32, с. 130; 12]. Зокрема, віртуальні активи не можуть бути віднесені до робіт чи послуг, бо роботи дають матеріальний результат, а послуги - нематеріальний результат, що споживається одразу [32, с. 132]. Від інформації їх відмежовує вичерпність: платіжні токени мають обмежену емісію, а невзаємозамінні токени є унікальними, тоді як інформації властива невичерпність [32, с. 131]. Симптоматичним є підсумок дослідника: значну частину віртуальних активів залежно від їх категорії можна співвіднести або з цінними паперами, або із засобом платежу, проте український законодавець обрав інший шлях, фактично прирівнявши всі віртуальні активи до речей через статтю 179-1 ЦК України за відсутності спеціального регулювання [32, с. 132-133].

Найгострішим у практичному вимірі є співвідношення віртуальних активів із грошима та засобами платежу. Частина сьома статті 4 нечинного профільного закону встановлює, що віртуальні активи не є засобом платежу на

території України та не можуть бути предметом обміну на майно (товари), роботи (послуги) [1]. С. О. Грицай, аналізуючи цю заборону, демонструє її умовність: попри декларацію, фактичні розрахунки віртуальними активами видаються можливими через механізми еквайрингу та обміну за участю постачальників послуг, пов'язаних з оборотом віртуальних активів [33, с. 132-135]. Слід, однак, наголосити, що цей автор оперує положеннями профільного закону як чинними, тоді як їх належить сприймати лише як характеристику нечинної, перспективної моделі, а *de lege lata* правовий статус віртуальних активів визначається чинним законодавством. Власне легального визначення «грошових коштів» чинне право не містить: стаття 3 Закону України «Про платіжні послуги» розкриває кошти через форму їх існування - готівкову та безготівкову [35], а стаття 2 Закону України «Про банки і банківську діяльність» визначає кошти як гроші у національній або іноземній валюті чи їх еквівалент [36]; гривня є законним платіжним засобом, а іноземна валюта застосовується у випадках, передбачених Законом України «Про валюту і валютні операції» [37; 34, с. 75-76]. Спираючись на функціональний підхід (гроші як міра вартості, засіб обміну та засіб збереження вартості), Л. А. Музика доходить висновку, що стейблкоїни, прив'язані до офіційної валюти, за своєю правовою, економічною та соціальною природою тяжіють до категорії грошових коштів, що узгоджується з підходом МіСА, який прирівнює режим таких стейблкоїнів до режиму електронних грошей [34, с. 76; 2]. Це, утім, доктринальне тлумачення з елементами *de lege ferenda*, а не позиція чинної норми.

Окремого розмежування потребують віртуальні активи й цінні папери та фінансові інструменти. Згідно зі статтею 8 Закону України «Про ринки капіталу та організовані товарні ринки», цінний папір посвідчує грошове або інше майнове право та існує в електронній або паперовій формі [38]. В. Ю. Легенько зауважує, що хоча віртуальний актив теж можна уявити як обліковий запис, він не обліковується в системі депозитарного обліку цінних паперів; натомість зарубіжні регулятори (зокрема Комісія з цінних паперів і бірж Сполучених Штатів Америки, що застосовує «тест Хоуї») кваліфікують частину віртуальних

активів як інвестиційні контракти, а низка юрисдикцій впроваджує категорію інвестиційних токенів [32, с. 132]. У праві ЄС цьому відповідає диференціація за MiCA, де токени з прив'язкою до активів і токени електронних грошей підпорядковано спеціальному режиму, а криптоактиви - фінансові інструменти взагалі виведено за межі регламенту [2; 26, с. 90-91]. Це питання має пряме кримінально-правове значення, оскільки кваліфікація конкретного віртуального активу як цінного папера чи фінансового інструмента впливає на встановлення предмета посягання.

Належність віртуальних активів до майна виразно проявляється в їх оборотоздатності - здатності бути об'єктом цивільно-правових договорів. Досліджуючи договір міни, Є. Ю. Савченко обґрунтовує, що віртуальні активи як об'єкти цивільних прав можуть бути його предметом: оскільки до договору міни застосовуються положення про купівлю-продаж (статті 715, 716 ЦК України), а закон може встановлювати лише особливості, а не заборони щодо його укладення, заборона «предмета обміну» в частині сьомій статті 4 нечинного профільного закону позбавлена чіткого правового наповнення і суперечить статті 715 ЦК України [39, с. 67-70; 27; 1]. Автор покликається на законопроекти, спрямовані на усунення цієї колізії, які, утім, є попередниками нової редакції профільного закону і предметно належать до проблематики підрозділу 2.4 [39, с. 70-71]. Не менш показовим є договір позики. Л. А. Музика встановлює, що його предметом є грошові кошти або інші речі, визначені родовими ознаками (стаття 1046 ЦК України) [34, с. 74; 27]. Це дозволяє провести внутрішнє розмежування й самих віртуальних активів: невзаємозамінні токени, що мають унікальний ідентифікатор і не визначаються родовими ознаками, не можуть бути об'єктом позики, тоді як інші, родовоозначені віртуальні активи - можуть, причому стейблкоїни, прив'язані до національної валюти, навіть із нарахуванням процентів, на відміну від решти віртуальних активів, передача яких як речей за родовими ознаками є безпроцентною з огляду на імперативність статті 1048 ЦК України [34, с. 74-77; 27]. Отже, категорія віртуальних активів є внутрішньо неоднорідною, що безпосередньо підводить до її класифікації.

Окремо слід застерегти від змішування цивілістичних категорій із міждисциплінарним слововжитком. Так, в економіко-управлінській літературі поняття «віртуальна річ» чи «цифровий товар» вживається в позаюридичному значенні - як електронні об'єкти (файлові сховища, електронні книги, музика та фільми в електронній формі, комп'ютерні програми), що мають ознаки товару й існують лише в мережі Інтернет [40, с. 3]. Таке слововживання не тотожне цивілістичній «цифровій речі» у розумінні статті 179-1 ЦК України і не може механічно переноситися у правову площину [40, с. 3; 27]. Цей приклад унаочнює, наскільки важливою є термінологічна дисципліна при визначенні предмета кримінально-правової охорони, адже неточність на понятійному рівні неминуче відтворюється у правозастосуванні.

Узагальнюючи, проведене розмежування дозволяє в цілях дослідження кримінально-правової політики підтримати запропонований у літературі ланцюг: цифрові речі (цифрові активи) - віртуальні активи - криптоактиви - криптовалюта, у якому кожне наступне поняття є видовим щодо попереднього [24, с. 240-241; 26, с. 94-95]. Віртуальні активи відмежовуються від нематеріальних благ та інформації, до яких вони не належать; від грошей і засобів платежу, статусу яких вони за чинним правом не мають, хоча окремі їх різновиди - стейблкоїни - функціонально тяжіють до грошових коштів; від цінних паперів, у депозитарній системі обліку яких вони не перебувають, хоча інвестиційні токени за своїми функціями до них наближаються; а від робіт і послуг - повністю. Водночас за чинним цивільним законодавством віртуальні активи належать до цифрових речей, а отже - до майна, будучи оборотоздатними об'єктами цивільних прав особливого роду (*sui generis*). Для цілей цього дослідження це означає, що віртуальний актив виступає самостійним предметом правовідносин, який не зводиться до жодної із суміжних категорій.

1.3. Класифікація віртуальних активів та її кримінально-правове значення

Систематизація віртуальних активів за певними критеріями становить необхідну передумову як належного правового регулювання їх обороту, так і

точного встановлення предмета кримінально-правової охорони. Класифікація дає змогу з'ясувати, у який спосіб окремі різновиди віртуальних активів використовуються в різних економічних і соціальних контекстах, а отже - і яку роль вони здатні відігравати у структурі складу кримінального правопорушення [41, с. 90]. Водночас у сучасній доктрині та законодавчій практиці не склалося єдиного підходу ні до видів віртуальних активів, ні до критеріїв їх поділу: тривале паралельне вживання понять «криптовалюти», «віртуальні валюти», «криптоактиви» зумовило співіснування численних, нерідко несумісних класифікацій, а запровадження узагальнюючого терміна «віртуальні активи» само по собі єдиної типології не сформувало [41, с. 90-91]. З огляду на це доцільно послідовно розглянути класифікації, закріплені в законодавстві України та Європейського Союзу, а також основні доктринальні підходи, після чого окреслити власне кримінально-правове значення поділу віртуальних активів, яке досі залишається малодослідженим.

Вихідним для національної правової системи є поділ, закріплений у Законі України «Про віртуальні активи» від 17 лютого 2022 р. № 2074-IX. Слід наголосити, що цей Закон є нечинним; відтак закріплені в ньому положення можуть розглядатися лише як перспективна (нечинна) модель, тоді як де-юре чинне визначення віртуального активу - похідне від Рекомендацій Групи з розроблення фінансових заходів боротьби з відмиванням коштів - міститься в Законі України № 361-IX [12]. За критерієм забезпеченості Закон № 2074-IX розрізняє два основних види віртуальних активів: забезпечений віртуальний актив, що посвідчує майнові права, зокрема права вимоги на інші об'єкти цивільних прав (пп. 3 п. 1 ст. 1, п. 3 ст. 4), та незабезпечений віртуальний актив, що не посвідчує жодних майнових або немайнових прав (пп. 6 п. 1 ст. 1, п. 2 ст. 4) [1]. Інших класифікацій віртуальних активів цей Закон не передбачає.

Забезпечений віртуальний актив набуває значення фінансового віртуального активу і, своєю чергою, зазнає внутрішнього поділу залежно від об'єкта забезпечення (п. 6 ст. 4 Закону): на забезпечений валютними цінностями (ЗВА(ВЦ)), державне регулювання обороту якого віднесено до компетенції Національного банку України, та забезпечений цінним папером або

деривативним фінансовим інструментом (ЗВА(ФІ)), регулювання обороту якого здійснює Національна комісія з цінних паперів та фондового ринку [43, с. 70]. Як зазначає В. Яроцький, саме фінансовий віртуальний актив - тобто актив, забезпечений валютною цінністю або одним із фінансових інструментів, допущених до торгівлі на ринках капіталу, - може виступати інструментом інвестування на організованих майданчиках, тоді як незабезпечений віртуальний актив залишається найменш визначеним у законодавстві за своєю правовою природою [42, с. 104-105]. Сам по собі віртуальний актив не є цінним папером у розумінні ст. 8 Закону України «Про ринки капіталу та організовані товарні ринки» [38], а фінансово-інструментальних властивостей набуває саме через об'єкт забезпечення.

Виокремлення категорії активів, забезпечених деривативним фінансовим інструментом, не є суто теоретичним. На базі віртуальних активів уже функціонують похідні фінансові інструменти, зокрема ф'ючерсні контракти - стандартизовані угоди про купівлю чи продаж базового активу за заздалегідь визначеною ціною у визначений момент у майбутньому, які за своєю природою є деривативами [44, с. 114]. Для криптоактивів найпоширенішим різновидом є безстроковий ф'ючерс (perpetual), що не має фіксованої дати поставки, розраховується грошима та виконується автоматично засобами смарт-контракту без участі посередника [44, с. 114-115]. Існування таких інструментів додатково ускладнює класифікацію віртуальних активів і підтверджує фінансово-інструментальну природу окремих їх різновидів.

Запропонований законодавцем поділ за критерієм забезпеченості зазнав у літературі обґрунтованої критики. Р. Самсін слушно зауважує, що така класифікація не забезпечує належного правового регулювання, оскільки не надає законодавцеві достатніх інструментів для впорядкування відносин у сфері обороту віртуальних активів [41, с. 91]. С. Цукан, своєю чергою, звертає увагу, що для світової законодавчої практики поділ на забезпечені та незабезпечені активи є досить незвичним [10, с. 616]. Відтак національна модель класифікації віртуальних активів - навіть у її перспективному вигляді - потребує узгодження з усталеними міжнародними та європейськими підходами.

Найавторитетнішим орієнтиром у цьому відношенні є право Європейського Союзу. Регламент (ЄС) 2023/1114 про ринки криптоактивів (MiCA), що застосовується в повному обсязі з 30 грудня 2024 р., класифікує криптоактиви на три типи: токени електронних грошей (electronic money tokens, EMT), вартість яких стабілізується через прив'язку до однієї офіційної валюти і функції яких подібні до функцій електронних грошей; токени, прив'язані до активів (asset-referenced tokens, ART), вартість яких підтримується прив'язкою до іншої цінності, права або їх комбінації, у тому числі до кількох офіційних валют; та криптоактиви, відмінні від ART і EMT, до яких належать, зокрема, службові (utility) токени (п. 18 преамбули) [2]. Категорія tokenів електронних грошей безпосередньо змодельована за зразком електронних грошей у розумінні Директиви 2009/110/EC, яка визначає електронні гроші як електронний сурогат монет і банкнот, призначений для здійснення платежів [45]. Поза основним предметом регулювання MiCA залишаються унікальні та невзаємозамінні токени (NFT) - крім випадків, коли вони фактично є взаємозамінними або випускаються великими серіями, - що додатково засвідчує невичерпність наведеної типології.

Запровадженню в праві ЄС видової класифікації передував етап недиференційованого визначення: Директива (ЄС) 2018/843 оперувала єдиним поняттям «віртуальні валюти», розуміючи під ними цифрове вираження вартості, яке не випускається й не гарантується центральним банком або державним органом, але приймається як засіб обміну та може передаватися, зберігатися й продаватися в електронному вигляді [46]. Перехід від цього єдиного поняття до триланкової типології MiCA, як зазначає С. Цукан, зумовлений розширенням змісту й технологічною еволюцією відповідних активів; при цьому в інших європейських правопорядках сформувалися власні переліки видів - зокрема, законодавство Великої Британії розрізняє обмінні, сек'юритизовані та службові токени [10, с. 617]. Саме класифікація за MiCA, на думку дослідника, має бути покладена в основу нової редакції національного профільного закону [10, с. 617], що узгоджується із загальним курсом України на імплементацію європейської регуляторної моделі.

Порівняльний зріз інституційних класифікацій, узагальнений Р. Самсіним, демонструє ще більшу їх варіативність: Всесвітній економічний форум виокремлював інвестиційні, утилітарні та валютні токени; Управління з нагляду за фінансовими ринками Швейцарії (FINMA) - платіжні, сервісні токени, токени активів і гібридні токени; Європейський центральний банк класифікував віртуальні валюти за критерієм їх взаємодії із законними платіжними засобами; а спільний документ Організації економічного співробітництва і розвитку, Євростату та Європейської економічної комісії ООН запропонував розгорнуту класифікацію криптоактивів за виконуваними ними функціями (загальний засіб платежу, платіжні токени, активи, що виконують функції цінних паперів, засіб накопичення та інші) [41, с. 91-94]. Спільним для цих підходів є те, що вид активу визначається залежно від типу криптотокена, який має цифрове вираження вартості та оборотоздатність.

Доктринальні класифікації віртуальних активів є не менш різноманітними. У систематизаціях, наведених Р. Самсіним та В. Яроцьким, відображено, зокрема, поділ Н. Пантелєєвої та Н. Рогової (криптовалюта, токени, криптотовари, стейблкоїни), А. Овчаренко (віртуальні валюти, віртуальні товари, віртуальні токени, доменні імена), а також дворівневу класифікацію А. Кудя (за технологічною природою - активи розподіленого та нерозподіленого реєстру; за економіко-правовою сутністю - токенований актив і криптоактив) [41, с. 95-96; 42, с. 105-106]. О. Черних поклала в основу поділу ознаку емітента, розрізняючи суверенні (цифрові валюти центральних банків, CBDC) і приватні віртуальні активи, тоді як С. Грицай систематизував їх за критерієм забезпеченості, виділяючи фінансові віртуальні активи (забезпечені валютними цінностями або цінними паперами чи деривативними фінансовими інструментами) та незабезпечені [41, с. 96-97]. Сам Р. Самсін як основний критерій пропонує характер випуску активу - централізований чи децентралізований, тобто наявність або відсутність емітента, наголошуючи, що регулювання відносин щодо централізованих активів має спрямовуватися на вимоги до емітентів і постачальників послуг, тоді як щодо децентралізованих - лише на постачальників послуг, які мають намір діяти легально, інакше

регулювання набуде декларативного характеру [41, с. 97]. В. Яроцький, погоджуючись, що найбільше юридичне значення має поділ за забезпеченістю, пропонує доповнити його критерієм форми (об'єкта) забезпечення [42, с. 106].

Викладене дає підстави окреслити кримінально-правове значення класифікації віртуальних активів. Вид віртуального активу безпосередньо впливає на встановлення предмета та на кваліфікацію відповідних кримінальних правопорушень. Так, забезпечений віртуальний актив, який посвідчує майнові права (зокрема права вимоги) і за чинною редакцією ЦК України прирівняний до майна як різновид цифрової речі [27], тяжіє до кваліфікації як предмет кримінальних правопорушень проти власності; натомість щодо незабезпеченого активу, позбавленого прив'язки до інших об'єктів цивільних прав, особливо гостро постають проблеми визначення предмета посягання та доказування його вартості. Фінансові віртуальні активи, що виконують інвестиційну функцію та забезпечуються цінними паперами або деривативами, окреслюють потенційну сферу посягань, пов'язаних із ринками капіталу та зловживаннями на них.

Водночас віртуальні активи, що фактично виконують платіжну функцію та забезпечують високий рівень анонімності трансакцій (передусім незабезпечені криптовалюти й окремі стейблкоіни), становлять підвищений ризик використання як засобу легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму. Нарешті, запропонований у доктрині поділ за характером випуску (централізовані / децентралізовані активи) має не лише регуляторне, а й кримінологічне значення, оскільки визначає коло суб'єктів, на яких може бути покладено обов'язки фінансового моніторингу, а отже - і реальні межі ефективної кримінально-правової охорони відповідних відносин: щодо децентралізованих активів превентивний потенціал зосереджується головню на постачальниках послуг. Таким чином, обрана законодавцем класифікаційна ознака зрештою зумовлює і конструкцію відповідних складів, і дієвість механізмів запобігання.

Узагальнюючи, слід констатувати, що з-поміж наявних класифікацій найбільше прикладне значення мають поділ за критерієм забезпеченості та

об'єктом забезпечення (характерний для законодавства України) і видова типологія за МіСА, що ґрунтується на прив'язці вартості та функціональному призначенні токена. Гармонізація національної моделі з європейською - зокрема через перехід до диференційованої класифікації криптоактивів - є необхідною передумовою як упорядкування їх обороту, так і формування узгодженого розуміння віртуального активу як предмета, засобу чи знаряддя кримінального правопорушення.

Висновки до розділу 1

Проведене в розділі дослідження теоретико-методологічних і понятійних засад охорони віртуальних активів дозволяє сформулювати такі висновки.

1. Віртуальні активи постали як новітнє явище на перетині економічних, технологічних і світоглядних передумов - ідей денаціоналізації грошей австрійської школи, криптоанархічного руху та тривалої еволюції технологій цифрових грошей, що завершилася появою біткоїна і технології блокчейн. Децентралізований і псевдонімний характер обігу, відсутність єдиного емітента та незворотність трансакцій визначають специфіку віртуальних активів водночас як предмета кримінальних правопорушень, засобу їх учинення та об'єкта доказування.

2. Понятійний апарат у досліджуваній сфері залишається неусталеним. Термінологічна еволюція пройшла шлях від «криптовалюти» через «віртуальні активи» до «криптоактивів», проте єдиного уніфікованого найменування на міжнародному рівні не сформовано. Для цілей дослідження прийнято диференційовану родо-видову модель, у якій віртуальні активи є родовим поняттям щодо криптоактивів і криптовалюти, що дозволяє уникнути термінологічного змішування, неприпустимого з огляду на принцип правової визначеності в кримінальному праві.

3. Національне регулювання має перехідний характер. Чинною легальною дефініцією віртуального активу залишається функціональне визначення Закону № 361-IX, тоді як цивілістично орієнтований профільний Закон № 2074-IX лишається нечинним, а орієнтиром майбутньої моделі

регулювання виступає Регламент (ЄС) 2023/1114 (MiCA) разом із чинним законодавством Європейського Союзу. Ця двоїстість дефініцій має принципове значення, оскільки від обраного визначення безпосередньо залежить кваліфікація віртуального активу у структурі складу кримінального правопорушення.

4. За правовою природою віртуальний актив є майном особливого роду (*sui generis*), субстратом якого виступає сама інформація, а не носій права вимоги: при переказі віртуального активу передається інформація, що становить актив, а не дані про права на інший об'єкт. За чинним цивільним законодавством (стаття 179-1 ЦК України) віртуальні активи віднесено до цифрових речей, а отже - до майна, що підтверджує їх придатність бути предметом злочинів проти власності.

5. Розмежування віртуальних активів із суміжними поняттями дозволило підтримати запропонований у літературі ланцюг «цифрові речі (цифрові активи) - віртуальні активи - криптоактиви - криптовалюта» та відмежувати віртуальні активи від нематеріальних благ та інформації, грошей і засобів платежу, цінних паперів і фінансових інструментів, а також робіт і послуг. Водночас встановлено внутрішню неоднорідність категорії: окремі різновиди (стейблкоїни) функціонально тяжіють до грошових коштів, інші (інвестиційні токени) - до фінансових інструментів, що й зумовлює потребу в класифікації.

6. Аналіз класифікацій засвідчив відсутність єдиного підходу як у доктрині, так і в законодавстві. Найбільше прикладне значення мають поділ за критерієм забезпеченості та об'єктом забезпечення, характерний для законодавства України (забезпечені та незабезпечені віртуальні активи; забезпечені валютними цінностями або фінансовими інструментами), і видова типологія за функціональним призначенням та прив'язкою вартості токена, запроваджена MiCA (токени електронних грошей, токени з прив'язкою до активів, інші криптоактиви). Гармонізація національної моделі з європейською є необхідною передумовою впорядкування обороту віртуальних активів.

7. Обґрунтовано самостійне кримінально-правове значення класифікації віртуальних активів: вид активу безпосередньо впливає на встановлення предмета та кваліфікацію відповідних правопорушень. Забезпечений віртуальний актив тяжіє до предмета злочинів проти власності; незабезпечений породжує проблему визначення предмета й доказування вартості; фінансові віртуальні активи окреслюють сферу посягань, пов'язаних із ринками капіталу; платіжні та анонімні активи становлять підвищений ризик використання як засобу легалізації (відмивання) доходів і фінансування тероризму, а поділ за характером випуску (централізовані та децентралізовані активи) визначає коло суб'єктів фінансового моніторингу і реальні межі кримінально-правової охорони.

8. У розділі сформульовано визначення віртуальних активів для цілей кримінально-правового дослідження та виокремлено низку пропозицій *de lege ferenda* - щодо визнання віртуальних активів майном *sui generis*, узгодження їх дефініції та класифікації з MiCA, усунення суперечностей чинного й перспективного регулювання.

РОЗДІЛ 2.

ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ВІРТУАЛЬНИХ АКТИВІВ

2.1. Стан наукової розробки проблеми та методологія дослідження кримінально-правової політики у сфері забезпечення охорони віртуальних активів

Дослідження кримінально-правової політики (далі - КПП) у сфері забезпечення охорони віртуальних активів вимагає попереднього з'ясування двох взаємопов'язаних питань - стану наукової розробки відповідної проблематики та методологічного інструментарію, придатного для пізнання порівняно нового об'єкта правової охорони. Хоча кожне з цих питань є самостійним, їх доцільно розглядати в єдності, оскільки саме наявні наукові напрацювання значною мірою визначають вибір методів, підходів і принципів подальшого дослідження, а виявлені в них прогалини окреслюють його завдання.

Вихідною теоретичною основою постає вчення про політику у сфері боротьби зі злочинністю, що в українській науці найповніше розроблене представниками наукової школи, заснованої П. Л. Фрісом. Згідно з його концепцією, політика у сфері боротьби зі злочинністю становить генеральну лінію внутрішньої політики держави, яка визначає основні напрями, цілі та способи впливу на злочинність через формування кримінального, кримінального процесуального та кримінально-виконавчого законодавства, регулювання практики його застосування, а також розроблення і реалізацію заходів запобігання злочинам [47]. У межах цієї цілісної політики КПП розглядається як її системоутворюючий елемент, що формулює стратегію і тактику, завдання, принципи та напрями кримінально-правового впливу, послуговуючись властивими їй методами криміналізації та декриміналізації,

пеналізації та депеналізації [47]. Засадниче значення має й те, що така політика розгортається в межах, окреслених правами людини, які виступають її природним обмежувачем [48].

Системний характер політики у сфері боротьби зі злочинністю передбачає узгодженість її підсистем. В. І. Борисов, окреслюючи напрями державної політики у цій сфері, обґрунтовує положення про те, що КПП є змістом кримінально-процесуальної політики і зумовлює підстави обрання відповідних форм її реалізації [49, с. 306]. Це має безпосереднє значення для предмета дослідження, оскільки охорона віртуальних активів засобами кримінального права не може розглядатися у відриві від процесуальних і виконавчих механізмів її реалізації. Структурно-функціональний вимір КПП, її місце в системі протидії злочинності та зміст притаманних їй функцій ґрунтовно опрацьовані І. В. Козичем [50]. Окремі підсистеми єдиної політики висвітлені у профільних дослідженнях: кримінальна процесуальна політика - у працях Ю. І. Микитина, який обстоює перевагу терміна «політика у сфері боротьби зі злочинністю» і поширює відповідну конструкцію на наднаціональний рівень Європейського Союзу [51, с. 187]; кримінально-виконавча політика України, її поняття, стан і тенденції - у монографічному дослідженні Ю. В. Кернякевич-Танасійчук [52]. Сукупно ці праці формують доктринальний каркас, у який вписується кримінально-правова охорона віртуальних активів і обґрунтовується доцільність її розгляду у зв'язку з процесуальною та виконавчою політикою.

Стан наукової розробки власне проблематики віртуальних активів характеризується вираженою міждисциплінарністю та нерівномірністю. Якщо понятійно-визначальні та класифікаційні аспекти набули достатнього висвітлення, що відображено в першому розділі цієї роботи, то кримінально-правовий і політико-правовий виміри досліджені фрагментарно. Показовим є бібліографічний огляд А. О. Кучерявого, який систематизує вітчизняний доробок за чотирма напрямками - інституціональне забезпечення обігу, теоретичні підвалини категорії, оцінка галузевого впливу та обліково-аналітичні аспекти [53, с. 124]. Запропонований автором розподіл публікацій

унаочнює переважання інституціонально-регуляторної та понятійної проблематики за помітного дефіциту власне кримінально-правових студій. Водночас автор фіксує відсутність уніфікованого підходу до трактування поняття «віртуальні активи» та єдиної їх класифікації як методологічну перешкоду прозорому регулюванню й протидії відмиванню коштів [53, с. 128]. Ця теза суголосна загальному висновку про незавершеність понятійно-методологічної єдності у досліджуваній сфері.

Зарубіжний сегмент наукової розробки дає змогу простежити різні методологічні моделі оцінки самого стану дослідженості галузі. Систематичний огляд літератури за протоколом PRISMA реалізовано в дослідженні D. Khan та співавторів, які шляхом послідовного відсіву публікацій - від первинного масиву до сорока п'яти статей за 2018-2022 роки - окреслили динаміку, географію і тематичну структуру студій про злочинність у криптовалютній сфері [54, с. 13-15]. Спорідненою, але ширшою за охопленням є *scoping*-методологія S. Navani та G. T. Cirella, які з понад чотирьох тисяч публікацій відібрали двісті двадцять вісім джерел і доповнили якісний аналіз бібліометричними зрізами - за континентами, роками та видавництвами [55, с. 2]. Прикметно, що в цьому дослідженні Україну віднесено до помітних осередків наукового опрацювання криптозлочинності, з покликанням на праці вітчизняних авторів [55, с. 2-3], що засвідчує інтегрованість української науки у глобальне дослідницьке поле.

Якісний тематичний огляд репрезентовано працею A. Guidara, який, узагальнивши масив емпіричних студій у сфері обліку та фінансів, виокремив три обмеження наявного доробку - переважання уваги до негативних аспектів, брак усталених облікових стандартів і норм та домінування якісних досліджень за дефіциту кількісних [56, с. 40]. Діахронний зріз розвитку закордонної дискусії подано в оглядово-аналітичній праці J. A. Collins, який, простежуючи еволюцію поглядів від ранніх досліджень до сучасних, констатує тривале відтворення тих самих регуляторних проблем упродовж понад десятиліття [57]. Порівняльно-правову методологію оцінки регуляторних моделей застосовано в дослідженні М. Карчевського та співавторів, які, спираючись на

документальний метод, зіставили підходи держав різних правових сімей і обґрунтували доцільність орієнтації України на романо-германську (європейську) модель поступового впровадження правового регулювання обігу криптовалют [58, с. 157-159].

Окрему лінію стану розробки утворюють праці, що оновлюють методологію кримінального права з огляду на дематеріалізацію об'єктів правової охорони. І. Газдайка-Василишин, виходячи з того, що класична, побудована на матеріалістичних уявленнях конструкція предмета злочину втрачає пояснювальну силу в умовах цифровізації, пропонує доповнити структуру об'єкта складу кримінального правопорушення новою факультативною ознакою - «ремою», яка охоплює нематеріальні феномени (інформацію, цифровий код, віртуальні активи), через вплив на які заподіюється шкода [59, с. 11-12]. Авторка обстоює трирівневу модель об'єкта (суспільні відносини - предмет - рема) та семіотико-інформаційну парадигму кримінально-правового мислення [59, с. 12-13]. Слід наголосити, що концепція «реми» є авторською доктринальною новацією, висунутою *de lege ferenda*, а не положенням чинного права; її значення для цього дослідження полягає насамперед у методологічному висвітленні проблеми нематеріального предмета.

Методологічно близький прийом раніше застосував М. В. Карчевський, який систематизував ознаки криптовалюти в межах традиційної для кримінального права системи ознак предмета злочину - фізичної, економічної та юридичної - і дійшов висновку, що криптовалюта становить дані в електронному вигляді, які мають ціну та є предметом реалізації права на інформацію [60, с. 108]. Цей висновок було сформульовано до набрання чинності законодавчими актами, що визначили легальний статус віртуальних активів, а тому його належить сприймати з відповідним застереженням; натомість методологічно значущим залишається обстоюваний автором принцип технологічної нейтральності законодавства, згідно з яким нормативні формулювання не повинні прив'язуватися до конкретних технологій [60, с. 115].

Узагальнення стану наукової розробки дає підстави для висновку, що дослідження КПП у сфері охорони віртуальних активів потребує не запозичення галузевого інструментарію в готовому вигляді, а формування інтегрованої методологічної системи. Орієнтиром тут слугують напрацювання О. В. Грунь, яка обґрунтовує розуміння методології у вузькому значенні як сукупності принципів, підходів і методів [61, с. 25] та пропонує впорядковану систему засобів дослідження правової регламентації відносин у віртуальному середовищі. Ця система охоплює чотири рівні методів - загальні методи пізнання, загальнонаукові (з визнанням діалектичного методу провідним), міждисциплінарні та спеціально-юридичні (формально-юридичний, порівняльно-правовий, юридична герменевтика) [61, с. 26-27], а її засадами є принципи плюралізму, додатковості та міждисциплінарності [61, с. 26]. Прийнятність такого підходу зумовлена тим, що віртуальні активи як об'єкт правової охорони лежать на перетині кількох галузей знання, а отже, не можуть бути адекватно пізнані засобами однієї галузі.

Не менш значущим є питання вибору дослідницького підходу. Є. О. Мічурін вирізняє три підходи до об'єктів цифрових технологій - технократичний, комплексно-правовий і спеціально-правовий - і надає перевагу останньому, обираючи в його межах приватноправовий ракурс [62, с. 23-24]. Для цілей цього дослідження продуктивним є поєднання спеціально-правового підходу з кримінально-правовим ракурсом: якщо приватноправовий аналіз з'ясовує природу віртуальних активів як об'єкта цивільних прав, то кримінально-правовий - умови та межі їх охорони засобами кримінального права. Водночас Є. О. Мічурін слушно звертає увагу на те, що нематеріальний об'єкт не може бути фізично вилучений чи арештований у спосіб, властивий речам [62, с. 26], чим оприявнюється методологічний дефіцит, подолання якого є одним із завдань цього дослідження.

Викладене дає змогу окреслити методологічну основу цього дослідження. Її ядром є діалектичний метод, що забезпечує розгляд КПП у сфері охорони віртуальних активів у розвитку та у взаємозв'язку з економічними й технологічними чинниками. Формально-юридичний метод застосовується для

аналізу змісту кримінально-правових норм і конструкцій складів відповідних правопорушень; юридична герменевтика - для тлумачення нормативних приписів, насамперед легальної дефініції віртуальних активів; системно-структурний метод - для з'ясування місця КПП у системі політики у сфері боротьби зі злочинністю та структури охоронюваних відносин; історико-правовий - для висвітлення генези відповідного регулювання; порівняльно-правовий - для зіставлення національних рішень із Регламентом (ЄС) 2023/1114 та досвідом окремих держав; статистичний - для опрацювання емпіричних даних про відповідну злочинність. З огляду на нематеріальну природу об'єкта залучається й онтологічний метод, що уможливорює адекватний опис посягань, позбавлених матеріального субстрату.

Стан наукової розробки та обрана методологія дають підстави сформулювати робочі гіпотези дослідження. По-перше, відсутність уніфікованого визначення та єдиної класифікації віртуальних активів, на яку вказують і вітчизняні, і зарубіжні автори, є не лише доктринальною, а й методологічною перешкодою для формування послідовної КПП; при цьому чинна легальна дефініція визначається статтею 1 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [12], тоді як профільний Закон України «Про віртуальні активи» [1] чинності не набрав, а на рівні Європейського Союзу авторитетним орієнтиром виступає Регламент (ЄС) 2023/1114 (MiCA) [2]. По-друге, потребує вироблення методика встановлення вартості віртуальних активів і доказування у відповідних провадженнях, брак якої констатують і кримінально-правові, і цивілістичні дослідження. По-третє, ефективне пізнання КПП у сфері охорони віртуальних активів можливе лише на основі інтегрованого міждисциплінарного інструментарію, що поєднує спеціально-юридичні методи з підходами, виробленими в межах порівняльно-правової парадигми.

2.2. Поняття, ознаки та структура кримінально-правової політики у сфері забезпечення охорони віртуальних активів

Кримінально-правова політика у сфері забезпечення охорони віртуальних активів є відносно самостійним сегментом, що перебуває на перетині двох ширших нормативно-політичних утворень - загальної кримінально-правової політики держави та державної політики у сфері обігу віртуальних активів. Її змістова своєрідність зумовлена щонайменше трьома обставинами. По-перше, об'єкт охорони - суспільні відносини, пов'язані зі створенням, обігом і використанням віртуальних активів, - є новим, високотехнологічним і транскордонним, а тому погано піддається традиційним механізмам правового впливу. По-друге, нормативна основа впорядкування цих відносин в Україні перебуває у стані переходу: модель Закону України «Про віртуальні активи» № 2074-IX [1] так і не набрала чинності, а перспективне регулювання вибудовується за зразком Регламенту (ЄС) 2023/1114 (MiCA) [2]. По-третє, переважна частина суспільно небезпечних посягань у цій сфері має транснаціональний і високолатентний характер. З огляду на це з'ясування поняття, ознак і структури досліджуваної політики потребує попереднього встановлення родових щодо неї конструкцій і послідовного відмежування власне кримінально-правового змісту від суміжних - адміністративно-правового та фінансово-правового - складників забезпечення охорони.

Найближчою родовою категорією виступає поняття забезпечення державної політики у відповідній сфері, докладно опрацьоване в адміністративно-правовій доктрині. Так, Д. М. Олійник, дослідивши зміст адміністративно-правового забезпечення державної політики щодо розвитку і функціонування ринку віртуальних активів, узагальнює п'ять усталених у науці підходів до категорії «забезпечення» - як до виду нормативно-правового забезпечення, безперервної діяльності зі створення певних умов, порядку діяльності, основи правового впливу, а також комплексу інструментів і методів їх застосування - і обґрунтовано критикує кожен із них за однобічність [63, с. 670-673]. На цій підставі автор пропонує розуміти адміністративно-правове

забезпечення державної політики у сфері віртуальних активів як цілеспрямований управлінський процес, у межах якого держава через органи публічної служби за участю інститутів громадянського суспільства, ґрунтуючись на нормах і принципах права, приймає рішення та здійснює дії з використанням відповідних правових інструментів задля створення умов, за яких держава правомірно, ефективно і передбачувано планує, розробляє, затверджує та реалізує політику у сфері віртуальних активів, гарантує права учасників ринку і забезпечує баланс публічних та приватних інтересів [63, с. 673]. При цьому автор наголошує на необхідності входження національного ринку до міжнародного, підпорядкованого правилам і рекомендаціям Групи з розроблення фінансових заходів боротьби з відмиванням коштів (далі - ФАТФ) [63, с. 674-675].

Наведена конструкція є придатною для побудови видового поняття за умови її послідовної трансформації у кримінально-правову площину. Принципова відмінність полягає у меті та методі. Якщо адміністративно-правове забезпечення спрямоване насамперед на організацію і розвиток ринку, то кримінально-правова політика у досліджуваній сфері має вужчу й водночас гострішу мету - визначення кола суспільно небезпечних посягань на відносини у сфері обігу віртуальних активів і засобів кримінально-правового реагування на них. З урахуванням обґрунтованого у науці загального розуміння кримінально-правової політики під **кримінально-правовою політикою у сфері забезпечення охорони віртуальних активів** пропонується розуміти *системну діяльність уповноважених суб'єктів щодо формування і реалізації стратегії кримінально-правової охорони суспільних відносин, які виникають у зв'язку зі створенням, обігом та використанням віртуальних активів, що здійснюється шляхом визначення підстав і меж криміналізації відповідних діянь, диференціації та індивідуалізації кримінальної відповідальності, а також забезпечення застосування кримінального закону з урахуванням міжнародних стандартів і європейської моделі регулювання обігу таких активів*. На відміну від адміністративно-правового забезпечення, ця політика реалізується насамперед засобами Кримінального кодексу України [64] і не зводиться до

регулятивного впливу на ринок, а доповнює його охоронним (заборонним) складником.

Із запропонованого визначення випливають основні ознаки досліджуваної політики. Вона, по-перше, є різновидом і загальної кримінально-правової політики держави, і державної політики у сфері обігу віртуальних активів, а отже підпорядкована як принципам кримінального права, так і завданням розвитку відповідного ринку. По-друге, їй властивий похідний (вторинний) характер щодо регулятивного законодавства: коло і зміст кримінально караних посягань значною мірою визначаються тим порядком обігу, який встановлюється регулятивними нормами, через що відповідні заборони здебільшого мають бланкетну природу. По-третє, для цієї політики характерна виражена міжнародна і європейська зумовленість, оскільки транскордонна природа віртуальних активів унеможлиблює суто національне впорядкування відповідних відносин. По-четверте, вона відзначається підвищеною технологічною складністю об'єкта, що вимагає від суб'єктів її формування і реалізації спеціальних знань про технологію розподіленого реєстру, смарт-контракти і токенизацію. Нарешті, ця політика є динамічною, позаяк змушена постійно реагувати на появу нових форм віртуальних активів і нових способів їх протиправного використання.

Структуру кримінально-правової політики у досліджуваній сфері доцільно розкривати через її об'єкт, суб'єктів, принципи, а також форми і засоби реалізації. Визначення об'єкта потребує з'ясування того, на яку сферу суспільних відносин спрямовано охоронний вплив. У вітчизняній доктрині ринок віртуальних активів запропоновано розглядати як самостійний об'єкт правового регулювання. О. І. Кулик, констатує, що цей ринок тривалий час існував фактично у правовому вакуумі й залишався «в тіні», що стримувало його розвиток і знижувало ефективність нормативно-правового впливу [65, с. 56-57], спирається на запропоноване В. П. Плавичем розуміння трьох напрямів впливу права на економіку - закріплення наявних економічних відносин, стимулювання нових і охорони вже сформованих - та виокремлює відповідні напрями правового регулювання ринку віртуальних активів: конкретизацію

правового режиму об'єктів ринку, визначення правового статусу його суб'єктів, відносини щодо функціонування і стимулювання розвитку ринку, а також державне регулювання і саморегулювання [65, с. 58].

Узагальнивши наявні в теорії підходи до категорії «ринок» і легальні дефініції суміжних ринків (зокрема ринку електричної енергії та ринку природного газу), сформульовані через сукупність відповідних правовідносин, О.І. Кулик визначає ринок віртуальних активів як об'єкт правового регулювання - сукупність суспільних відносин, що виникають між учасниками ринку щодо створення та обігу віртуальних активів, здійснення державного регулювання і саморегулювання ринку [65, с. 60]. Водночас автор слушно застерігає проти поширеного у законопроектній практиці визначення ринку через просту сукупність його учасників, оскільки такий підхід не відповідає напрацюванням теорії права [65, с. 58-59]. Це застереження є методологічно важливим і для кримінально-правового дослідження, позаяк дозволяє чітко відмежувати об'єкт політики (відносини) від кола її суб'єктів (учасників). Прикметно, що автор пропонує закріпити відповідну дефініцію в акті «м'якого» права - Дорожній карті регулювання ринку, наголошуючи на корисності досвіду Європейського Союзу [65, с. 59-60].

Самі ж відносини, що становлять сферу обігу, мають складну внутрішню будову. О. Починок, аналізуючи структуру правовідносин, пов'язаних з обігом віртуальних активів, виокремлює в ній суб'єктів (постачальників послуг та інших учасників ринку), об'єкт (віртуальний актив як нематеріальне благо, що є об'єктом цивільних прав, має вартість і виражене сукупністю даних в електронній формі) і зміст (права та обов'язки учасників), а також пов'язані елементи - обіг віртуальних активів, публічну пропозицію та систему забезпечення їх обігу [66, с. 225-226]. Автор окремо звертає увагу на поділ віртуальних активів на забезпечені та незабезпечені, а серед забезпечених - на фінансові віртуальні активи, забезпечені валютними цінностями або цінними паперами чи деривативними фінансовими інструментами, вбачаючи в них національний відповідник передбачених МіСА «токенів, пов'язаних з активами», і токенів електронних грошей, і водночас вказуючи на

термінологічну неповноту вітчизняної моделі порівняно з європейською [66, с. 224-226].

Слід урахувати, що О. Починок реконструює цю структуру за нормами Закону № 2074-IX, який сам же визнає таким, що не набрав чинності [66, с. 221]. Тому в умовах чинного правопорядку легальне підґрунтя поняття віртуального активу слід виводити насамперед із Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» № 361-IX [12], тоді як модель Закону № 2074-IX має використовуватися лише як перспективна. Транспонуючи поняття об'єкта у кримінально-правову площину, можна стверджувати, що об'єктом досліджуваної політики є суспільні відносини, які забезпечують правомірне створення, обіг і використання віртуальних активів, охорону майнових та інших прав учасників ринку, а також безпеку інфраструктури такого ринку від суспільно небезпечних посягань. Цей об'єкт не тотожний об'єктові державного регулювання ринку: останнє охоплює всю сукупність відносин розвитку ринку, тоді як кримінально-правова охорона зосереджується на тій їх частині, що зазнає найбільш небезпечних порушень. Водночас наведена цивілістична характеристика віртуального активу як нематеріального блага, що має вартість, має значення і для кримінального права, оскільки визначає роль такого активу у структурі конкретних посягань - як їх предмета, засобу чи знаряддя.

Другим елементом структури є суб'єкти, причому саме тут необхідне особливо чітке розмежування, оскільки суб'єкти забезпечення обігу віртуальних активів і суб'єкти кримінально-правової політики не збігаються. Систему перших ґрунтовно описав О. В. Бондаренко, віднісши до неї органи загальної компетенції - Кабінет Міністрів України та Президента України, повноваження яких прямо не спрямовані на забезпечення обігу, але створюють умови для належної фінансової діяльності, елементом якої мають стати віртуальні активи, - та органи спеціальної компетенції: Національну комісію з цінних паперів та фондового ринку, Національний банк України, Міністерство

цифрової трансформації, Міністерство фінансів, Державну службу фінансового моніторингу і Бюро економічної безпеки [67, с. 242-243]. Автор показує, що профільне законодавство відводить ключову роль Національній комісії з цінних паперів та фондового ринку, проте чинні положення про відповідні органи повноважень саме щодо віртуальних активів не містять, з огляду на що автор формулює низку пропозицій *de lege ferenda* щодо їх доповнення [67, с. 243-244].

Водночас О. В. Бондаренко справедливо наголошує, що повноваження більшості названих органів щодо віртуальних активів набудуть повноти лише з моменту набрання чинності профільним законодавством [67, с. 245], а отже *de lege lata* вони реалізуються переважно в межах законодавства про фінансовий моніторинг.

Наведена інституційна карта становить адміністративно-правовий субстрат, у якому функціонує кримінально-правова політика, проте її власні суб'єкти є іншими.

Визначальним суб'єктом формування цієї політики є Верховна Рада України, адже відповідно до пункту 22 частини першої статті 92 Конституції України виключно законами України визначаються діяння, які є кримінальними правопорушеннями, та відповідальність за них [68]. Суб'єктами її реалізації виступають органи досудового розслідування (зокрема Бюро економічної безпеки України, відповідні підрозділи кіберполіції тощо), прокуратура, суд, а також органи, що забезпечують виявлення, розшук і управління активами, одержаними злочинним шляхом. Таким чином, окремі органи - насамперед Бюро економічної безпеки та Державна служба фінансового моніторингу - є спільними вузлами для адміністративно-правового забезпечення обігу і для кримінально-правової політики, проте виконують у них різні за природою функції: регулятивно-наглядові у першому випадку і правоохоронні у другому.

Самостійне значення для з'ясування суб'єктного виміру має питання про коло учасників відносин обігу, на яких поширюється охоронний вплив. О. А. Ушинкіна, дослідивши суб'єктний склад відповідних правовідносин, доходить висновку про доцільність широкого підходу до його визначення та про необхідність запозичення найбільш універсальних рішень із міжнародної

практики [69, с. 102]. Авторка показує, що саме на міжнародному рівні сформовано базові категорії учасників: у стандартах ФАТФ, до Глосарію яких ще у 2018 році включено поняття «віртуальні активи» та «постачальник послуг, пов'язаних з віртуальними активами», а згодом затверджено Керівництво щодо застосування ризик-орієнтованого підходу, окреслено широке коло підзвітних суб'єктів, а в Регламенті МіСА визначено правовий статус постачальника послуг щодо криптоактивів, емітента та інших осіб [69, с. 98-100]. Поряд із цим авторка наводить доктринальні класифікації суб'єктів - поділ В. Д. Іванюка на внутрішніх і зовнішніх учасників та запропонований А. А. Кудем поділ користувачів системи обліку на базі технології розподіленого реєстру на «постачальників» і «споживачів» послуг [69, с. 100-101].

Український законодавець, за оцінкою О. А. Ушинкіної, урахував наведені міжнародні стандарти лише частково, не охопивши значної кількості суб'єктів, зокрема майнерів і користувачів віртуальних активів [69, с. 102]. Цю прогалину підтверджує і С. О. Грицай, який, проаналізувавши учасників ринку віртуальних активів за моделлю Закону № 2074-IX (постачальників послуг чотирьох видів - зі зберігання або адміністрування, обміну, переказу та посередництва - і будь-яких осіб, що здійснюють операції у своїх інтересах), окремо вказує на те, що так звані майнери залишилися поза сферою його дії, оскільки оборот віртуального активу починається лише з моменту його створення [70, с. 153, 156]. Дослідник також звертає увагу на те, що низка оціночних формулювань щодо обмежень для постачальників послуг здатна спричиняти корупційні ризики під час видачі дозволів [70, с. 156-157]. Для кримінально-правової політики ці спостереження мають практичне значення, оскільки невизначеність кола суб'єктів обігу безпосередньо ускладнює встановлення суб'єкта відповідних кримінальних правопорушень, а отже - і коректну криміналізацію діянь у цій сфері.

Третім і одним із центральних для цього підрозділу елементом структури є принципи. Їх з'ясування потребує опори на загальну теорію принципів права, адаптовану до сфери віртуальних активів. С. В. Цукан, проаналізувавши термінологічні відмінності між суміжними поняттями «засада», «ідея»,

«положення» і «вимога» та виокремивши ознаки принципів права (нормативність, імперативність, фундаментальність і об'єктивну зумовленість), визначає принципи державного регулювання обороту віртуальних активів як норми-ідеї, вихідні положення, закріплені, зокрема, у нормативно-правових актах, що визначають зміст і спрямованість регулювання та забезпечують цілеспрямований вплив на систему відносин між учасниками ринку [71, с. 676-677]. Принципово важливою є його теза про правову природу таких принципів: на відміну від норм, вони жорстко не фіксують зміст поведінки, а тому здатні швидше реагувати на зміни суспільного життя, що зумовлює вимогу тлумачити і застосовувати норми у сфері віртуальних активів відповідно до принципів [71, с. 678]. Ця теза має пряме методологічне значення для кримінально-правової політики: в умовах незавершеності національного регулювання саме принципи, а через них - міжнародні та європейські стандарти, набувають значення визначального орієнтира.

Розгорнуту систему принципів забезпечення обігу віртуальних активів запропонував О. В. Бондаренко, виокремивши три їх групи: загальні принципи функціонування суб'єктів владних повноважень (законність, юридична визначеність, заборона свавілля, рівність перед законом, прозорість, підзвітність, ефективність, неупередженість); спеціальні принципи використання цифрових технологій у публічному секторі (цифрове за замовчуванням, одноразове введення інформації, сумісність за замовчуванням, інтероперабельність, відкритість, безпека і довіра); та власне принципи обігу віртуальних активів [72, с. 87-89]. Серед останніх для нашого дослідження визначальним є принцип адаптації та подальшого вдосконалення політики у сфері обігу віртуальних активів до стандартів Європейського Союзу - поряд із постійним моніторингом стану регулювання, врахуванням потреб усіх учасників ринку без дискримінації та доброчесністю учасників як умовою їх допуску до ринку [72, с. 88-89]. Запропоноване ним доповнення профільного закону окремою статтею про принципи слід кваліфікувати як пропозицію *de lege ferenda*, а не як чинну норму.

Подальшу систематизацію цих засад здійснив С. В. Цукан, який, розмежувавши типологізацію і класифікацію як споріднені, проте відносно самостійні прийоми пізнання, не лише відтворив триланкову систему О. В. Бондаренка, а й виокремив окрему групу принципів регуляторної діяльності - доцільність, адекватність, ефективність, збалансованість, передбачуваність, прозорість та врахування громадської думки, - а також принципи у сферах оподаткування операцій з віртуальними активами і державного фінансового контролю [73, с. 198-200]. Слід, однак, ураховувати, що перелічену групу регуляторних принципів автор пов'язує зі статтею 14 нечинного Закону № 2074-IX; тому коректно розглядати їх як засади регуляторної політики загалом, а не як чинні приписи саме цього акта.

Наведені доктринальні напрацювання утворюють підґрунтя, на якому має вибудовуватися власна - кримінально-правова - система принципів досліджуваної політики. До неї належать передусім принцип законності криміналізації, що випливає зі статті 92 Конституції України [68] і вимагає визначення кола кримінальних правопорушень виключно законом; принцип юридичної визначеності, який у цій сфері набуває особливої ваги з огляду на бланкетний характер відповідних заборон і незавершеність регулятивного законодавства; принципи пропорційності та гуманності, що обмежують обсяг кримінально-правової репресії й узгоджують її з європейськими стандартами; а також принцип невідворотності кримінальної відповідальності. Зв'язок цих засад із розглянутими вище регулятивними принципами не є механічним: останні визначають зміст того правопорядку, який охороняється кримінальним законом, тоді як кримінально-правові принципи окреслюють допустимі межі та форми самої охорони. Саме тому неповнота або суперечливість регулятивного законодавства (на яку вказують наведені вище автори) безпосередньо позначається на якості кримінально-правової охорони, ускладнюючи дотримання вимоги юридичної визначеності.

Четвертим елементом структури є форми і засоби реалізації політики, з'ясування яких доцільно розпочати від суміжної категорії правового впливу. Д. М. Олійник, чітко розмежувавши «вплив права» як безпосередню дію норм і

ширший за змістом «правовий вплив», що охоплює також правосвідомість і правову культуру, характеризує адміністративно-правовий вплив на ринок віртуальних активів як форму правового впливу, що реалізується державою через органи виконавчої влади та нормативно-правові акти і спрямована на регулювання, організацію, контроль і забезпечення законності та сталого розвитку відносин обігу [74, с. 919-920]. Автор виокремлює три групи ознак такого впливу - загальні, галузеві та інституційні. До галузевих (адміністративно-правових) він відносить, зокрема, публічний характер впливу, його об'єктивацію у відносинах субординації, застосування контролю і нагляду, дозвільних та реєстраційних процедур, заходів примусу і притягнення до адміністративної відповідальності [74, с. 921-922].

Названі засоби належать до адміністративно-правового інструментарію і не повинні ототожнюватися із засобами кримінально-правової політики, якими є криміналізація і декриміналізація діянь, пеналізація і депеналізація, а також застосування покарання та інших заходів кримінально-правового характеру. Водночас сама матриця ознак, запропонована Д. М. Олійником, є корисною аналогією для опису ознак досліджуваної політики, оскільки демонструє поєднання технологічної новизни, транскордонності та потреби в експертному потенціалі суб'єктів, що рівною мірою притаманне і кримінально-правовому реагуванню.

Особливої уваги заслуговує виокремлена Д. М. Олійником інституційна ознака, згідно з якою ринок віртуальних активів не обмежується територією України, а тому правові інструменти повинні враховувати міжнародні принципи і стандарти, зокрема ФАТФ та Європейського Союзу, і потенціал транскордонного співробітництва [74, с. 923]. До завдань відповідного впливу автор відносить, серед іншого, попередження зловживань на ринку, шахрайства, відмивання доходів, одержаних злочинним шляхом, та фінансування тероризму [74, с. 922] - тобто саме тих посягань, протидія яким становить предметне ядро кримінально-правової охорони і докладно аналізується в наступному розділі цієї роботи із застосуванням відповідних статей Кримінального кодексу України [64]. Це підтверджує, що

адміністративно-правовий і кримінально-правовий складники забезпечення охорони віртуальних активів є взаємодоповнювальними: перший формує і підтримує правомірний порядок обігу, другий охороняє його від найбільш небезпечних порушень.

Зі сказаного випливає висновок про співвідношення кримінально-правової політики у досліджуваній сфері з адміністративно-правовим і фінансово-правовим забезпеченням обігу віртуальних активів. Усі три складники мають спільний об'єкт впливу - відносини обігу - і частково спільну суб'єктну систему, проте різняться методом: адміністративно-правове забезпечення діє переважно регулятивними та контрольно-наглядовими засобами, фінансово-правове - засобами фінансового моніторингу і державного фінансового контролю, тоді як кримінально-правова політика застосовує заборонно-охоронний метод. Саме тому остання є субсидіарною щодо регулятивних механізмів: вона вступає в дію там, де регулятивні та адміністративно-деліктні засоби виявляються недостатніми, а її змістове наповнення значною мірою залежить від того, який саме порядок обігу встановлено регулятивним законодавством. Це співвідношення має не лише теоретичне, а й суто практичне значення, позаяк визначає послідовність законодавчих кроків: належна криміналізація посягань у сфері віртуальних активів є можливою лише за умови попереднього або одночасного впорядкування регулятивної основи їх обігу.

Останнє зауваження виводить на ключовий для цього підрозділу висновок щодо джерел досліджуваної політики. Оскільки переважна частина кримінально-правових заборон у сфері обігу віртуальних активів має бланкетний характер, їх зміст визначається не самим кримінальним законом, а тим регулятивним порядком, до якого вони відсилають. В Україні цей порядок перебуває у стані переходу до європейської моделі: модель нечинного Закону № 2074-IX [1] поступається місцем регулюванню за зразком Регламенту МіСА [2], а коло учасників ринку і стандарти їхньої діяльності визначаються відповідно до підходів ФАТФ та Європейського Союзу. Як було показано вище, на цьому наголошують і дослідники забезпечення обігу: принцип

адаптації політики до стандартів Європейського Союзу прямо закладено в систему принципів регулювання [72, с. 88-89]; коло суб'єктів обігу пропонується визначати за міжнародними категоріями постачальників послуг, закріпленими ФАТФ і МіСА [69, с. 98-100]; а транскордонність ринку розглядається як ознака, що зобов'язує враховувати міжнародні принципи і стандарти [74, с. 923].

З огляду на це *визначальним джерелом кримінально-правової політики* у сфері забезпечення охорони віртуальних активів виступає саме законодавство Європейського Союзу і позитивний досвід країн світу: європейська регуляторна модель та міжнародні стандарти не лише формують той правопорядок, який підлягає кримінально-правовій охороні, а й задають зміст бланкетних кримінально-правових заборон, межі допустимої криміналізації та орієнтири гармонізації національної відповідальності. На відміну від традиційних сфер кримінально-правової охорони, де визначальними джерелами політики виступають передусім внутрішні соціально-економічні чинники і національна правова традиція, у сфері віртуальних активів первинним джерелом є зовнішній - наднаціональний - нормативний і досвідний масив, що зумовлено транскордонною природою самих цих активів.

2.3. Міжнародні стандарти та зарубіжний досвід як орієнтири кримінально-правової політики у сфері забезпечення охорони віртуальних активів

2.3.1. Міжнародні стандарти регулювання та охорони віртуальних активів

Віртуальні активи за своєю технологічною й економічною природою є транскордонним явищем: вони створюються, зберігаються та обертаються у децентралізованих мережах поза традиційними фінансовими посередниками й майже з будь-якої точки світу. Ця властивість зумовлює об'єктивну обмеженість суто національних правових механізмів охорони та актуалізує потребу в побудові симетричного міжнародно-правового регулювання, зрозумілого як учасникам ринку, так і національним регуляторам, що спирається на спільні базові принципи [75, с. 229]. Водночас наразі у світі не

сформовано єдиного підходу до регулювання обігу віртуальних активів: швидкість і моделі державного реагування залишаються фрагментованими та неоднорідними, адже кожна держава обирає власний регуляторний вектор відповідно до національних інтересів [75, с. 229]. Саме тому з'ясування змісту міжнародних стандартів у цій сфері є відправним пунктом для формування та реалізації національної кримінально-правової політики: предмет охорони - віртуальні активи - має наднаціональний вимір, а ефективність національних заборон і санкцій безпосередньо залежить від узгодженості вітчизняного правопорядку зі світовими орієнтирами.

Як слушно наголошує А. Пазюк, децентралізована природа віртуальних активів, їх транскордонний обіг та відсутність єдиної правової рамки створюють підвищені ризики у сферах відмивання коштів, фінансування тероризму, шахрайства та кіберзлочинності, а отже кидають виклик класичним принципам міжнародного права, що ґрунтуються на державному суверенітеті й територіальній юрисдикції [76, с. 363, 365]. Подолання цього виклику дослідник убачає в досягненні балансу між цифровим суверенітетом держави та її глобальними зобов'язаннями: національні правові норми мають враховувати особливості конкретної юрисдикції, але водночас бути сумісними з міжнародними стандартами та механізмами транскордонної координації [76, с. 367]. Для кримінально-правової політики такий баланс означає, що криміналізація суспільно небезпечних діянь у сфері віртуальних активів і подальше правозастосування не можуть вибудовуватися ізольовано, у відриві від узгодженого міжнародного стандарту.

Ядром системи міжнародних стандартів у досліджуваній сфері виступають Рекомендації Групи з розробки фінансових заходів боротьби з відмиванням грошей (ФАТФ) - комплексна й узгоджена сукупність заходів, які держави мають імплементувати для протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення [77]. Саме у стандартах ФАТФ закріплено базову дефініцію віртуального активу як цифрового представлення вартості, яким можна торгувати або яке можна передавати в цифровому вигляді та використовувати для цілей платежу чи

інвестицій; при цьому віртуальні активи не охоплюють цифрового представлення фіатних валют, цінних паперів та інших фінансових активів, що вже врегульовані іншими Рекомендаціями [77; 76, с. 365]. Ця дефініція набула значення міжнародного стандарту-орієнтира: її, по суті, відтворено в легальній дефініції статті 1 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [12], який наразі й закріплює чинне в Україні нормативне розуміння віртуальних активів.

Генеza стандартів ФАТФ щодо віртуальних активів відображає поступове розширення мандата цієї міжурядової організації. Як зазначає С. Гончаренко, ФАТФ було створено у 1989 р. на саміті «Великої сімки» в Парижі; у 1990 р. оприлюднено «Сорок рекомендацій», а після терористичних актів 11 вересня 2001 р. систему доповнено спеціальними рекомендаціями щодо протидії фінансуванню тероризму («40 + 9 рекомендацій») [78, с. 129]. Поворотним для сфери віртуальних активів став 2018 рік: у жовтні ФАТФ доповнила Рекомендацію 15 «Нові технології» дефініціями віртуального активу та постачальника послуг, пов'язаних з обігом віртуальних активів, поширивши на відповідну діяльність увесь комплекс вимог щодо протидії відмиванню коштів і фінансуванню тероризму [77; 78, с. 130]. Слід, однак, урахувати, що праця С. Гончаренка датована 2020 роком і фіксує стан правової невизначеності щодо обігу криптовалют в Україні, характерний для 2019-2020 рр.; нині ці оцінки значною мірою подолані з огляду на впровадження національного режиму фінансового моніторингу віртуальних активів, тож відповідні положення доцільно сприймати як історичний зріз генези стандартів ФАТФ, а не як характеристику чинного правопорядку.

Зміст вимог ФАТФ, сконцентрованих у Рекомендації 15 та Пояснювальній записці до неї, полягає в тому, що держави повинні виявляти й оцінювати ризики сектору віртуальних активів, ліцензувати або реєструвати постачальників відповідних послуг і наглядати за ними на тому ж рівні, що й за традиційними фінансовими установами; самі постачальники зобов'язані застосовувати превентивні заходи - належну перевірку клієнтів, ведення обліку

операцій, подання звітів про підозрілі транзакції, зберігання й передання інформації про власників коштів [76, с. 365]. Методологічною основою цього підходу є ризик-орієнтований підхід, за якого інтенсивність регуляторного й наглядового впливу узгоджується з рівнем виявлених ризиків. У жовтні 2021 р. ФАТФ ухвалила Оновлене керівництво щодо застосування ризик-орієнтованого підходу до віртуальних активів і постачальників відповідних послуг, яке зосереджене на шести ключових напрямках: уточненні дефініцій віртуальних активів і постачальників послуг; застосуванні стандартів до стейблкоїнів; протидії ризикам однорангових (peer-to-peer) операцій; ліцензуванні та реєстрації постачальників; запровадженні «правила подорожей»; обміні інформацією між наглядовими органами [79].

Особливе місце серед стандартів ФАТФ посідає «правило подорожей» (travel rule), закріплене Рекомендацією 16. Як докладно показують Т. Дмитренко, О. Любіч та Ю. Пархоменко, це правило, що є аналогом відповідної вимоги Закону США про банківську таємницю, зобов'язує постачальників послуг, які беруть участь у переданні віртуальних активів, отримувати, зберігати й надійно та невідкладно передавати постачальникові-бенефіціарові інформацію про ініціатора й одержувача операції (зокрема ім'я, номер рахунку, адресу) [80, с. 33-34]. Мета цього механізму - забезпечити простежуваність операцій із віртуальними активами та ідентифікацію їх сторін у разі потенційного відмивання коштів чи фінансування тероризму, а ключовим викликом для його дотримання є псевдоанонімність транзакцій [80, с. 34]. Дослідники наводять також таксономію віртуальних активів за невід'ємним ризиком, за якою псевдоанонімні (біткоїн) та анонімні (Monero) активи оцінюються як такі, що мають дуже високий рівень ризику [80, с. 46], і розмежовують суміжні категорії: цифрові валюти центральних банків не визнаються віртуальними активами; децентралізований застосунок сам собою не є постачальником послуг, однак його оператори можуть ним бути; окремі незамінні токени (NFT), що первісно не є віртуальними активами, можуть набувати їх ознак на вторинних ринках [80, с. 42-43]. Для кримінально-правової політики ці класифікації мають безпосереднє значення, оскільки визначають

коло активів і діянь підвищеного ризику й формують предметну базу для предикатних злочинів, насамперед легалізації (відмивання) майна, одержаного злочинним шляхом (стаття 209 Кримінального кодексу України [64]).

Європейський компонент міжнародних стандартів історично формувався в тісному зв'язку з вимогами ФАТФ. П'ята Директива про запобігання використанню фінансової системи для відмивання коштів або фінансування тероризму (5AMLD) поширила режим протидії відмиванню коштів на провайдерів обміну віртуальних активів на фіатні валюти та на постачальників послуг зберігання гаманців [46]. Водночас Т. Дмитренко та О. Любіч ще у 2020 р. констатували, що європейський режим для віртуальних валют уже відставав від чинних на той час стандартів ФАТФ для криптоактивів [81, с. 69]. У вітчизняному правопорядку імплементаційним інструментом став Закон № 361-IX, який, набравши чинності 28 квітня 2020 р., запровадив постачальників послуг, пов'язаних з обігом віртуальних активів (біржі, обмінники), як суб'єктів первинного фінансового моніторингу та розширив коло суб'єктів державного фінансового моніторингу [12; 81, с. 71-72]. Інституційним містком між національним і міжнародним рівнями виступає Комітет експертів Ради Європи з оцінки заходів боротьби з відмиванням грошей і фінансуванням тероризму (Moneyval) - регіональний орган за типом ФАТФ, перед яким Україна звітує щодо імплементації Рекомендацій [81, с. 73-74]. Оцінки 2020 р. слід сприймати з поправкою на час: вони фіксують перехідний момент, коли профільний закон про віртуальні активи перебував іще на стадії проєкту, а тому відповідні положення використовуються тут як історичний зріз генези імплементації міжнародних стандартів, тоді як актуальним регуляторним орієнтиром для України є Регламент (ЄС) 2023/1114 (MiCA) [2].

Поза межами власне стандартів ФАТФ щодо протидії відмиванню коштів і фінансуванню тероризму міжнародна архітектура регулювання охоплює й макрофінансовий контур. Рада з фінансової стабільності (FSB) - дорадчий орган «Групи двадцяти» - у 2023 р. затвердила фінальні Рекомендації високого рівня щодо регулювання, нагляду та спостереження за діяльністю і ринками криптоактивів, які встановлюють глобальну регуляторну базу й ґрунтуються на

принципі «однакова діяльність, однаковий ризик, однакове регулювання» та на технологічній нейтральності [82; 76, с. 366]. Своєю чергою Міжнародний валютний фонд (МВФ) у лютому 2023 р. оприлюднив програмний документ «Елементи ефективної політики щодо криптоактивів», який пропонує членам Фонду дев'ять елементів комплексної політики: забезпечення грошового суверенітету й відмову від надання криптоактивам статусу офіційної валюти чи законного платіжного засобу; запобігання надмірній волатильності потоків капіталу; однозначний податковий режим і розкриття фіскальних ризиків; забезпечення юридичної визначеності та усунення правових ризиків; пруденційні, поведінкові й наглядові вимоги до всіх учасників крипторинку; створення спільної системи моніторингу; запровадження міжнародних механізмів співробітництва; моніторинг впливу криптоактивів на міжнародну валютну систему; зміцнення глобальної співпраці щодо цифрових інфраструктур і транскордонних платежів [83].

Узагальнюючи наднаціональну архітектуру, А. Кудь відносить до кола ключових регуляторів сфери віртуальних активів МВФ, Базельський комітет з банківського нагляду, ФАТФ і Раду з фінансової стабільності, а також форуми держав («Групу двадцяти», Організацію економічного співробітництва та розвитку) [84, с. 60]. Спираючись на оцінки Всесвітнього економічного форуму, дослідник виокремлює три головні перешкоди для досягнення глобального консенсусу: відсутність стандартизованих визначень і таксономій, регуляторний арбітраж та фрагментарність моніторингу, нагляду й правозастосування [84, с. 69-71]. На національному рівні він систематизує п'ять регуляторних підходів - регулювання на основі принципів (очікуваних результатів), ризик-орієнтоване регулювання, гнучке регулювання (із застосуванням «регуляторних пісочниць»), саморегулювання й співрегулювання та регулювання за примусом [84, с. 71-74]. Водночас критичні висновки автора про те, що ні МіСА, ні розроблюваний на його основі український законопроект нібито не обіцяють значного сприяння технологічним інноваціям у сфері забезпечених токенізованих активів [84, с. 77], слід сприймати з обережністю: А. Кудь виступає співрозробником

децентралізованих платформ і відповідних комерційних проєктів, а тому ця позиція є радше пропозицією *de lege ferenda* з боку зацікавленої сторони, ніж нейтральним науковим висновком; описова ж частина його праці щодо складу наднаціональних стандартів зберігає довідкову цінність.

Окремо слід наголосити на проблемі регуляторного арбітражу, що має пряму кримінально-правову релевантність. Нехтування узгодженням національних режимів призводить до того, що постачальники послуг мігрують до найменш контрольованих юрисдикцій, утворюючи «лазівки» для протиправної діяльності [76, с. 365-366]. Звідси випливає, що криміналізація діянь у сфері віртуальних активів і практика її застосування мають спиратися на спільний міжнародний стандарт: прогалина в охороні в одній державі об'єктивно послаблює захищеність відповідних відносин в усіх інших, з якими ця держава пов'язана транскордонним обігом активів.

Таким чином, система міжнародних стандартів регулювання та охорони віртуальних активів є багаторівневою: її ядро утворюють Рекомендації ФАТФ (насамперед Рекомендації 15 і 16), макрофінансовий контур - рекомендації FSB та елементи політики МВФ, а регіональну гармонізацію забезпечує право Європейського Союзу на чолі з Регламентом MiCA. Ці стандарти формують зовнішню рамку, у межах якої Україна як держава-кандидат на членство в ЄС вибудовує національну кримінально-правову політику у сфері забезпечення охорони віртуальних активів [75, с. 233]. Саме вони визначають канонічну дефініцію предмета охорони, окреслюють коло суб'єктів (постачальників послуг) та їхніх обов'язків, виокремлюють діяння підвищеного ризику (відмивання коштів і фінансування тероризму, обхід «правила подорожей») й тим самим задають орієнтири для криміналізації та диференціації відповідальності.

2.3.2. Законодавство і досвід Європейського Союзу та держав-членів Європейського Союзу

Право Європейського Союзу становить основний зовнішній орієнтир кримінально-правової політики України у сфері забезпечення охорони

віртуальних активів. Цей висновок зумовлений не лише загальним зобов'язанням гармонізації, що випливає з Угоди про асоціацію, а й конкретним політико-правовим контекстом: після набуття Україною статусу кандидата на членство в ЄС приведення національного законодавства про віртуальні активи у відповідність до *acquis communautaire* перетворилося з академічної рекомендації на політичне зобов'язання. Цей орієнтир набуває особливого значення з огляду на те, що профільний Закон України «Про віртуальні активи» № 2074-IX [1] залишився невведеним у дію, а отже, зміст суспільних відносин, які мають стати об'єктом кримінально-правової охорони, наразі окреслюється не стільки чинним національним регулюванням, скільки правом ЄС, передусім Регламентом (ЄС) 2023/1114 про ринки криптоактивів (MiCA) [2]. Методологічно це означає, що кримінально-правова охорона віртуальних активів не може випереджати їх регуляторне визначення: межі правомірної діяльності, статус її суб'єктів і перелік охоронюваних благ задаються насамперед регуляторним правом, і саме від його точності залежить можливість коректної кримінально-правової кваліфікації.

Генеza правового статусу постачальників послуг, пов'язаних з оборотом віртуальних активів, у ЄС демонструє, що цей статус формувався поступово й передусім у площині протидії відмиванню коштів. Як показує бібліографічний аналіз ключових документів європейських інституцій, проведений О. А. Музикою-Стефанчук і С. С. Мохнєвим [85, с. 36-40], розвиток правового регулювання загалом збігся з етапами становлення самого ринку: від перших аналітичних документів Європейського центрального банку 2012 року, які давали визначення «віртуальних валют», але не торкалися правового статусу учасників ринку, до попереджень Європейського банківського управління 2013-2014 років, що вперше окреслили коло таких учасників (користувачі, обмінні сервіси, торгові платформи, провайдери гаманців), залишивши їх, однак, поза регуляторним периметром. Показово, що Директива 2009/110/ЄС про електронні гроші (EMD2) [45], у супереч поширеній у літературі думці, поняття криптовалюти не охоплювала, оскільки роботу над її текстом було розпочато ще до появи першої децентралізованої криптовалюти.

Першим інструментом, який реально поширив правові обов'язки на постачальників послуг, стало антивідмивне законодавство. Четверта Директива (ЄС) 2015/849 [86] положень про віртуальні валюти й відповідних провайдерів ще не містила, тоді як П'ята Директива (ЄС) 2018/843 (5AMLD) [46] вперше включила провайдерів гаманців та сервіси обміну віртуальних валют на фіатні кошти до переліку «зобов'язаних осіб» - щоправда, виключно для цілей протидії відмиванню коштів і фінансуванню тероризму, з кінцевим строком транспозиції до 10 січня 2020 року [85, с. 38]. Саме цей крок, на думку дослідників, формально започаткував регулювання постачальників послуг у ЄС. Водночас антивідмивний режим мав суттєві вади: оскільки 5AMLD була директивою, а не регламентом, держави-члени зберігали широку дискрецію, а сам режим не передбачав права «паспортизації» послуг, властивого, наприклад, EMD2 [45] чи Другій платіжній директиві (ЄС) 2015/2366 (PSD2) [87], - що породжувало фрагментацію й регуляторний арбітраж [85, с. 39]. Для цілей цього дослідження принциповим є те, що антивідмивне право стало першою «несучою конструкцією» правової охорони віртуальних активів: ще до спеціального регулювання саме воно запровадило робочі визначення та поширило на ринок обов'язки належної перевірки клієнта, оцінки ризиків і звітування про підозрілі операції.

Системний характер європейської таксономії віртуальних активів і логіку її імплементації ґрунтовно розкриває Т. Л. Дмитренко [88, с. 59-63], яка показує, що правовий режим ЄС вибудовується на розмежуванні трьох категорій активів: криптоактивів, що є фінансовими інструментами (та підпадають під Директиву 2014/65/ЄС про ринки фінансових інструментів), електронних грошей (EMD2) і решти криптоактивів, охоплених MiCA. Дослідниця водночас фіксує термінологічну двоїстість, важливу для подальшої кваліфікації: міжнародні стандарти Групи з фінансових дій (FATF) оперують поняттям «постачальник послуг, пов'язаних з віртуальними активами» (VASP), тоді як MiCA - поняттям CASP, причому ці терміни не є тотожними. Саме імплементація Рекомендації 15 FATF [77] стала відправною точкою національної реформи: в Україні першим кроком став Закон № 361-IX [12],

чинний з 28 квітня 2020 року, який поширив на ринок віртуальних активів заходи з протидії відмиванню коштів [88, с. 66]. Це принципово важливо для кримінально-правової політики, адже саме коло суб'єктів первинного фінансового моніторингу окреслює тих адресатів правових обов'язків, недотримання яких безпосередньо межує з кримінально караною поведінкою.

Антивідмивний пакет ЄС, що став відправною точкою для української реформи, на сьогодні зазнав суттєвого оновлення, яке необхідно враховувати при формуванні перспективної моделі. Регламент (ЄС) 2024/1624 (AMLR) [89] запроваджує єдиний для всього Союзу безпосередньо застосовний звід антивідмивних правил, Директива (ЄС) 2024/1640 (AMLD6) [90] із 10 липня 2027 року скасовує попередні директиви 2015/849 та 2018/843, а Регламент (ЄС) 2024/1620 [91] засновує наднаціональний Орган з протидії відмиванню коштів (AMLA). Окремо слід виділити Регламент (ЄС) 2023/1113 [92], який із 30 грудня 2024 року поширив на перекази криптоактивів так зване «правило подорожі» (Travel Rule), зобов'язавши постачальників послуг супроводжувати перекази інформацією про відправника й одержувача. Для кримінально-правової політики ці зміни мають подвійне значення: по-перше, єдиний звід правил і наднаціональний нагляд звужують простір регуляторного арбітражу, на якому традиційно ґрунтується відмивання коштів через віртуальні активи; по-друге, обов'язкова ідентифікація сторін переказу створює документальну основу для виявлення й доказування відповідних діянь.

Порівняльна картина національного досвіду держав-членів до уніфікації засвідчує саме ту дивергенцію, яку нинішній пакет ЄС покликаний усунути. Узагальнення законодавства десяти держав показує, що антивідмивний режим повсюдно став першою й базовою формою правового «приборкання» віртуальних активів [93, с. 35, 115, 176], а спільною інституційною ознакою стала обов'язкова реєстрація або ліцензування постачальників із прив'язкою до єдиного наглядового органу. Спектр моделей при цьому виявився доволі широким: від реєстраційного треку під егідою центрального банку чи фінрегулятора (Ірландія [93, с. 143], Швеція [93, с. 565], Іспанія [93, с. 155]) і ліцензування обмінників як платіжних установ (Люксембург [93, с. 243]) - до

найсуворішої моделі повноцінного ліцензування криптобірж і кастодіальних сервісів як фінансових послуг із пруденційним наглядом, реалізованої у Німеччині під егідою BaFin [93, с. 286]. Показовим є комплексний французький режим DASP, запроваджений Законом RASTE [93, с. 518-520], а також включення кастодіальних гаманців до кола підзвітних суб'єктів у Бельгії, Данії, Ірландії та Румунії [93, с. 35, 115, 143, 352], що закрило один із головних каналів анонімізації. Застережним є кейс Румунії, зволікання якої з імплементацією 5AMLD спричинило рішення Суду ЄС про невиконання зобов'язань [93, с. 352].

Якісно новий етап охорони пов'язаний із Регламентом MiCA [2], що вперше створив комплексний наднаціональний режим. Як докладно показано у дисертаційному дослідженні Г. І. Воєводиної [94, с. 51-74], MiCA набрав чинності 29 червня 2023 року, а його положення застосовуються з 30 грудня 2024 року (для розділів про токени, забезпечені активами, і токени електронних грошей - з 30 червня 2024 року); регламент запроваджує трикомпонентну класифікацію криптоактивів (токени, забезпечені активами, - ART; токени електронних грошей - EMT; інші криптоактиви, включно зі службовими) і водночас виводить за межі свого застосування унікальні (незамінні) токени, криптоактиви - фінансові інструменти та певні форми децентралізованих фінансів. Слід враховувати, що авторка дослідження афілійована з юридичним консалтингом криптоіндустрії, тож її акценти на інновація-дружньому характері регулювання доцільно сприймати як обґрунтовану позицію, а не як нейтральну даність. Пропоновану MiCA класифікацію корисно зіставити з пре-MiCA підходами: О. І. Кулик [95, с. 71-79] ще до ухвалення регламенту систематизував європейське регулювання за трикласифікацією платіжних, інвестиційних і службових активів, виведеною з директив 2009/110/ЄС, 2015/2366/ЄС, 2014/65/ЄС та 2018/843/ЄС.

Із кримінально-правового погляду найважливішим елементом MiCA є те, що регламент чітко окреслює коло постачальників послуг і перелік самих послуг. На відміну від чотирьох видів послуг, передбачених первинною редакцією Закону № 2074-IX [1], MiCA встановлює десять видів послуг,

запроваджує інститут «білої книги» (whitepaper), фігуру «оферента» та механізм публічної пропозиції, а також єдину авторизацію постачальника з правом «паспортизації» на всю територію Союзу. Порівняльне дослідження В. А. Устименка, Р. А. Джабраїлова та Т. С. Гудіми [96, с. 48-61] демонструє системну невідповідність первинної редакції № 2074-ІХ вимогам МіСА та окреслює напрям гармонізації. Принциповим є те, що саме чітко окреслене коло авторизованих послуг утворює межу між правомірною й неправомірною діяльністю у сфері віртуальних активів, а отже, формує контур об'єкта кримінально-правової охорони й підстави для конструювання відповідних складів, зокрема неліцензованої діяльності постачальника.

Ефективність європейського режиму забезпечується розгалуженою системою наднаціональних і державних органів. Як систематизує Г. І. Воєводіна [97, с. 246-250], ця система має дворівневу архітектуру: на наднаціональному рівні Європейська комісія, Європейське банківське управління (ЕВА), Європейське управління з цінних паперів та ринків (ESMA) і Європейське управління з питань страхування та професійних пенсій (EIOPA), що утворюють спільну систему європейських наглядових органів (ESA), що встановлюють загальні принципи й технічні стандарти; на національному рівні держави-члени транспонують їх, а підрозділи фінансової розвідки й органи пруденційного нагляду здійснюють безпосередній контроль. Елементом цієї системи є й Регламент (ЄС) 2022/2554 про цифрову операційну стійкість фінансового сектору (DORA) [98], що набрав чинності 16 січня 2023 року й застосовується з 17 січня 2025 року, поширюючи на постачальників послуг із криптоактивами вимоги до кіберстійкості - аспект, безпосередньо дотичний до охорони інфраструктури обороту віртуальних активів. Слід зауважити, що в окремих оглядових працях трапляються неточності щодо дат (зокрема, набрання чинності 5AMLD інколи помилково датується січнем 2020 року, тоді як ідеться про строк транспозиції; сама директива набрала чинності 9 липня 2018 року), які при використанні таких джерел слід коригувати за первинними актами.

Окремий пласт європейського досвіду становить судова практика держав-членів, що до уніфікації демонструвала виразний різнобій у кваліфікації віртуальних активів. Порівняльний аналіз Г. І. Воєводиної [99, с. 73-77] показує, що в Польщі біткоїн кваліфікувався судами як майнове право, в Литві - як «інше майно» в розумінні цивільного кодексу (постанова Верховного суду від 22 лютого 2016 року), у Німеччині фінансовий регулятор ще 2013 року визнав віртуальні активи фінансовим інструментом («приватними грошима»), в Австрії - ані фінансовим інструментом, ані платіжним засобом, на Мальті запроваджено категорію «віртуальних фінансових активів», а в Естонії особу, що торгує біткоїном, визнано постачальником послуг альтернативних платіжних засобів (рішення Верховного суду РКНКо 3-3-1-75-15 від 11 квітня 2016 року). Узагальнюючим для цього напрямку є рішення Суду ЄС у справі С-264/14 «Skatteverket v Hedqvist» від 22 жовтня 2015 року [100], яким біткоїн для цілей оподаткування ПДВ визнано засобом платежу. Водночас слід зважати на те, що згадане джерело здебільшого ототожнює віртуальні активи з віртуальними валютами, тоді як у межах цього дослідження обстоюється диференційована родо-видова модель; відповідні приклади доцільно сприймати саме як національні пре-MiCA дефініції «віртуальної валюти», а не як визначення віртуальних активів у широкому значенні.

Особливе значення для теми дослідження має те, що судова кваліфікація віртуальних активів дедалі частіше відбувається саме в кримінально-правовому контексті. Показовим є рішення Касаційного суду Італії № 44378 від 22 листопада 2022 року, ухвалене його Кримінальною палатою у справі про обґрунтованість арешту майна у зв'язку зі «самовідмиванням» (self-laundering): суд визнав, що віртуальний актив може кваліфікуватися як фінансовий продукт незалежно від способу його реалізації на ринку, продовживши лінію, започатковану судом Верони ще 2017 року [99, с. 74-75]. Цей приклад наочно демонструє, що від цивільно-правової та регуляторної кваліфікації віртуального активу безпосередньо залежить визначення предмета й об'єкта в кримінальних провадженнях, зокрема у справах про відмивання коштів.

Найбільш насиченим кримінально-правовим змістом є європейське регулювання інсайдерської інформації та зловживань на ринку віртуальних активів. Як показує В. Г. Ганган [101, с. 49], MiCA у розділі VI (статті 86-92) запроваджує самостійний режим протидії ринковим зловживанням: інсайдерська інформація визначається у статті 87, заборона інсайдерської торгівлі - у статті 89, а заборона маніпулювання ринком - у статті 91. Для тих криптоактивів, що мають ознаки фінансових інструментів (так званих security-токенів), цей режим діє паралельно з Регламентом (ЄС) № 596/2014 про зловживання на ринку (MAR) [102], тоді як критерії віднесення активу до фінансових інструментів визначаються Директивою 2014/65/ЄС (MiFID II) [103]. Слід зазначити, що у вказаному джерелі поняття «внутрішньої інформації» MiCA помилково пов'язане зі статтею 97 регламенту, тоді як насправді його закріплено у статті 87; цю неточність необхідно враховувати при цитуванні.

Для кримінально-правової політики України принциповим є те, що право ЄС містить не лише регуляторний (MAR), а й власне кримінально-правовий шар протидії ринковим зловживанням. Директива 2014/57/ЄС про кримінальні санкції за зловживання на ринку (CSMAD) [104] зобов'язує держави-члени встановити кримінальну відповідальність за інсайдерську торгівлю, незаконне розкриття внутрішньої інформації та маніпулювання ринком принаймні у серйозних умисних випадках, а Директива (ЄС) 2018/1673 про боротьбу з відмиванням коштів засобами кримінального права [105] гармонізує кримінально-правові підходи до легалізації. Саме ці акти, а не лише регуляторні регламенти, утворюють профільний орієнтир для національної криміналізації у сфері охорони віртуальних активів, оскільки демонструють європейський стандарт мінімального обсягу кримінально караних діянь.

У національному праві поняття інсайдерської інформації наразі закріплене статтею 145 Закону України «Про ринки капіталу та організовані товарні ринки» [38] стосовно фінансових інструментів, а кримінальну відповідальність за її незаконне використання передбачено статтею 232-1 Кримінального кодексу України [64]; поняття ж інсайдерської угоди на ринку

віртуальних активів чинне законодавство не охоплює. Проект Закону № 10225 [106] пропонує запровадити для віртуальних активів інститути інсайдерської інформації (стаття 92) та заборони інсайдерської торгівлі (стаття 94), що за змістом відповідають визначенню «внутрішньої інформації» MiCA [101, с. 49-50]. Водночас В. Г. Ганган обґрунтовано критикує запропоноване регулювання за те, що воно не враховує вимог MAR щодо токенизованих фінансових інструментів, унаслідок чого security-токени фактично залишаються поза контролем, а інсайдерські правила обмежуються емітентами службових токенів [101, с. 50-52]. Принциповим є його висновок про те, що дефініцію інсайдерської інформації слід уточнити відповідно до Регламенту (ЄС) № 596/2014, аби в процесі застосування статті 232-1 КК України не виникало проблем із правовою кваліфікацією предмета кримінального правопорушення [101, с. 53-55], - теза, що прямо стосується бланкетного характеру відповідної кримінально-правової норми.

Європейська судова практика дає й змістовний орієнтир для тлумачення відповідних дефініцій. У рішенні Суду ЄС у справі C-628/13 «Lafonta проти AMF» від 11 березня 2015 року [107] сформульовано чотири елементи поняття «inside information» і, що важливо, встановлено, що інформація вважається точною навіть тоді, коли вона не дає змоги передбачити напрям зміни ціни фінансового інструменту [101, с. 52-53]. Цей підхід є цінним орієнтиром для визначення предмета не лише статті 232-1, а й статті 222-1 КК України про маніпулювання на ринку в частині, що стосуватиметься віртуальних активів.

Імплементація європейської моделі класифікації та статусу постачальників у національне право відбувається через перегляд профільного закону. С. О. Грицай [108, с. 74-78] показує, що відповідальним органом в Україні визначено Національну комісію з цінних паперів та фондового ринку, а реформа передбачає розширення переліку послуг із чотирьох до десяти, заміну поділу на забезпечені й незабезпечені активи трикласифікацією ART/EMT/службові токени, запровадження «білої книги» та фігури «оферента», а також створення регуляторних «пісочниць» для децентралізованих фінансів і незамінних токенів, що не охоплюються MiCA

повною мірою. Слід враховувати, що це джерело подає вже застарілі прогнози щодо набрання чинності МіСА, які необхідно коригувати за первинним актом [2]. Деталізованіший зріз пропонованої редакції містить Т. П. Овсійчук [109, с. 69-72], яка аналізує проєкт № 10225: віртуальний актив визначається в ньому як «цифрова річ» у розумінні статті 179-1 Цивільного кодексу України [27], доданої Законом № 3320-IX [28], що, як зазначає й Є. О. Мічурін [62], дає підстави застосовувати до віртуальних активів режим речових прав; класифікація активів приводиться у відповідність до МіСА, а закон уперше врегульовує майнінг та обмежує організаційно-правові форми постачальників послуг.

Імплементацийний вимір має й антивідмивну складову, що безпосередньо межує з кримінально-правовою політикою. Т. Л. Дмитренко [88, с. 65-68] докладно окреслює коло підзаконних актів, які мають розробити Національна комісія з цінних паперів та фондового ринку й Державна служба фінансового моніторингу для запровадження ризик-орієнтованого підходу відповідно до Рекомендації 1 FATF [77]. Деталізований режим фінансового моніторингу є предметом окремого аналізу в подальших підрозділах дослідження; для цілей цього підрозділу істотно, що постачальники послуг із віртуальними активами стають суб'єктами первинного фінансового моніторингу, а порушення ними відповідних обов'язків безпосередньо межує з діями, що утворюють відмивання коштів чи обхід санкцій.

Перспективи загальноєвропейського регулювання, окреслені в літературі [110, с. 240-244], пов'язуються з динамічним оновленням правил, технологічною нейтральністю, розвитком наглядових технологій (RegTech і SupTech), регуляторними «пісочницями» та глобальною координацією через FATF, Міжнародну організацію комісій з цінних паперів (IOSCO) і G20. Хоча відповідне джерело має радше форсайтний характер, його висновки корисні для України: регуляторні «пісочниці» й аналітичні інструменти нагляду слугують засобами ранньої локалізації ризиків, зокрема відмивання коштів, які логічно передують криміналізації й дають змогу диференціювати справді суспільно небезпечні дії від звичайних регуляторних порушень.

Узагальнюючи європейський досвід під кутом зору кримінально-правової політики, можна сформулювати кілька висновків. По-перше, право ЄС задає регуляторний каркас, у межах якого тільки й може формуватися кримінально-правова охорона віртуальних активів: об'єкт охорони окреслюється через статус постачальника послуг (CASP), класифікацію активів і режим публічної пропозиції та «білої книги». По-друге, європейський досвід чітко вирізняє три магістральні напрями криміналізації: протидія відмиванню коштів (5AMLD [46], оновлений пакет AMLR/AMLD6 [89; 90], Директива 2018/1673 [105] та Travel Rule [92]), що співвідноситься зі статтею 209 КК України й системою фінансового моніторингу; протидія ринковим зловживанням (MAR [102] і CSMAD [104] у поєднанні з розділом VI MiCA), що співвідноситься зі статтями 232-1 та 222-1 КК України; нарешті, протидія неліцензованим і недобросовісній діяльності постачальників послуг. По-третє, необхідною умовою успішної криміналізації є точність регуляторних дефініцій, оскільки відповідні кримінально-правові норми мають переважно бланкетний характер, - на чому прямо наголошують і вітчизняні дослідники [101, с. 53-55], і практика Суду ЄС [107].

По-четверте, формуючи перспективну національну модель, слід зважати на те, що Закон № 2074-IX [1] так і не запроваджено в дію, а отже, орієнтиром має слугувати не його первинна редакція, а актуальний проект змін [106] та його доопрацьовані версії. Так само неприпустимо будувати національну кримінально-правову політику на застарілих проектних редакціях актів ЄС: орієнтуватися належить на чинний пакет - MiCA [2], MAR [102], CSMAD [104], антивідмивний пакет 2024 року [89; 90; 91] і Travel Rule [92]. Саме узгодженість національних дефініцій із цими актами є передумовою того, щоб кримінально-правова охорона віртуальних активів в Україні була не декларативною, а здатною до практичного застосування.

2.3.3. Досвід окремих держав, які не є членами ЄС

З'ясувавши міжнародні стандарти регулювання та охорони віртуальних активів (підрозділ 2.3.1) і модель Європейського Союзу та держав-членів ЄС

(підрозділ 2.3.2), доцільно звернутися до досвіду окремих зарубіжних держав, що не входять до ЄС. Такий аналіз має на меті не стільки опис іноземного регулювання, скільки виокремлення придатного для запозичення позитивного досвіду, що слугуватиме орієнтиром для формування національної кримінально-правової політики у сфері забезпечення охорони віртуальних активів. Власне національний стан розглядається окремо (підрозділ 2.4), тоді як тут увагу зосереджено на зарубіжних моделях, згрупованих за правовими сім'ями та регіонами. Аналіз провадиться передусім крізь призму протидії відмиванню коштів і фінансуванню тероризму, відповідно до Рекомендації 15 ФАТФ [77], розглянутої в підрозділі 2.3.1, з урахуванням режиму постачальників послуг, пов'язаних з обігом віртуальних активів, і кримінального правозастосування.

Європейські держави, що не входять до ЄС, демонструють відмінні регуляторні філософії, які, попри спільну відправну точку - антивідмивний режим, - суттєво різняться за інтенсивністю втручання: від реєстраційної моделі Великої Британії, через мінімалістичне «лише-ПВК» охоплення в Норвегії, до швейцарської моделі саморегулювних організацій, доповненої комплексним законодавством про технологію розподіленого реєстру. Зіставлення цих підходів дає Україні корисний діапазон рішень - від «легкого» до «насиченого» регулювання.

Основою британського режиму є Положення від 22 червня 2017 року № 692 про відмивання коштів, фінансування тероризму та переказ коштів, дія якого з 10 січня 2020 року поширена на фірми, що провадять діяльність із криптоактивами, - постачальників послуг з обміну криптоактивів і постачальників послуг зі збереження гаманців [93, с. 87]. Прикметним є широке, технологічно нейтральне визначення криптоактиву як криптографічно захищеного цифрового представлення вартості або договірних прав на основі технології розподіленого реєстру. Для провадження діяльності такі постачальники зобов'язані зареєструватися в Управлінні з фінансового регулювання та контролю (FCA) і виконувати ризик-орієнтовані обов'язки з виявлення та оцінки ризиків відмивання коштів і фінансування тероризму [93,

с. 87]. Біржі віртуальних валют кваліфікуються як постачальники послуг з обміну криптоактивів і підлягають тій самій реєстрації; якщо ж відповідні активи є фінансовими інструментами, додатково застосовуються правила ринку фінансових інструментів [93, с. 90]. Цей вектор згодом отримав розвиток: ще консультаційний документ Казначейства (січень 2021 року) пропонував спершу включити стейблкоїни до регуляторного периметра, а далі запровадити ширші зміни [93, с. 106], і вже після підготовки огляду Велика Британія, що не входить ні до ЄС, ні до Європейського економічного простору, послідовно розбудовує власний режим у межах наявної фінансової архітектури. Передісторію цього курсу відображають і ранні кроки: ще з 2014 року Банк Англії досліджував ризики цифрових валют для кредитно-грошової системи, дійшовши висновку про мінімальність ризиків і доцільність регулювання задля запобігання злочинному використанню, а ініціатива Project Innovate надала FCA додаткові повноваження з консультування учасників ринку [111, с. 21]. Сильні сторони британської моделі для запозичення - концентрація нагляду в єдиного регулятора, «майбутньостійке» визначення предмета регулювання та поетапне розширення периметра.

Норвезький підхід ілюструє межі суто антивідмивного регулювання. Закон про боротьбу з відмиванням грошей, чинний з 15 жовтня 2018 року, імплементував Четверту директиву ЄС [86] та окремі положення Директиви (ЄС) 2018/843 [46], поширивши сферу дії на постачальників послуг обміну між віртуальними та фіатними валютами й на постачальників кастодіальних гаманців, які відтепер є зобов'язаними суб'єктами [93, с. 297]; нагляд і реєстрацію здійснює Управління фінансового нагляду. Водночас спеціального режиму ліцензування бірж на момент підготовки огляду не було: діяльність бірж не підпадала під регулювання фінансових послуг, якщо вони не надавали послуг обміну або кастодіального зберігання [93, с. 299], а самі норвезькі регулятори визнавали, що для повноцінного охоплення довелося б змінювати профільне законодавство [93, с. 305]. Прикметно, що цю прогалину Норвегія закриває саме в напрямі ринкового регулювання: як держава Європейського економічного простору вона імплементує MiCA окремим актом про

криптоактиви через відсилання до регламентів ЄС. Звідси урок для України: антивідмивне охоплення є необхідною, але недостатньою умовою - без ринкового регулювання залишаються прогалини.

Швейцарія репрезентує найбільш насичену модель з-поміж розглянутих держав, причому її доцільно реконструювати з кількох джерел. Антивідмивну основу становлять Федеральний закон від 10 жовтня 1997 року про боротьбу з відмиванням коштів та фінансуванням тероризму і Постанова Федеральної ради від 11 листопада 2015 року; вони поширюються, зокрема, на фінансових посередників, до яких належить будь-яка особа, що на професійній основі залучає, утримує чи депонує чужі активи або сприяє їх інвестуванню [93, с. 542]. Характерною рисою є те, що фінансовий посередник зобов'язаний бути пов'язаним з уповноваженою саморегульовною організацією (СРО) з протидії відмиванню коштів, виконувати обов'язки з ідентифікації та «знай свого клієнта» щодо сторін і бенефіціарних власників, а також повідомляти про підозри до відповідного інформаційного управління [93, с. 542]. Цю антивідмивну рамку доповнює Федеральний закон про адаптацію федерального права до розвитку технології розподіленого електронного реєстру (чинний із серпня 2021 року), який запровадив окрему категорію ліцензій для торговельних майданчиків, де торгуються DLT-права, що розглядаються як цінні папери [93, с. 546], усунувши значні перешкоди для функціонування первинного й вторинного ринків токенизованих прав [93, с. 556]. Докладнішу картину дає аналіз класифікації віртуальних активів, здійсненої Швейцарською службою нагляду за фінансовими ринками (FINMA): у Керівних принципах щодо первинного розміщення монет (2018) застосовано примат економічної сутності над формою, за яким віртуальні активи поділено на платіжні токени, токени активів, службові токени та згодом стейблкоїни [112, с. 45]. Платіжні токени (криптовалюта) не визнаються цінними паперами, проте їх емітенти підпадають під антивідмивне законодавство як фінансові посередники; токени активів кваліфікуються як цінні папери у значенні законів про інфраструктуру фінансового ринку та про фондові біржі; службові токени за загальним правилом виведено з-під антивідмивних вимог, окрім випадку додаткової

інвестиційної мети [112, с. 45-48]. Конкретні заходи державного регулювання доповнюють цей портрет: ліцензування діяльності учасників ринку, реєстрація торговельних майданчиків, вимоги до статутного капіталу, аудит звітності та нагляд з боку FINMA [113, с. 139]. Поєднання CPO-моделі (делегований комплаєнс під наглядом регулятора), класифікаційної визначеності й інфраструктурного ліцензування робить швейцарський досвід особливо показовим: він демонструє, що чіткість класифікації безпосередньо посилює правову визначеність щодо застосовних норм, а отже - і щодо предмета кримінально-правової охорони.

Зіставлення трьох європейських поза-ЄС юрисдикцій підтверджує висновок, зроблений на матеріалі держав ЄС: антивідмивний режим усюди є відправною формою регулювання, проте інтенсивність охоплення суттєво різниться. Для України з цього випливає кілька орієнтирів: широке технологічно нейтральне визначення криптоактиву (британський зразок) придатне для майбутньостійкого формулювання предмета регулювання; швейцарська CPO-модель пропонує життєздатну со-регуляторну опцію делегування частини комплаєнс-функцій під наглядом державного регулятора; норвезький випадок застерігає від обмеження реформи лише антивідмивним блоком, без ринкового регулювання за моделлю MiCA [2].

Північноамериканська модель вирізняється тим, що не створює для віртуальних активів окремої регуляторної категорії «з нуля», а інтегрує їх у наявний режим суб'єктів грошових послуг, доповнюючи його потужними кримінально-правовими нормами про відмивання коштів та активним, зокрема екстериторіальним, правозастосуванням. Базовим федеральним актом США є Закон про банківську таємницю (§§ 5311-5332 розділу 31 Кодексу США), що покладає на фінансові установи обов'язки з протидії відмиванню коштів [93, с. 426]; адміністратором і органом фінансової розвідки виступає FinCEN. Прикметною є технологічно нейтральна техніка охоплення ринку: ще у 2011 році FinCEN розширив поняття переказу коштів, додавши «вартість, яка замінює валюту», аби підвести діяльність із віртуальними валютами під дію закону, а у 2020 році Закон про протидію відмиванню коштів розширив

визначення фінансової установи [93, с. 426]. Антивідмивну рамку посилює кримінально-правовий блок: відмивання коштів криміналізоване у §§ 1956 і 1957 розділу 18 Кодексу США [93, с. 426], і саме широке формулювання цих приписів дало змогу поширювати їх на складні цифрові схеми та реалізовувати екстериторіальне правозастосування щодо найбільших учасників ринку. Складність американського регулювання обумовлена співвідношенням федерального права і права штатів та відсутністю єдиної позиції щодо статусу криптовалюти, яка розглядається водночас як кошти, як власність і як біржовий товар; криптокомпанії реєструються федерально як оператори з переказу коштів і у FinCEN, а на рівні штатів отримують ліцензії [111, с. 21]. Як зауважують дослідники, у США немає єдиного федерального закону про віртуальні активи, а сферу регулюють кілька органів (Комісія з цінних паперів і бірж, Комісія з торгівлі товарними ф'ючерсами, Служба внутрішніх доходів, FinCEN), причому акцент робиться на протидії шахрайству та захисті інвесторів за допомогою чинного законодавства, а не на створенні спеціального [114, с. 621].

У Канаді антивідмивну систему очолює Центр аналізу фінансових операцій та звітів (FINTRAC), відповідальний за виконання Закону про доходи, одержані злочинним шляхом, і фінансування тероризму; постачальники послуг із віртуальними валютами кваліфікуються як суб'єкти грошових послуг і підлягають реєстрації, ідентифікації клієнтів, веденню обліку та звітуванню про підозрілі операції [93, с. 221]. Заходи державного регулювання деталізують і профільні дослідження: реєстрація провайдерів грошових послуг у FINTRAC, упровадження процедури «знай свого клієнта», подання фінансової звітності, покладення функцій нагляду на службу комплаєнсу та вимога залучення спеціаліста з комплаєнсу [113, с. 138-139]. Особливістю канадської системи є дворівневість: поряд із федеральним антивідмивним наглядом діє провінційне регулювання ринку цінних паперів [93, с. 221]. Координація федерального й провінційного рівнів є ключем до повноти охоплення. Для України з північноамериканського досвіду впливає таке: функціональне, технологічно нейтральне перевизначення наявних понять дає змогу охопити ринок без

тривалого створення нового спеціального статусу; інституційну спроможність національного органу фінансової розвідки (Державної служби фінансового моніторингу) доцільно посилювати за функціональним аналогом FinCEN і FINTRAC; кримінально-правова складова (передусім стаття 209 Кримінального кодексу України [64]) має надійно охоплювати схеми з використанням віртуальних активів, проте, як свідчить цей досвід, акцент доцільно робити на якості наглядово-регуляторного механізму та правозастосуванні, а не лише на редагуванні диспозиції.

Азійські держави демонструють два протилежні полюси регуляторної зрілості: розвинені фінансові хаби з комплексними режимами та юрисдикції з тривалою регуляторною невизначеністю. Сінгапурський режим протидії відмиванню коштів значною мірою відповідає рекомендаціям ФАТФ [77]; принципово важливою є позиція тамтешнього грошово-кредитного управління, за якою для послуг із цифровими платіжними токенами не передбачено підгрупи з низьким рівнем ризику - усі постачальники таких послуг зобов'язані дотримуватися заходів протидії відмиванню коштів і фінансуванню тероризму [93, с. 375]. Інституційно ринок структуровано за функціональним призначенням: платформи обміну цифрових платіжних tokenів кваліфікуються як платіжні послуги й потребують ліцензії, тоді як платформи інвестиційних tokenів підпадають під законодавство про цінні папери [93, с. 376]. Японія є одним із піонерів регулювання: послуги з обміну криптоактивів регулюються законом про платіжні послуги, за яким відповідні особи мають бути зареєстровані як надавачі послуг з обміну криптоактивів із квазіпруденційними вимогами до капіталу та організаційної структури [93, с. 578], а антивідмивну складову забезпечує закон про запобігання переказу доходів від злочинної діяльності з обов'язками «знай свого клієнта» та звітування [93, с. 577].

Особливий інтерес становить досвід Спеціального адміністративного району КНР Гонконг, який, користуючись високим ступенем автономії, проводить політику, протилежну материковій [115, с. 207]. Легальну дефініцію віртуального активу закріплено в секції 53ZRA Закону про протидію відмиванню коштів та фінансуванню тероризму як криптографічно захищеного

цифрового вираження вартості, що використовується як засіб обміну, оплати чи інвестування, з виключенням цифрових валют центрального банку, токенів обмеженого призначення, цінних паперів і депозитів засобу зберігання вартості [115, с. 208]. Прикметним є прецедентне визнання криптовалюти власністю у справі *Re Gatecoin Ltd* (2023) з можливістю бути предметом трасту [115, с. 209]. Найважливішим для цілей кримінально-правової політики є режим ліцензування: з 1 червня 2023 року запроваджено систему ліцензування операторів платформ для торгівлі віртуальними активами з вимогою подвійного ліцензування - за законом про цінні папери та ф'ючерси і за антивідмивним законом, - причому надання таких послуг без ліцензії становить кримінальне правопорушення, що тягне штраф і позбавлення волі для відповідальних осіб [115, с. 209]. Гонконгівський законодавець рекомендує закладати регулювання в єдиному нормативному акті, узгодженому з MiCA [2], а не таким, що йому суперечить [115, с. 209-210]. Натомість індійський випадок ілюструє ризики правової невизначеності: спеціального регулювання бірж немає, норми «знай свого клієнта» поширюються лише на обмежене коло суб'єктів, а де-факто банківські обмеження витісняють діяльність у менш прозорі форми [93, с. 128-129]. Азійський блок дає Україні позитивний і застережний орієнтири: ліцензування постачальників послуг у єдиного фінрегулятора з універсальним антивідмивним охопленням без «пільгових» винятків, функціональне розмежування платіжного та інвестиційного треків, а також - що принципово для кримінально-правового виміру - модель, за якої неліцензована діяльність оператора платформи сама собою є кримінальним правопорушенням.

Близькосхідно-офшорна група репрезентує найбільш інституційно спеціалізовані моделі - від спеціальних законів про постачальників послуг віртуальних активів до окремих профільних регуляторів, - однак саме тут потрібна методологічна обережність. В Об'єднаних Арабських Еміратах антивідмивну основу становлять Декретний федеральний закон 2018 року № 20 і Постанова Кабінету Міністрів 2019 року № 10 [93, с. 318]; на цьому фундаменті в «оншорній» частині Положення Управління з цінних паперів та

товарів від 31 жовтня 2020 року вимагає ліцензії для управління біржею криптоактивів, а паралельно діють спеціалізовані режими фінансових вільних зон, зокрема настанови регулятора Глобального ринку Абу-Дабі [93, с. 326]. Кайманові Острови дають взірець спеціального профільного акта: Закон про віртуальні активи та постачальників послуг набув чинності 31 жовтня 2020 року з поетапним переходом від реєстрації до ліцензування та регуляторною «пісочницею» [93, с. 187], а антивідмивний контур забезпечує закон про доходи, одержані злочинним шляхом, із прямим включенням послуг з віртуальних активів до «відповідного фінансового бізнесу» [93, с. 193]. Для України практично цінними є саме архітектурні рішення - поетапний механізм «реєстрація → ліцензування» та інститут регуляторної «пісочниці», - однак, із міркувань академічної об'єктивності, наголосимо: запозичувати слід регуляторну техніку цих юрисдикцій, а не їхні низькоподаткові чи пов'язані з конфіденційністю риси, які створюють ризики регуляторного арбітражу.

Окрему групу становлять ринки, що розвиваються, цінність яких для дослідження є переважно застережною. В Аргентині єдиним спеціальним актом щодо криптовалют є Резолюція підрозділу фінансової інформації № 300/2014, що, прикметно, вимагає звітувати про всі операції з криптовалютами незалежно від суми [93, с. 20]. У Бразилії спеціального антивідмивного режиму для операцій з віртуальними валютами на момент огляду не було, а загальний закон поширювався лише на обмежене коло осіб [93, с. 61]. У Нігерії проблемою є суперечливість позицій регуляторів: обмежувальна лінія центрального банку співіснувала з більш відкритим підходом комісії з цінних паперів [93, с. 257]. В Азербайджані спеціального регулювання немає, а антивідмивне законодавство не проводить істотної різниці між операціями з фіатною та віртуальною валютою [93, с. 12]. Для України звідси впливає потреба чіткого розмежування повноважень між Національним банком України і Національною комісією з цінних паперів та фондового ринку, аби уникнути конфлікту регуляторів, а також прямого включення постачальників послуг до периметра фінансового моніторингу. Самостійний полюс діапазону утворюють держави, що пішли шляхом заборони або обмеження обігу віртуальних активів, - зокрема

Китай, В'єтнам і Болівія [113, с. 137; 111, с. 20]. Цей досвід становить інтерес радше як застереження: абсолютна заборона не усуває попиту, а витісняє відповідну діяльність у тіньовий сегмент, ускладнюючи її контроль і кримінально-правову оцінку.

Підсумовуючи регуляторний огляд, доцільно окремо зупинитися на кримінально-правовому вимірі зарубіжного досвіду, що становить безпосередній інтерес для цього дослідження. На рівні міжнародного стандарту опорними є Рекомендації ФАТФ [77]: криміналізація відмивання коштів, одержаних від тяжких злочинів (Рекомендація 4), та арешт і конфіскація злочинних доходів (Рекомендація 7) [116, с. 698]. Водночас, як слушно зауважують дослідники, застосування цих стандартів не повинно перетворюватися на запровадження надмірних заборонних приписів: критику в цьому контексті дістала, зокрема, норма пункту 8 частини 4 статті 9 Закону України «Про віртуальні активи» [1] (який, утім, не набрав чинності) щодо заборони статусу постачальника послуг для осіб із засновниками з «недобросовісних» юрисдикцій [116, с. 699]. Це застереження актуальне для української кримінально-правової політики: імплементація стандартів має бути пропорційною й не підміняти регуляторні механізми надмірною криміналізацією чи заборонами.

Емпіричний зріз іноземного правозастосування демонструє як небезпеки, так і дієві інструменти протидії. Серед резонансних справ - злам японської біржі «Mt.Gox» (2011-2014), за результатами якого Окружний суд Токіо засудив колишнього керівника біржі за підробку документів [117, с. 82-83]; виведення коштів із платформи «Poly Network» (2022), коли прозорість блокчейну та аналітичні інструменти унеможливили відмивання й спонукали зловмисника повернути активи [117, с. 83]; нарешті, справа біржі «Bitfinex», у якій після арешту 2022 року обвинуваченим у змові з метою відмивання коштів було погоджено покарання у виді позбавлення волі, а виявлені віртуальні активи піддано безпрецедентній конфіскації на суму близько шести мільярдів доларів США (за оцінкою на момент розслідування), частину якої спрямовано на відшкодування шкоди потерпілим [117, с. 83-84]. Останній приклад

особливо показовий для української кримінально-правової політики, оскільки демонструє реальну можливість конфіскації віртуальних активів і відшкодування шкоди - що кореспондує з Рекомендацією 7 ФАТФ [77] та з потребою вдосконалення відповідного інституту в національному праві.

Не менш важливим є інституційний орієнтир: у США для координації протидії злочинності у сфері віртуальних активів створено спеціалізовану Національну групу з питань криптовалют у складі Кримінального департаменту Міністерства юстиції, що зосереджується на біржах, сервісах змішування та провайдерах інфраструктури й координує співпрацю з державними органами та приватним сектором [117, с. 84]. Дієвість міжнародної співпраці підтверджує і скоординована ліквідація даркнет-маркетів «AlphaBay» та «Hansa» (2017) за участю правоохоронних органів кількох держав і Європолу [117, с. 85]. Узагальнюючи, дослідники виокремлюють чотири чинники ефективної протидії: розробку правового регулювання обігу віртуальних активів; співпрацю правоохоронних органів з учасниками ринку; використання спеціальних інструментів відстеження транзакцій; міжнародну співпрацю [117, с. 84-85]. Звідси випливає принциповий висновок: кримінально-правовий примус у цій сфері є дієвим не сам собою, а в поєднанні з аналітичною спроможністю, наглядово-регуляторним механізмом і міжнародною кооперацією.

Проведений аналіз дозволяє узагальнити спільні закономірності й сформулювати орієнтири для кримінально-правової політики України. По-перше, у всіх розглянутих державах антивідмивний режим є відправною, несучою конструкцією правової охорони віртуальних активів, тоді як національні моделі різняться передусім інтенсивністю нагляду - від реєстрації постачальників послуг (Велика Британія, Норвегія, США, Канада) через ліцензування з квазіпруденційними вимогами (Японія) і спеціальні профільні закони з поетапним переходом «реєстрація - ліцензування» (Кайманові Острови) до моделі саморегулювних організацій, доповненої інфраструктурним ліцензуванням (Швейцарія). По-друге, найкращі зразки поєднують юридичну точність із технологічною нейтральністю дефініцій, що безпосередньо корисно

для уточнення предмета регулювання й, відповідно, предмета кримінально-правової охорони. По-третє, у вимірі взаємодії з кримінальним правом більшість юрисдикцій спирається на загальні кримінально-правові норми в поєднанні з антивідмивним режимом, тоді як США демонструють потужні спеціальні приписи про відмивання та практику екстериторіального примусу; звідси випливає, що кримінально-правові засоби доцільно застосовувати як крайні (*ultima ratio*) у межах узгодженого регуляторно-запобіжного механізму, з акцентом на якості нагляду, аналітичній спроможності органу фінансової розвідки та дієвому правозастосуванні. По-четверте, окремі моделі дають застережні уроки: регуляторна невизначеність та міжвідомчий конфлікт не знижують ризиків, а витісняють ринок у менш прозорі форми, що актуалізує потребу правової визначеності та чіткого розподілу повноважень між Національним банком України і Національною комісією з цінних паперів та фондового ринку. Нарешті, гонконгівський досвід криміналізації неліцензованої діяльності операторів платформ, американська модель спеціалізованої інституції протидії та практика конфіскації віртуальних активів окреслюють конкретні напрями вдосконалення національної кримінально-правової політики в умовах підготовки до імплементації MiCA [2] та оновлення профільного законодавства, що має замінити Закон, який не набрав чинності [1], відповідно до чинного реформаторського вектора (проект № 10225-д) [106].

2.4. Національне регулювання обігу віртуальних активів як нормативна основа кримінально-правової політики: чинний стан і напрями реформування

Аналіз міжнародних, європейських і зарубіжних моделей регулювання обігу віртуальних активів, здійснений у попередніх підрозділах, дає підстави перейти до національного рівня - до того нормативного середовища, у якому має формуватися й діяти кримінально-правова політика України у сфері охорони обігу ВА. Кримінально-правова політика не є самодостатньою: криміналізація, пеналізація та правозастосування у будь-якій сфері спираються на регулятивну основу, що визначає правомірну поведінку, окреслює предмет

охорони й задає межі дозволеного. Стосовно ВА така основа в Україні перебуває у стані переходу: профільний Закон України «Про віртуальні активи» від 17.02.2022 № 2074-IX [1] лишається нечинним, тоді як орієнтиром подальшого реформування слугує Регламент (ЄС) 2023/1114 про ринки криптоактивів (MiCA) [2], а до запровадження профільного режиму обіг ВА регулюється фрагментарно - насамперед через Закон України № 361-IX [12] та консолідований законопроект № 10225-д [106]. Саме ця нормативна невизначеність формує специфічне середовище, у якому належить діяти кримінальному закону (КК України [64]), тому з'ясування чинного стану й напрямів реформування національного регулювання є необхідною передумовою оцінки кримінально-правових засобів охорони обігу ВА.

Вихідним пунктом є констатація розриву між де-юре закладеною та де-факто наявною моделлю регулювання. Як показують Т. Гудіма та інші [118, с. 137, 140-141], попри ухвалення профільного закону практика використання ВА - Національним банком України, органами державної влади, суб'єктами господарювання та фізичними особами - розгорталася за умов несформованості системи регулювання; відтермінування набрання чинності ключовим актом породжує «сірі зони», існування яких несумісне із засадами правової держави, зокрема з юридичною визначеністю та легітимними очікуваннями як складниками верховенства права. Причина нечинності має суто нормативний характер: момент набрання чинності Законом № 2074-IX [1] прив'язано до набрання чинності законом про внесення змін до Податкового кодексу України (ПКУ) щодо оподаткування операцій з ВА [118, с. 138]. С. Грицай [119, с. 66] уточнює, що відкладальна умова є подвійною: за пунктом 1 розділу VI «Прикінцеві та перехідні положення» закон набере чинності з дня набрання чинності законом про відповідні зміни до ПКУ, а застосування санкцій за порушення вимог до постачальників послуг додатково обумовлене впровадженням Державного реєстру постачальників послуг, пов'язаних з оборотом ВА. Отже, чинним станом національного регулювання обігу ВА є саме нечинність профільного закону, а не його дія.

Зміст закладеної, але незапущеної моделі окреслює коло відносин, які мають стати предметом правової охорони. За Законом № 2074-IX ВА визначено як нематеріальне благо - об'єкт цивільних прав, що має вартість і виражене сукупністю даних в електронній формі; активи поділено на забезпечені та незабезпечені, причому забезпечений ВА посвідчує майнові права, а незабезпечений - не посвідчує жодних прав [119, с. 66]. Усередині забезпечених («фінансових») ВА закон вирізняє забезпечені валютними цінностями (ЗВА(ВЦ)) та забезпечені цінним папером чи деривативним фінансовим інструментом (ЗВА(ФІ)), оборот яких віднесено відповідно до компетенції НБУ та НКЦПФР [119, с. 66-67]. Цей зміст слід читати з огляду на чинне цивільне законодавство: як зауважує І. Верес [120, с. 104], ЦК України доповнено статтею 179-1 (цифрова річ), різновидом якої є ВА, - тобто загальний цивільно-правовий режим уже діє, тоді як профільний спеціальний режим залишається відкладеним. Зіставлення національної класифікації (забезпечені / незабезпечені) з функціональною типологією MiCA [2] - токен, прив'язаний до активу (ART), токен електронних грошей (EMT), інші криптоактиви - виявляє суттєве розходження підходів [120, с. 104-105], що згодом стане одним із напрямів реформування.

Закладена модель містить і внутрішню неузгодженість, яка прямо стосується предмета майбутньої охорони: частина 7 статті 4 Закону № 2074-IX встановлює, що ВА не є засобом платежу і не можуть бути предметом обміну на майно, роботи чи послуги, тоді як пункт 13 частини 1 статті 1 Закону № 361-IX [12] визначає ВА як цифрове вираження вартості для платіжних або інвестиційних цілей; таке звуження функцій у профільному законі суперечить уже наявним нормам і світовим тенденціям, послаблюючи юридичну визначеність [118, с. 140]. Просторово-суб'єктні межі дії закону окреслює С. Грицай [121, с. 57], відносячи до складу законодавства про ВА Конституцію України [68], міжнародні договори, ЦК України, сам Закон № 2074-IX, Закон № 361-IX [12] та інші акти, а сферу застосування - до правовідносин за наявності територіальної прив'язки (місцезнаходження чи представництво постачальника в Україні, вибір права України, резидентність сторін). Водночас автор слушно

характеризує регламентацію сфери застосування у статті 2 як значною мірою декларативну: за чинного технологічного стану держава не має дієвих інструментів ані відстежити всі операції з ВА, ані результативно відреагувати на них [121, с. 58]. Цю позицію доцільно сприймати як доктринальну проблематизацію меж правозастосування, а не як категоричне твердження про цілковиту неможливість контролю. Показовим виявом розриву де-факто/де-юре є й те, що в умовах війни державні органи відкривали криптогаманці для отримання благодійної допомоги - дії, які, як зазначають Т. Гудіма та інші [118, с. 139-140], потребують узгодження з вимогою частини 2 статті 19 Конституції України [68], за якою органи влади діють лише на підставі та в межах, передбачених законом. Саме на перетині декларативної сфери застосування і фактичної невідконтрольності обігу виникає та «сіра зона», що становить середовище підвищеного криміногенного ризику.

Подоланню цієї невизначеності має слугувати перехід до моделі, узгодженої з MiCA [2]. Інструментом такої гармонізації є консолідований законопроект № 10225-д [106], який, спираючись на функціональну типологію криптоактивів (ART, EMT та інші - пор. [42]), має замінити відкладену модель Закону № 2074-IX. Інституційну архітектуру майбутнього регулювання вибудовано навколо двох регуляторів. Як показує Р. Самсін [122, с. 70], державне регулювання ринку ВА за частиною 1 статті 16 Закону № 2074-IX охоплює комплекс заходів з упорядкування, контролю й нагляду за ринком, регулювання діяльності постачальників послуг, а також запобігання і протидію зловживанням та порушенням - формулювання, що вже на нормативному рівні пов'язує регулювання із запобіжною функцією. Ключовою є запроваджувана конструкція допуску на ринок: діяльність постачальників послуг, пов'язаних з оборотом ВА (далі - ППВА), допускається виключно за умови отримання дозволу (стаття 18), за видачу якого справляється плата (стаття 19). Р. Самсін [122, с. 70-71] обґрунтовано кваліфікує цей «дозвіл» як ліцензію за змістом, хоча законодавець уникає терміна «ліцензування»: вимоги до заявника (бездоганна ділова репутація засновників і керівників, розкриття структури власності, підтвердження джерел статутного капіталу, диференційовані пороги

капіталу - від 35 000 до 350 000 неоподатковуваних мінімумів доходів громадян (нмдг) залежно від виду послуг і резидентності) функціонально становлять ліцензійні умови. Ця кваліфікація має пряме значення для кримінально-правового аналізу: оскільки діяльність без дозволу заборонено, постає питання про криміналізацію неліцензованого надання послуг з ВА, до якого ми повернемося в наступному під-підрозділі.

Розподіл регуляторних повноважень докладно розкриває С. Грицай [123, с. 88-89]: за пунктом 1 статті 16 Закону № 2074-IX державне регулювання поділено між НБУ (оборот ЗВА(ВЦ)) та НКЦПФР (оборот решти ВА, зокрема ЗВА(ФІ) і незабезпечених). На НКЦПФР покладено формування й реалізацію державної політики розвитку ринку, адаптацію законодавства до міжнародних стандартів, ведення Державного реєстру постачальників, видачу й анулювання дозволів, нормотворчість, нагляд і застосування заходів впливу, а також повноваження суб'єкта державного фінансового моніторингу [123, с. 89-91]. Особливе значення для теми має те, що серед повноважень НКЦПФР закон передбачає направлення до правоохоронних органів матеріалів щодо фактів правопорушень, за які встановлено адміністративну та кримінальну відповідальність [123, с. 91], - це прямий нормативний місток від адміністративного нагляду до кримінально-правового реагування. Засади такого регулювання (доцільність, адекватність, ефективність, збалансованість, передбачуваність, прозорість) узгоджуються з доктринальними побудовами принципів державного регулювання обороту ВА [71] і поняттям адміністративно-правового забезпечення державної політики [63], а самі правовідносини на ринку ВА мають визначену структуру суб'єктів та об'єктів [66].

Водночас навіть запроєктована модель залишає контрольний дефіцит. В. Волинець [124, с. 30] звертає увагу, що Закон № 2074-IX не пропонує конкретних механізмів контролю за постачальниками після їх реєстрації і не регулює діяльність децентралізованих бірж, а правоохоронний зріз ілюструє типологією, наведеною за даними Державної служби фінансового моніторингу України (Держфінмоніторинг): цифрові активи використовуються для

фінансування тероризму, відмивання доходів від корупції та розкрадання бюджетних коштів, легалізації коштів, здобутих шахрайством. В. Добровольська [125, с. 59-60] кваліфікує державний контроль за обігом ВА як різновид фінансового контролю й окреслює супутні ризики - заміщення національної валюти та паралельний грошовий обіг поза наглядом НБУ, використання ВА в обхід державного регулювання. Узяті в сукупності, ці спостереження показують, що недієвість профільного режиму не лише залишає обіг ВА поза наглядом, а й безпосередньо живить криміногенний потенціал сфери.

Звідси випливає потреба реформування, найповніше систематизована В. Рядінською [126, с. 101-105], яка, відштовхуючись від MiCA [2] як орієнтира, виокремлює чотири напрями. Перший - зміна термінологічного апарату й узгодження дефініцій: на тлі того, що три національні акти визначають ВА по-різному (Закон № 2074-IX - як «нематеріальне благо», стаття 179-1 ЦК України - як «цифрову річ», Закон № 361-IX [12] - як «цифрове вираження вартості»), саме дефініція Закону № 361-IX відповідає поняттю «криптоактив» MiCA, тож пропонується перехід від терміна «віртуальні активи» до «криптоактиви» [126, с. 102]. Другий - заміна класифікації «забезпечені / незабезпечені» функціональною типологією MiCA (ART, EMT, інші криптоактиви) [126, с. 102-103]. Третій - закріплення вимог за зразком MiCA до публічної пропозиції та допуску ВА до торгівлі, до постачальників послуг, до прозорості й розкриття інформації, до авторизації та нагляду, до захисту власників і клієнтів, а також заходів проти інсайдерських зловживань і маніпулювання ринком [126, с. 103-104]. Четвертий - окреме врегулювання тих ВА, що перебувають поза сферою MiCA (зокрема NFT та криптоактивів, які кваліфікуються як фінансові інструменти) [126, с. 104-105]. Подібні напрями, зокрема переваги орієнтації на європейські стандарти, відзначає й Л. Чернов [127, с. 130]. Ці чотири напрями становлять авторську програму *de lege ferenda*, орієнтовану на гармонізацію з правом ЄС, а не виклад чинних норм.

Оцінка національного регулювання обігу ВА як такого, що перебуває на етапі початкового формування й потребує гармонізації з MiCA та подальшого

вдосконалення, є усталеною у фаховій літературі [128-134]. У межах цього доктринального консенсусу окремої уваги заслуговують дві позиції. К. Некіт [132, с. 47-49] як вагому опору напряду зміни термінології обґрунтовує перехід до поняття «криптоактиви» зі спеціальним правовим режимом для кожного виду активів, оцінюючи термін «віртуальні активи» як надто широкий для регулювання саме криптовалют і токенів. В. Грудницький [133, с. 45, 48] прямо називає кримінальне право серед галузей, що мають унормовувати обіг ВА, і, відтворюючи за Т. Гудімою та іншими [118] аргумент «сірих зон» та вимогу частини 2 статті 19 Конституції України [68], фіксує безпосередній вихід регуляторної прогалини на кримінально-правову площину. Прикладний характер має й позиція В. Нагнибіди [135, с. 48-50], який, по-перше, наголошує, що дієвість профільного закону залежатиме не лише від норми, а й від гнучкості підзаконних актів та правозастосовної практики регуляторів, а по-друге, виявляє прогалину у сфері ліцензування: перелік видів діяльності, що підлягають дозволу, не охоплює очевидно некастодіальних гаманців і P2P/DEX-сервісів на смарт-контрактах, унаслідок чого ціла категорія операцій ризикує опинитися поза дозвільним режимом. Саме ця прогалина утворює субстрат для майбутньої криміналізації неліцензованої діяльності, що розглядатиметься в підрозділі 2.4.2.

Особливої гостроти проблема нечинного регулювання набуває у вимірі воєнного стану та протидії обходу санкцій. О. Любіч та інші [136, с. 41, 49] показують подвійну природу нерегульованого ринку ВА в умовах війни: він забезпечив оперативну фінансову підтримку Збройних Сил і постраждалих через криптофонди й волонтерів, але водночас, за відсутності державного регулювання, став середовищем криміногенного ризику. Методологічно важливою є їхня теза про нейтральність технології: технологія розподіленого реєстру (DLT) сама по собі не є ані «доброю», ані «поганою» - значення мають суб'єкт і намір її використання [136, с. 43], що узгоджується з обстоюваним у цій роботі підходом, за яким предметом кримінально-правової протидії є не технологія, а суспільно небезпечне діяння [59]. Криміногенні типології, наведені авторами (використання криптоактивів структурами держави-

агресора, програми-вимагачі, спроби обходу санкцій), доцільно сприймати як ілюстрацію середовища, а не як встановлені статистичні факти [136, с. 44, 46-48].

Національний санкційно-кримінологічний зріз докладно розкриває Т. Дмитренко [137, с. 119-121], обґрунтовуючи, що відсутність чинного регулювання ринку ВА послаблює спроможність держави протидіяти обходу санкцій проти держави-агресора та фінансуванню збройної агресії. Авторка вказує на наглядову прогалину - невизначеність регулятора (за базовим Законом № 361-IX [12] відповідні функції тяжіють до сфери цифрової трансформації, тоді як профільний Закон № 2074-IX покладає їх на НКЦПФР і НБУ, які не можуть здійснювати нагляд, оскільки закон не діє) - і описує національні механізми протидії, що функціонують у режимі воєнного стану: заморожування активів із повідомленням Служби безпеки України (СБУ) та Держфінмоніторингу, діяльність оперативної групи з виявлення й арешту активів осіб, причетних до агресії, ідентифікацію криптообмінників, пов'язаних із підсанкційними суб'єктами [137, с. 118-121]. Звідси випливає кримінально-правовий вихід цього вузла. Діяння у сфері обходу санкцій і фінансування агресії з використанням ВА здатні зачіпати спектр складів КК України [64] - насамперед фінансування тероризму (стаття 258-5) та легалізацію (відмивання) майна, одержаного злочинним шляхом (стаття 209), а в умовах війни - й суміжні спеціальні склади; конкретна ж кваліфікація потребує самостійного кримінально-правового аналізу, а не запозичення оцінок з економіко-фінансових джерел, і має зважати на конституційні межі криміналізації, що впливають із вимоги діяти на підставі закону (стаття 19 Конституції України [68]). Зазначений авторкою ризик-орієнтований підхід до перевірки джерел походження ВА [137, с. 121-122] утворює місток до запобіжно-ризикового виміру, що розглядатиметься в наступному під-підрозділі.

Таким чином, нормативною основою кримінально-правової політики у сфері охорони обігу ВА в Україні нині слугує не чинний профільний закон, а сукупність загального цивільного режиму (стаття 179-1 ЦК України), антилегалізаційного законодавства (Закон № 361-IX [12]) і відкладеної моделі

Закону № 2074-IX [1], доповнена перспективою гармонізації з MiCA [2] через законопроект № 10225-д [106]. Така конфігурація має двоїстий вплив на кримінально-правову політику: з одного боку, регуляторна прогалина окреслює предмет, що потребує охорони, і навіть прямо передбачає канал передання матеріалів до правоохоронних органів; з другого - нечинність профільного режиму та технологічна непідконтрольність обігу звужують реальні можливості правозастосування. Дослідження того, як за цих умов розподіляється навантаження між кримінально-правовими засобами та ризик-орієнтованими засадами запобігання, і становить предмет наступного підрозділу.

2.5. Місце кримінально-правових засобів у механізмі охорони обігу віртуальних активів та ризик-орієнтовані засади запобігання кримінальним правопорушенням

Чинний режим первинного фінансового моніторингу за Законом України про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом [12], нечинна перспективна модель Закону України «Про віртуальні активи» № 2074-IX [1] і доопрацьований законопроект № 10225-д [106], зорієнтований на Регламент MiCA [2] утворюють статичний контур, у межах якого кримінально-правові засоби набувають свого місця. Водночас, варто також показати, як регуляторний субстрат обігу ВА переходить у площину кримінально-правової охорони і як ризик-орієнтований та запобіжний виміри вписуються у кримінально-правову політику поряд із криміналізацією, пеналізацією та правозастосуванням.

Вихідним для кримінально-правового аналізу є дозвольно-авторизаційний режим діяльності постачальників послуг, пов'язаних з оборотом ВА. За перспективною (нечинною) моделлю № 2074-IX [1] така діяльність провадиться лише за умови попереднього одержання дозволу, який видає НКЦПФР окремо на кожен із видів послуг, із вичерпними підставами для відмови та анулювання, зокрема анулювання в разі вчинення постачальником більш ніж двох правопорушень протягом календарного року [138, с. 13-15]. Системний аналіз

цих положень дає підстави стверджувати, що спеціальна (виключна) правосуб'єктність постачальника виникає не з державної реєстрації юридичної особи, а лише після одержання дозволу, тоді як провадження відповідних видів діяльності без нього перебуває поза межами легальної правосуб'єктності [139, с. 285-286]. Це міркування слід сприймати з поправкою на те, що Господарський кодекс України втратив чинність із 28 серпня 2025 року [140], унаслідок чого статус суб'єктів господарювання визначається тепер нормами Цивільного кодексу України [27] та спеціального законодавства; для сфери ВА таким спеціальним джерелом має стати профільний закон, а отже якісна відмінність діяльності «з дозволом» і «без дозволу» зберігає значення незалежно від кодифікаційної реформи.

Перспективна модель передбачає й диференційовану відповідальність постачальників: за провадження діяльності з ознаками діяльності постачальника без дозволу № 2074-IX [1] встановлював фінансові санкції, а контроль покладав на НКЦПФР [141, с. 64-65]. Принциповим для кримінально-правової політики є те, що серед повноважень регулятора прямо передбачено направлення до правоохоронних органів матеріалів щодо фактів правопорушень, за які настає адміністративна та кримінальна відповідальність [141, с. 63-64]. Саме цей припис утворює інституційний місток від адміністративно-санкційного блоку до кримінально-правової площини й окреслює нормативну базу для можливої криміналізації провадження діяльності постачальника без дозволу. Водночас зауважена в літературі ймовірність накладення кількох санкцій різними суб'єктами - НБУ та НКЦПФР - за одне діяння [141, с. 65-67] актуалізує для політики проблему розмежування адміністративної та кримінальної відповідальності й дотримання засади *ne bis in idem*.

Доопрацьований законопроект № 10225-д [106] зміщує акцент із суто дозвільної на реєстраційно-наглядову конструкцію: він зобов'язує постачальників стати на облік протягом 60 днів від початку надання послуг резидентам України та подавати щорічну звітність, передбачає штрафні санкції за порушення цих вимог і гармонізацію з правом ЄС. Така еволюція - від

реєстраційної моделі ранніх законопроектів [142, с. 63-64] через дозвоільну конструкцію № 2074-IX до змішаної архітектури № 10225-д - засвідчує, що питання про межі криміналізації неліцензованого (нереєстрованого) провадження діяльності залишається відкритим і потребує узгодження з обраним регуляторним режимом. Переконливим порівняльним орієнтиром тут є проаналізований раніше досвід Гонконгу, де провадження діяльності оператора без ліцензії прямо визнане кримінальним правопорушенням [115]; це свідчить про передбачуваність кримінально-правового захисту дозвоільного режиму як наряду політики.

Перехід від регуляторного до власне кримінально-правового механізму найповніше простежується там, де ВА розглядають одночасно як предмет, засіб і знаряддя кримінальних правопорушень. Притаманні їм анонімність, конфіденційність операцій і транснаціональність перетворюють ВА на новий інструмент учинення кримінальних правопорушень, насамперед легалізації (відмивання) доходів [143]. У процесуальній площині ВА та апаратні носії інформації про них можуть визнаватися речовими доказами (ч. 1 ст. 98 Кримінального процесуального кодексу України, далі - КПК [144]) з оглядом за правилами ст. 237 і фіксацією за статтями 104-105 КПК [143], а їх арешт із метою забезпечення конфіскації застосовується за ст. 170 КПК [144]. Оскільки віртуальний актив не є платіжним засобом і не має гривневого еквівалента, його ринкову вартість встановлюють за даними відповідних майданчиків на час операції або звернення [143].

Матеріально-правовий вимір охоплює конфіскацію як вид покарання (ст. 59 Кримінального кодексу України [64]) і спеціальну конфіскацію (статті 96-1, 96-2 КК України [64]). Можливість їх застосування до ВА обґрунтовують через ст. 177 Цивільного кодексу України [27], яка відносить до об'єктів цивільних прав і блага, що можуть існувати в цифровому середовищі [143]. Цьому протиставлено позицію, за якою з огляду на зміст нечинного № 2074-IX [1] ВА не є майном, а отже законних підстав для їх конфіскації бракує, що потребує доповнення КК України окремою нормою про конфіскацію віртуальних активів [143]. Цю доктринальну дискусію слід кваліфікувати як відкриту й таку, що має

значення *de lege ferenda*: оскільки № 2074-IX лишається невведеним у дію, кваліфікацію віртуального активу як об'єкта правовідносин нині доцільно вести через чинний Цивільний кодекс України [27], а перспективу - через № 10225-д [106]. Для кримінально-правової політики ця дилема є прямим орієнтиром, адже вона визначає, чи достатньо наявного інструментарію, чи потрібні спеціальні норми про предмет кримінально-правової охорони та про конфіскацію і управління ВА.

Узагальнюючи, дослідники наголошують на потребі поєднання адміністративно-правових і кримінально-правових механізмів охорони обігу ВА та фіксують прогалину в кримінально-правовому регулюванні незаконного обігу [145, с. 68-69]. Саме тут кримінально-правова політика стикається з вимогою пропорційності та визначеності криміналізації, що впливає з Конституції України [68], і водночас із потребою враховувати фактори ризику, на яких ґрунтується наглядова модель ФАТФ [145, с. 72]. Останнє утворює змістовий перехід до запобіжно-ризикового виміру.

Ризик-орієнтований нагляд є інструментом кримінально-правової політики остільки, оскільки він структурує середовище, у якому реалізуються запобігання і правозастосування. Його нормативним ядром слугує тріада стандартів ФАТФ - Рекомендація 1 (ризик-орієнтований підхід), Рекомендація 15 (поширення вимог на ВА та постачальників послуг) і Пояснювальна записка до неї (червень 2019 року), які вимагають регулювання, ліцензування чи реєстрації постачальників, ефективного моніторингу й нагляду та заходів, сумірних виявленим ризикам [77]. Ризик-орієнтований підхід виходить із того, що через підвищену анонімність і заплутування фінансових потоків ВА та постачальники послуг можуть мати підвищений ризик відмивання коштів і фінансування тероризму, а держави зобов'язані ідентифікувати, розуміти й оцінювати ці ризики [146, с. 96-98]. Кримінологічним тлом для криміналізації та запобігання слугує типологія ризиків - поширення криптовалют із посиленою анонімністю, міксерів і тумблерів, що приховують походження коштів через нашарування операцій [146, с. 98]. Цей орієнтир актуалізовано в оновленому керівництві ФАТФ [79], підкріплено рекомендаціями Ради з

фінансової стабільності [82] та Міжнародного валютного фонду [83], а на рівні ЄС втілено в Регламенті MiCA [2].

Запобігання кримінальним правопорушенням у сфері ВА є самостійною складовою кримінологічної політики. Його доцільно структурувати за усталеною кримінологічною моделлю трьох рівнів - загальносоціального, спеціально-кримінологічного та індивідуального - у проєкції на сферу ВА [147, с. 289-291]. На загальносоціальному рівні запобіжний потенціал пов'язується з належним державним регулюванням ринку і контролем за діяльністю його учасників, інституційно закріпленим за НКЦПФР та НБУ - перспективно за ст. 16 нечинного № 2074-IX [1], а де-факто через режим первинного фінансового моніторингу за № 361-IX [12]; спеціально-кримінологічний рівень охоплює усунення детермінант відповідних правопорушень, а індивідуальний - запобіжну роботу з конкретними особами [147, с. 290].

Ризик-орієнтований контроль має водночас чіткі межі. Він не може перетворюватися на презумпцію винуватості учасника ринку «за замовчанням»: згідно з ч. 2 ст. 77 Кодексу адміністративного судочинства України [149] тягар доказування правомірності рішень покладено на регулятора, а ч. 5 ст. 12 Цивільного кодексу України [27] закріплює презумпцію добросовісності, тож саме регулятор має спростовувати її в судовому порядку [148, с. 19]. Принципово важливою для кримінально-правової політики є теза про те, що межа добросовісної поведінки збігається з межею поведінки, яка не суперечить законодавству про кримінальну відповідальність [148, с. 19], - вона безпосередньо пов'язує запобіжний контроль із пропорційністю криміналізації (Конституція України [68]). Ілюстрацією ризику надмірної криміналізації у перспективному регулюванні є критика положення ранньої редакції законопроекту № 10225, за яким порушення вважається вчиненим умисно, якщо відповідні обставини встановить сам регулятор, - конструкція, що нагадує формулювання обвинувального акту й суперечить презумпції добросовісності [148, с. 20]. У тому ж напрямі діє застереження проти запровадження державного контролю за інформаційним контентом, який прямо стикається з правом особи на інформацію [147, с. 290].

Запобіжну архітектуру доповнює співрегулювання: делегування саморегульованим організаціям частини наглядових функцій, зокрема контролю за дотриманням законодавства учасниками ринку, розвантажує державний нагляд і відповідає принципіві «не нашкодь» на стадії становлення ринку [150, с. 100-102]; зарубіжні приклади саморегульованих організацій на ринку ВА підтверджують життєздатність такої моделі [150, с. 102]. У підсумку запобіжно-ризиковий вимір постає як перспективний - з огляду на нечинність № 2074-IX [1] - складник кримінально-правової політики, що має бути збалансований гарантіями добросовісності, права на інформацію та пропорційності криміналізації і зорієнтований на поступовий перехід до європейської моделі регулювання (Регламент MiCA [2]; законопроект № 10225-д [106]).

Висновки до розділу 2

Проведене в розділі дослідження теоретико-методологічних засад формування та реалізації кримінально-правової політики у сфері забезпечення охорони віртуальних активів дозволяє сформулювати такі висновки.

1. Стан наукової розробки проблеми є нерівномірним: понятійно-класифікаційні аспекти опрацьовані достатньо, тоді як власне кримінально-правовий і політико-правовий виміри досліджені фрагментарно, а відсутність уніфікованого визначення та єдиної класифікації віртуальних активів становить не лише доктринальну, а й методологічну перешкоду.

2. Кримінально-правову політику у сфері забезпечення охорони віртуальних активів визначено як системну діяльність уповноважених суб'єктів щодо формування і реалізації стратегії кримінально-правової охорони відносин, що виникають у зв'язку зі створенням, обігом та використанням таких активів. Її основними ознаками є подвійна родова належність, похідний характер щодо регулятивного законодавства з переважно бланкетною природою заборон, міжнародна і європейська зумовленість, технологічна складність об'єкта та динамічність.

3. Структуру політики розкрито через її об'єкт, суб'єктів, принципи та засоби реалізації. Об'єктом є суспільні відносини правомірного створення, обігу й використання віртуальних активів та охорони майнових прав учасників ринку; суб'єктом формування - Верховна Рада України (стаття 92 Конституції України), а суб'єктами реалізації - органи досудового розслідування, прокуратура, суд та органи виявлення, розшуку й управління активами. За методом ця політика є субсидіарною щодо регулятивних механізмів.

4. Власну систему принципів досліджуваної політики утворюють законність криміналізації, юридична визначеність (що набуває особливої ваги з огляду на бланкетність заборон і незавершеність регулятивного законодавства), пропорційність і гуманність та невідворотність відповідальності. Неповнота або суперечливість регулятивного законодавства безпосередньо знижує якість кримінально-правової охорони.

5. Обґрунтовано положення, що на відміну від традиційних сфер охорони, де визначальними є внутрішні соціально-економічні чинники, у сфері віртуальних активів первинним джерелом політики виступає зовнішній наднаціональний нормативний і досвідний масив, що зумовлено транскордонною природою активів. Європейська модель і міжнародні стандарти задають зміст бланкетних заборон, межі допустимої криміналізації та орієнтири гармонізації національної відповідальності.

6. Система міжнародних стандартів є багаторівневою: її ядро утворюють Рекомендації ФАТФ (насамперед Рекомендації 15 і 16 з «правилом подорожей»), макрофінансовий контур - рекомендації Ради з фінансової стабільності та елементи політики Міжнародного валютного фонду, а регіональну гармонізацію забезпечує право Європейського Союзу на чолі з Регламентом (ЄС) 2023/1114 (MiCA). Самостійне кримінально-правове значення має проблема регуляторного арбітражу, оскільки прогалина в охороні в одній державі послаблює захищеність відповідних відносин в усіх інших.

7. Право Європейського Союзу задає регуляторний каркас охорони і вирізняє три магістральні напрями криміналізації - протидію відмиванню коштів, протидію ринковим зловживанням (MAR і CSMAD у поєднанні з

розділом VI MiCA) та протидію неліцензованій діяльності постачальників послуг. Порівняльний аналіз держав ЄС і держав поза ЄС засвідчив, що антивідмивний режим усюди є базовою конструкцією, а кримінально-правові засоби доцільно застосовувати як крайні (*ultima ratio*); орієнтирами для запозичення є технологічно нейтральні дефініції, гонконгівська криміналізація неліцензованої діяльності операторів платформ, спеціалізовані інституції протидії та практика конфіскації активів.

8. Актуалізованим станом національного регулювання є саме нечинність профільного Закону № 2074-IX, прийнятого, але не введенного в дію: де-юре статус віртуального активу визначається функціональною дефініцією Закону № 361-IX і статтею 179-1 ЦК України, а орієнтиром реформування виступає Регламент MiCA через консолідований законопроект № 10225-д. Розрив між де-юре і де-факто породжує «сірі зони», несумісні з юридичною визначеністю; напрямами реформування *de lege ferenda* є узгодження термінології, заміна класифікації функціональною типологією MiCA, закріплення вимог за її зразком та окреме врегулювання активів поза сферою Регламенту.

9. Місце кримінально-правових засобів визначається їх субсидіарністю щодо регулятивних механізмів: дозвольно-авторизаційний режим діяльності постачальників послуг утворює нормативний субстрат для можливої криміналізації її провадження без дозволу, а віртуальні активи здатні виступати водночас предметом, засобом і знаряддям правопорушень, причому питання їх конфіскації потребує спеціальних норм. Запобіжно-ризиковий вимір - ризик-орієнтований нагляд за стандартами ФАТФ і трирівнева модель запобігання - є перспективним складником політики, збалансованим гарантіями добросовісності, права на інформацію та пропорційності криміналізації.

РОЗДІЛ 3.

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ, ЩО ВЧИНЯЮТЬСЯ ЩОДО ВІРТУАЛЬНИХ АКТИВІВ АБО З ЇХ ВИКОРИСТАННЯМ

3.1. Віртуальні активи в системі об'єктів та предметів кримінальних правопорушень

Стрімке поширення віртуальних активів у цивільному та господарському обороті закономірно зумовило їх залучення до сфери суспільно небезпечних діянь, що, своєю чергою, поставило перед наукою кримінального права питання про місце віртуальних активів у структурі складу кримінального правопорушення. Це питання не є суто термінологічним: від того, яку саме функцію виконує віртуальний актив у механізмі вчинення посягання, залежить кримінально-правова кваліфікація діяння, розмежування суміжних складів та визначення обсягу заподіяної шкоди. У наукових дослідженнях слушно наголошується, що віртуальні активи можуть виступати водночас фінансовим засобом, платіжним інструментом, а подеколи й безпосереднім предметом вчинення правопорушень [151, с. 368], і саме ця багатфункціональність вимагає попереднього розмежування ролей, які віртуальний актив здатний відігравати в складі кримінального правопорушення.

Першим і найбільш дискусійним є питання про те, чи може віртуальний актив визнаватися майном і предметом злочину, чи він є лише засобом його вчинення. У літературі це формулюється як ключова дихотомія, від вирішення якої залежить як кваліфікація, так і доказування у відповідних провадженнях [151, с. 194]. Залежно від фактичних обставин віртуальний актив здатний виступати: предметом кримінального правопорушення, насамперед проти власності; засобом або знаряддям його вчинення; предметом незаконного збагачення та об'єктом фінансового моніторингу. Таке розрізнення має не лише теоретичне, а й цілком практичне значення, оскільки помилкове ототожнення

предмета посягання із засобом його вчинення спотворює юридичну оцінку діяння.

Центральне місце серед перелічених ролей посідає визнання віртуального активу предметом кримінальних правопорушень проти власності. У теорії кримінального права предмет таких посягань традиційно характеризується трьома обов'язковими ознаками - фізичною (матеріальною), економічною та юридичною [152, с. 138]. Дослідники, які зверталися до цього питання ще на етапі ухвалення профільного законодавства, відзначали, що майно як предмет правопорушень, пов'язаних із викраденням, характеризується фізичною ознакою, юридичною ознакою (предмет є чужим для винної особи, тобто має власника чи законного володільця, якому заподіюється шкода) та економічною (соціальною) ознакою, що передбачає наявність у майна певної економічної цінності [153, с. 228]. Перевірка притаманності цих ознак віртуальним активам становить вихідний пункт для визнання їх предметом посягань на власність.

Традиційний підхід пов'язує фізичну ознаку предмета злочинів проти власності зі здатністю об'єкта матеріального світу до фізичного сприйняття. Водночас у сучасній доктрині обґрунтовано відхід від ототожнення предмета виключно з матеріальним об'єктом: посягання може стосуватися і так званих безтілесних речей, що мають специфічну природу та набувають реальності лише через матеріалізовану форму свого прояву, до яких теоретично можна віднести й віртуальні активи [152, с. 138]. Стосовно віртуальних активів фізична ознака проявляється в можливості їх вимірювання в певних одиницях, участі в обігу на електронних біржах та здатності до вилучення. Економічна ознака також є їм притаманною, оскільки для віртуальних активів встановлюється курс щодо офіційних фіатних валют, а самі вони здатні виконувати функцію засобу розрахунку за товари та послуги; з огляду на це вони наділені як міноюю, так і споживчою вартістю [152, с. 139]. Юридична ж ознака полягає в тому, що віртуальний актив є чужим для особи, яка вчиняє посягання, тобто має власника або законного володільця, якому протиправними діями заподіюється шкода [152, с. 139; 153, с. 228].

Саме юридична ознака предмета - належність віртуального активу певній особі на праві власності - потребує звернення до його цивільно-правової природи. Можливість визнання віртуального активу майном забезпечується чинним цивільним законодавством: Законом України «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав» [28] Цивільний кодекс України було доповнено статтею 179-1, згідно з якою цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність, причому до цифрових речей віднесено й віртуальні активи [27]. Оскільки цифрова річ є об'єктом цивільних прав (частина перша статті 177 Цивільного кодексу України), а окрема річ визнається майном (частина перша статті 190 цього Кодексу), віртуальний актив за чинним регулюванням кваліфікується як цифрова річ і, відповідно, як майно [154, с. 108-109]. Розміщення статті 179-1 у главі 13 «Речі. Майно» Цивільного кодексу України дає підстави стверджувати, що законодавець мав на меті віднести віртуальні активи до категорії майна, а отже, і до охоронюваних законом про кримінальну відповідальність благ [152, с. 139].

Водночас правова природа віртуальних активів не є однорідною, що безпосередньо впливає на встановлення предмета посягання. Незабезпечені віртуальні активи кваліфікуються у складі майна як цифрові речі, тоді як забезпечені віртуальні активи мають подвійну природу, будучи одночасно цифровою річчю та сукупністю майнових прав на об'єкт забезпечення [154, с. 110-111]. Це означає, що при кваліфікації посягання необхідно враховувати, на який саме різновид віртуального активу спрямоване діяння, оскільки від цього залежить характеристика предмета та обсяг прав, яких позбавляється потерпілий.

Цивільно-правовий аналіз дає змогу уточнити й момент, у який віртуальний актив набуває власника, а отже, стає «чужим» для винного. У доктрині обґрунтовано, що віртуальні активи за своєю юридичною природою є майном і різновидом цифрової речі, об'єктом цивільних прав, на який поширюються правомочності володіння, користування та розпорядження, а ключову роль у визначенні належності активу відіграє контроль над приватним

ключем [155, с. 171-174]. Передання віртуального активу через блокчейн-транзакцію за своєю природою нагадує передачу володіння рухомими речами, а право власності переходить у момент, коли актив унаслідок підтвердженої транзакції прив'язується до публічної адреси набувача і стає доступним для користування та розпорядження за допомогою приватного ключа [156, с. 60-61]. Ця технологічна особливість має пряме кримінально-правове значення: оскільки фактичне панування над віртуальним активом забезпечується контролем над приватним ключем, а транзакції є незворотними, ускладнюється встановлення особи власника та моменту, у який актив вибуває з його володіння, що позначається на доказуванні у відповідних провадженнях.

Поряд із визнанням віртуального активу майном слід враховувати варіативність його правового режиму, яка зумовлює відмінності у кваліфікації. Порівняльно-правовий аналіз засвідчує, що в різних правопорядках віртуальні активи (криптовалюти) кваліфікуються неоднаково - як форма грошей, законний чи основний засіб платежу, товар, нематеріальне благо або фінансовий інструмент [157, с. 166-168]. Така багатоманітність підходів означає, що кримінально-правова оцінка діяння з віртуальним активом залежить від того, який саме правовий режим визнається за відповідним активом у національному праві: визнання його майном відкриває шлях до кваліфікації посягань як злочинів проти власності, тоді як трактування його як фінансового інструменту чи засобу платежу зміщує акценти до інших груп складів. Для України орієнтиром гармонізації у цій сфері залишається Регламент (ЄС) 2023/1114 про ринки криптоактивів (MiCA) [2], а легальне визначення віртуального активу де-юре наразі ґрунтується на Законі України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [12], який відтворює формулювання, запропоноване у Рекомендаціях Групи з розробки фінансових заходів боротьби з відмиванням грошей.

Розмежування ролей віртуального активу у складі правопорушення вимагає також відмежування посягань, предметом яких є сам актив, від діянь,

що стосуються порушення встановленого порядку обігу або генерування віртуальних активів. Відповідальність за порушення вимог щодо обігу віртуальних активів, передбачена профільним законодавством, має переважно фінансово-правовий характер: за модель, закладену в Законі України «Про віртуальні активи», державне регулювання покладається на Національний банк України (щодо віртуальних активів, забезпечених валютними цінностями) та Національну комісію з цінних паперів та фондового ринку (щодо інших віртуальних активів), а до постачальників послуг, які провадять діяльність без відповідного дозволу, застосовуються фінансові санкції; кримінально-правова ж реакція реалізується опосередковано - через направлення регулятором матеріалів до правоохоронних органів щодо діянь, за які передбачена адміністративна та кримінальна відповідальність [141, с. 63-65]. Оскільки відповідні норми містяться в Законі, що не набрав чинності, наведений режим відповідальності також має розглядатися як перспективний.

Самостійного значення набуває питання про способи набуття віртуальних активів, оскільки воно пояснює, яким чином актив потрапляє в оборот і стає можливим предметом посягання. У наукових дослідженнях виокремлюють три основні шляхи набуття криптовалют: майнінг (видобуток), купівля-продаж та бартер [158, с. 90]. При цьому майнінг розглядається як вид діяльності, що за своїми ознаками - самостійністю, ризиковим характером, систематичністю та спрямованістю на отримання прибутку - наближається до підприємницької, однак залишається без належного законодавчого врегулювання, перебуваючи у своєрідному «юридичному вакуумі» [160, с. 67-68]. Це питання, як і питання регуляторної кваліфікації майнінгу, профільно належить до сфери господарсько-правового та фінансово-правового регулювання; для цілей кримінально-правового дослідження істотним є те, що генерування та обіг віртуальних активів самі по собі утворюють окрему площину правового впливу, відмінну від охорони власності.

Ця відмінність увиразнюється на прикладі суміжних складів. Так, протиправне зниження витрат на електроенергію під час майнінгу шляхом самовільного використання електричної енергії кваліфікується за статтею 188-1

Кримінального кодексу України, а умисне пошкодження об'єктів електроенергетики - за статтею 194-1 цього Кодексу [64; 151, с. 371], тобто посягання спрямоване не на віртуальний актив, а на інші охоронювані блага. Водночас легалізація операцій із віртуальними активами та їх оподаткування створюють підстави для застосування до правопорушників норм про ухилення від сплати податків (стаття 212 Кримінального кодексу України) [160, с. 70]. Наведені приклади підтверджують, що зіткнення кримінального права з віртуальними активами не завжди означає посягання на власність: віртуальний актив може бути як предметом такого посягання, так і елементом діяльності, що оцінюється за іншими складами.

Нарешті, віртуальний актив виступає об'єктом фінансового моніторингу та може бути пов'язаний із незаконним збагаченням, що доповнює систему його ролей у структурі складу. В Україні сформовано багаторівневу систему протидії незаконному обігу віртуальних активів, у якій координацію аналітичної роботи та виявлення ризикових транзакцій забезпечує Державна служба фінансового моніторингу, а контроль за декларуванням віртуальних активів публічними службовцями здійснює Національне агентство з питань запобігання корупції, причому приховування таких активів або заниження їх вартості може свідчити про ознаки незаконного збагачення [151, с. 371-372]. Особливу увагу привертає те, що окремі учасники процесу видобутку - майнери або валідатори - за певних умов, зокрема за наявності контролю над транзакціями у мережі, можуть підпадати під визначення постачальників послуг, пов'язаних з оборотом віртуальних активів, а щойно згенеровані віртуальні активи здатні слугувати каналом легалізації доходів [159, с. 90, 92]. Ці аспекти, профільні для дослідження легалізації майна та фінансового моніторингу, тут окреслюються лише в обсязі, необхідному для повноти уявлення про роль віртуального активу у складі кримінального правопорушення.

Окремою та практично значущою проблемою, що супроводжує визнання віртуального активу предметом посягання, є проблема його визначення та доказування. Чинне кримінальне та кримінальне процесуальне законодавство

не містить норм, які б прямо згадували віртуальні активи: у Кримінальному кодексі України [64] відсутня пряма відповідальність за незаконне заволодіння криптовалютою, а норми Кримінального процесуального кодексу України [144] не пристосовані до розслідування у цій сфері і не передбачають належного порядку вилучення, зберігання та конфіскації віртуальних активів, передбачаючи лише можливість накладення арешту на них [151, с. 197]. Внаслідок цього слідчі та прокурори діють фактично на власний розсуд, а доказування ускладнюється потребою встановлення власника віртуального активу, верифікації цифрових слідів у блокчейні та фіксації відповідних доказів [151, с. 194]. Додаткові труднощі створює висока волатильність віртуальних активів: розмір заподіяної шкоди на момент вчинення посягання та на момент постановлення вироку може суттєво відрізнятись, що безпосередньо впливає на кримінально-правову кваліфікацію і потребує розроблення національної методології оцінки вартості віртуальних активів [152, с. 140]. Зазначені труднощі доказування значною мірою зумовлені вже згаданими технологічними особливостями - незворотністю транзакцій та визначальною роллю контролю над приватним ключем, - які ускладнюють встановлення як належності активу, так і моменту посягання [155, с. 173-174; 156, с. 62].

Підсумовуючи, віртуальні активи посідають у системі об'єктів та предметів кримінальних правопорушень неоднозначне місце, зумовлене їх особливою правовою та технологічною природою. За чинним цивільним законодавством вони визнаються майном і різновидом цифрової речі, що дає змогу розглядати їх як предмет кримінальних правопорушень проти власності, оскільки їм притаманні всі необхідні ознаки такого предмета - фізична, економічна та юридична. Водночас віртуальний актив здатний виступати знаряддям чи засобом вчинення правопорушення, предметом незаконного збагачення та об'єктом фінансового моніторингу, а діяльність з його обігу та генерування утворює самостійну площину правового регулювання, відмінну від охорони власності. Реалізація кримінально-правової охорони віртуальних активів натрапляє на низку перешкод, пов'язаних із відсутністю прямих норм у Кримінальному та Кримінальному процесуальному кодексах, складністю

визначення вартості активу та встановлення його власника, а також із тим, що профільний Закон України «Про віртуальні активи» досі не набрав чинності. Усунення цих перешкод потребує як удосконалення матеріального і процесуального законодавства, так і гармонізації національного регулювання з європейською моделлю, що має створити належні умови для кваліфікації посягань, предметом яких є віртуальні активи.

3.2. Загальна характеристика та типологія кримінальних правопорушень у сфері віртуальних активів

Поширення віртуальних активів як нового об'єкта майнового обороту супроводжується формуванням специфічного сегмента злочинності, у якому ВА виступають водночас фактором, що полегшує вчинення посягань, їх предметом, засобом або знаряддям. Загальна характеристика та типологія цих правопорушень мають передувати аналізу окремих складів, оскільки саме систематизація дає змогу впорядкувати емпіричний матеріал, узгодити кримінологічні спостереження з кримінально-правовою кваліфікацією та забезпечити єдність судової практики. З огляду на наскрізне розуміння ВА, прийняте в Розділі 1, термін «криптовалюта», яким оперує більшість використаних джерел, надалі вживається як позначення найпоширенішого різновиду ВА, а не як їх синонім.

Кримінологічна характеристика злочинності у сфері ВА має враховувати співвідношення між абсолютними обсягами та відносною часткою незаконного використання. За оцінкою Європолу, попри прискорене залучення криптовалют до злочинних схем, їх частка у злочинній економіці залишається обмеженою порівняно з готівкою, а висока волатильність стримує довгострокове «інвестування» злочинних коштів [161, с. 2]. Водночас складність такого використання зростає: криптовалюти застосовують не лише для обфускації фінансових потоків (відмивання), а й як засіб платежу та як «валюту» інвестиційного шахрайства, тоді як випадки фінансування тероризму залишаються порівняно нечисленними [161, с. 2]. Принципово важливою для побудови типології є теза про те, що злочинне використання криптовалют

більше не обмежується кіберзлочинністю, а охоплює всі види злочинів, що потребують передавання вартості [161, с. 2, 4]. Показовою є й розбіжність кількісних оцінок: якщо за оцінкою приватного сектору частка незаконних транзакцій становила близько 0,34 % загального обсягу (2020 р.), то за окремими академічними підрахунками - приблизно 23 %, причому розбіжність пояснюється методологією, тоді як щодо самої тенденції - зменшення відносної частки за зростання абсолютного обсягу - спостерігається згода [161, с. 4-5]. У функціональному вимірі найчастіше виявлюваним предикатним напрямом є шахрайство, на яке, за наведеними Європолем даними, припадало понад половину виявлених злочинних транзакцій [161, с. 5, 13].

Систематизація злочинного використання ВА є усталеним напрямом і в зарубіжній доктрині. За результатами Arnone G., Scirè G., Bivona E. систематичного огляду літератури, що охопив 127 релевантних публікацій 2020-2024 рр., виокремлено сім тематичних кластерів зловживання криптовалютами: фінансування тероризму; відмивання коштів; даркнет-ринки; кіберзлочинність; наркотрафік; торгівля людьми; корупція [162, с. 827-833]. Привабливість ВА для організованої злочинності пов'язується з їх децентралізацією, псевдонімністю та глобальним охопленням, що в сукупності з юрисдикційною фрагментацією породжує стійкі регуляторні виклики [162, с. 820, 835-837]. Ця модель доповнює функціональну типологію Європолу під кутом видів злочинної діяльності й водночас засвідчує, що впорядкування форм криптозлочинності є самостійним завданням, актуальним для багатьох правопорядків.

На вітчизняному матеріалі кримінологічну характеристику цього сегмента злочинності здійснили Д. В. Казначєєва та А. О. Дорош, які звертають увагу на те, що Україна належить до лідерів за рівнем застосування ВА населенням, проте відповідний ринок розвивається переважно в «сірій зоні», що становить загрозу для держави, бізнесу й користувачів [163, с. 149-150]. До криміногенних властивостей криптовалюти як фактора злочинності автори відносять анонімність, швидкість і незворотність переказів, заплутаність ланцюжків транзакцій, глобальну доступність та відсутність єдиного керівного

органу [163, с. 151]. Основними ознаками протиправних посягань у цій сфері визнано електронну (цифрову) природу, за якої криптовалюта є предметом або засобом, вчинення через віртуальні мережі та майновий чи особистий мотив [163, с. 152-153]. Саме на цьому ґрунті формується ключова для систематизації дуалістична рамка - поділ за роллю ВА на «засіб (спосіб) вчинення» та «предмет посягання» [163, с. 153-157]. Водночас слід урахувати, що теза праць 2020-2021 рр. про цілковиту відсутність правового статусу ВА відображала стан, який відтоді змінився: чинний Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» оперує поняттям ВА для цілей фінансового моніторингу [12]; Цивільний кодекс України доповнено категорією цифрової речі (ст. 179-1) Законом № 3320-IX [28]; а спеціальний Закон України «Про віртуальні активи» хоч і прийнято, проте він не набрав чинності [1]. Тому положення про «відсутність статусу» доцільно сприймати в історичному контексті, а не як актуальну характеристику.

Розгорнуту систематизацію за роллю ВА запропонував В. В. Саєнко, який виходить із того, що поняття «злочинна діяльність» є ширшим за «злочин», а модель злочинної діяльності окремого виду слугує підставою для подальшого розмежування та кваліфікації [164, с. 409-410]. На першому рівні автор поділяє таку діяльність на ту, у якій ВА є засобом вчинення правопорушень, і ту, у якій ВА є об'єктом замаху (предметом посягання) [164, с. 411]. Деталізуючи групу, де ВА виступають засобом, дослідник пов'язує конкретні види злочинної діяльності з відповідними статтями Кримінального кодексу України [64]: легалізацію (відмивання) майна (ст. 209), ухилення від сплати податків (ст. 212), одержання неправомірної вигоди (ст. 368, 369, зокрема з використанням невзаємозамінних токенів), шахрайство та шахрайство з фінансовими ресурсами (ст. 190, 222), фінансування тероризму (ст. 258-5), створення й обіг шкідливих програмних чи технічних засобів (ст. 361-1), незаконний обіг наркотичних засобів (ст. 307), виготовлення та обіг матеріалів, що містять зображення сексуального насильства над дітьми (ст. 301-1), посягання на

свободу й особисту недоторканність особи (ст. 146, 149, 303), незаконний обіг зброї (ст. 263) та незаконні дії з документами на переказ і платіжними засобами (ст. 200) [164, с. 411-418]. Цей перелік має значення своєрідної «навігаційної карти» для подальшого аналізу окремих складів, оскільки впорядковує види злочинної діяльності за об'єктом кримінально-правової охорони. Слід зважати, що праця В. В. Саєнка має криміналістичне спрямування, тому в межах цього підрозділу запозичується саме типологічний шар, а не методика розслідування.

Сучасний емпіричний зріз дають аналітичні звіти 2025-2026 рр. За оцінкою TRM Labs, обсяг незаконних криптопотоків у 2025 р. сягнув приблизно 158 млрд дол. США, зрісши майже на 145 % порівняно з попереднім роком, що є найвищим показником за останні п'ять років [165, с. 1-3, 7]. Водночас відносна частка незаконної активності у загальному обсязі знизилася приблизно до 1,2 % [165, с. 2, 4], - кримінологічний нюанс «зростання абсолюту за зменшення частки» узгоджується з висновком Європолу. Цей звіт прямо застерігає про оцінний характер показників та зміну методики, через яку наведені ряди не можна напряду зіставляти з попередніми, а саму оцінку слід сприймати як консервативну «нижню межу» [165, с. 4, 11-12]. За категоріями злочинного використання виокремлено обхід санкцій, зломи й експлойти сервісів, шахрайство, програми-вимагачі, незаконний обіг наркотиків, відмивання коштів та фінансування тероризму [165, с. 5-59], причому 2025 р. позначений зсувом до «інституціоналізації» криптоінфраструктури державно-афілійованими акторами. Ця категорійна типологія накладається на структуру статей КК України [64], що визначає предмет подальшого аналізу.

Шахрайський кластер, на який припадає значна частка виявлених посягань, потребує окремої деталізації. За результатами оглядового дослідження та експертної консенсус-сесії інвентаризовано до 47 унікальних видів криптошахрайства, з-поміж яких найчастіше обговорюваними є фінансові піраміди та високодохідні інвестиційні програми, шахрайство під час первинного розміщення монет (ICO), фішинг і маніпулювання ринком за схемою «pump-and-dump» [166, с. 5-9]. Принципове методологічне значення має застосована друга, незалежна вісь класифікації - поділ на кіберуможливлені

(cyber-enabled) та суто кіберзалежні (cyber-dependent) посягання: більшість видів криптошахрайства лише відтворюють у цифровому середовищі давно відомі механізми (піраміди, маніпулювання ринком), тоді як суто кіберзалежними є переважно прихований майнінг та зловживання гаманцевими й біржовими сервісами [166, с. 12]. Цю вісь доцільно застосовувати паралельно з поділом за роллю ВА, отримуючи два незалежні критерії систематизації. Водночас наголошується, що кількість описаних у літературі видів не дорівнює їх реальній поширеності, а наскрізною проблемою є брак узгоджених дефініцій [166, с. 12-13], - спостереження, що прямо обґрунтовує потребу систематизації для цілей кваліфікації.

Найповніше поєднання доктринального й емпіричного підходів на вітчизняному ґрунті пропонує М. В. Карчевський. Дослідник розкриває структуру відносин у сфері обігу ВА, виокремлюючи трьох учасників транзакції - відправника (власника активу), одержувача та «майнерів» (валідаторів), які забезпечують перевірку й підтвердження транзакцій [167, с. 54-55], і характеризує відповідні правопорушення за трьома ознаками: технологічною (розподілений реєстр і послідовність ініціювання, перевірки та формування блоків), економічною (ринкове, позбавлене єдиного регулятора, ціноутворення) та юридичною, причому щодо останньої автор слушно зазначає незавершеність національного регулювання й те, що Закон України «Про віртуальні активи» не набрав чинності [1; 167, с. 56-57]. Особливу цінність для кримінологічної характеристики має проведений автором моніторинг Єдиного державного реєстру судових рішень (далі - ЄДРСР): якщо станом на 2021-2023 рр. ішлося про кілька десятків обвинувальних вироків, у яких переважали справи щодо незаконного обігу наркотичних засобів та «комп'ютерні» злочини, то станом на серпень 2025 р. автор обліковує близько 214 судових рішень із відчутним переважанням посягань на власність, незаконного обігу наркотиків та правопорушень у сфері використання інформаційних технологій (ст. 361-362 КК України [64]) [167, с. 60-61]. З огляду на оцінний характер та авторську методику підрахунку, ці показники потребують самостійної звірки, проте навіть у такому вигляді вони наочно ілюструють динамічну зміну структури

криптозлочинності в Україні. Автор також розмежовує централізовані (CEX) та децентралізовані (DEX) криптобіржі: перші мають керівно-контрольну структуру й забезпечують процедури ідентифікації клієнта (KYC) та фінансового моніторингу, тоді як другі суттєво ускладнюють нагляд [167, с. 62-63], - і пов'язує перспективи протидії з орієнтацією на Регламент Європейського Союзу про ринки криптоактивів (MiCA) [2]. Узагальнюючи, дослідник констатує «неспівмірність» традиційних інститутів злочинів проти власності з новітніми технологіями та фрагментарність регулювання, що обмежує можливості кваліфікації та розслідування [167, с. 61, 65-66].

Прикладний зріз доповнює оглядове видання поліції Великої Британії, яке систематизує сучасні форми криптозлочинності з позицій профілактики. З-поміж них - інвестиційне шахрайство та схеми Понці, маніпулювання ринком і «rump-and-dump», раптове залишення проєкту з привласненням залучених коштів («rug pull»), романтичне та «соціально-інженерне» інвестиційне шахрайство («pig butchering»), видавання себе за іншу особу, шахрайство під час ICO, фейкові гаманцеві застосунки, крадіжка цифрових активів, прихований майнінг, фішинг (зокрема смішинг і квішинг), використання шкідливого програмного забезпечення (у тому числі програм-вимагачів), залучення «грошових мулів», відмивання через крипто-банкомати, а також низка посягань, пов'язаних з невзаємозамінними токенами (NFT) [168, с. 20-50]. Хоча це джерело має просвітницький, а не доктринальний характер і спирається на британські інституції, воно корисне як упорядкований опис способів вчинення (*modus operandi*), що ілюструє вісь «види злочинної діяльності». Окремо варто відзначити роль ВА як засобу відмивання: на підвищених ризиках, що їх створюють децентралізовані сервіси для протидії відмиванню коштів, наголошується й у фаховій літературі [57], а відповідний напрям детально розглянуто в підрозділі 3.3.1.

Зіставлення наведених джерел дає змогу запропонувати багатовимірну систематизацію кримінальних правопорушень у сфері ВА. За роллю ВА у складі правопорушення доцільно розрізняти посягання, у яких ВА є предметом (передусім злочини проти власності, корупційні та господарські), засобом чи

способом вчинення (відмивання, фінансування тероризму, ухилення від сплати податків, придбання заборонених товарів і послуг) та об'єктом протиправного впливу (несанкціоноване втручання в роботу інформаційних систем криптобірж і гаманців із заволодінням активами); цей поділ узгоджується з дуалістичною рамкою «засіб/предмет» [163; 164] та функціональними типологіями [161; 162; 165]. Паралельно застосовним є поділ за технологічним критерієм на кіберуможливлені та кіберзалежні посягання [166], а також за об'єктом кримінально-правової охорони - із прив'язкою до відповідних статей КК України [64], що й визначає структуру подальшого викладу. Потребу такої систематизації обґрунтовують щонайменше три обставини: методологічна нестабільність і розбіжність кількісних оцінок, що унеможлиблює покладання на «сирі» статистичні показники [161; 165; 166]; брак узгоджених дефініцій форм криптозлочинності [166]; а також констатована «неспівмірність» традиційних кримінально-правових інститутів з технологічними реаліями [167]. Упорядкування видів злочинної діяльності за наведеними критеріями є передумовою правильної кваліфікації та єдності судової практики, що зумовлює перехід до характеристики окремих складів кримінальних правопорушень у наступних підрозділах.

3.3. Типові кримінальні правопорушення, що пов'язані з віртуальними активами

3.3.1. Легалізація (відмивання) майна, одержаного злочинним шляхом, із використанням віртуальних активів

Стан наукової розробки проблеми кримінально-правової протидії легалізації (відмиванню) майна, одержаного злочинним шляхом, із використанням віртуальних активів характеризується виразною диспропорцією між суспільною значущістю питання та обсягом його доктринального опрацювання. Як засвідчує наукометричний зріз, здійснений А. С. Політовою, у масиві дисертаційних тем юридичного профілю частка робіт, присвячених ст. 209 КК України, упродовж 2020-2024 рр. коливалася в межах від 0,20 % до 0,5 % річного обсягу, причому серед них лише поодинокі торкалися

віртуальних активів, а за предметом «протидія легалізації за допомогою віртуальних активів» не було захищено жодної кваліфікаційної роботи [169, с. 124, 127-128]. Попри це у відповідному сегменті сформувалося коло дослідників, праці яких утворюють фактичну основу подальшого аналізу [169, с. 125]. Прикметно, що відправною точкою більшості розвідок слугує констатація неузгодженості легальної термінології - між нечинним Законом України «Про віртуальні активи» № 2074-IX [1] і чинним Законом № 361-IX, що відносить криптовалюту до віртуальних активів [12]. Ця неузгодженість, як буде показано далі, безпосередньо проєктується на визначення предмета злочину й залишається наскрізним нервом усієї проблематики.

Кримінально-правову заборону легалізації закріплено у ст. 209 КК України [64], диспозиція якої охоплює набуття, володіння, використання та розпорядження майном, щодо якого фактичні обставини свідчать про його одержання злочинним шляхом, а також вчинення з таким майном фінансових операцій і правочинів, його переміщення, зміну форми (перетворення) та дії, спрямовані на приховування чи маскування його походження, за умови усвідомлення винним злочинного характеру походження майна. Офіційна статистика правозастосування демонструє висхідну динаміку: за даними Офісу Генерального прокурора, до судів скеровано обвинувальних актів за ст. 209 КК у 2022 р. - 189, у 2023 р. - 460, а у 2024 р. - 496 [170, с. 773]. Дослідження експліцитних ознак складу, тобто ознак, доступних спостереженню, вимірюванню та реєстрації, проведене Є. Ю. Самойловим, виводить на перший план питання предмета як факультативної, але вирішальної для кваліфікації ознаки: предметом легалізації за ст. 209 КК визнаються кошти або інше майно, одержане внаслідок предикатного діяння [170, с. 776-777].

Саме навколо предмета зосереджено центральну доктринальну суперечку підрозділу. Бланкетний характер диспозиції ч. 1 ст. 209 КК зумовлює залежність кваліфікації від регулятивного, передусім цивільного, законодавства [170, с. 779]. Унаслідок доповнення Цивільного кодексу України статтею 179-1 «Поняття цифрової речі», запровадженою Законом № 3320-IX (чинним з 3 вересня 2023 р.) [28], за якою віртуальні активи визнаються різновидом

цифрових речей із поширенням на них положень про речі, у системному зв'язку зі ст. 190 ЦК України [27] Є. Ю. Самойлов обґрунтовує висновок про розширення предмета ст. 209 КК: саме з 3 вересня 2023 р. цей предмет охопив і віртуальні активи, тоді як акти крипто-легалізації, вчинені до зазначеної дати, не можуть кваліфікуватися за ст. 209 КК через відсутність такої експліцитної ознаки, як предмет [170, с. 778-779]. Натомість Д. В. Каменський та О. О. Дудоров обстоюють протилежну позицію: легальні дефініції віртуального активу, на їхню думку, засвідчують його немайновий характер як різновиду цифрової речі, відмінної від «звичайної» речі, звідки автори виводять невизнання криптовалюти майном - а отже, і предметом - чинної редакції ст. 209 КК [171, с. 507]. Попри протилежність висновків, обидва підходи зближує визнання того, що остаточне зняття невизначеності пов'язане з удосконаленням понятійного апарату, зокрема у проєкті нового КК України, де поняття «активи (доходи)» прямо охоплює нематеріальні активи з криптовалютами включно [170, с. 774-775; 171, с. 507]. Водночас слід наголосити, що апеляція до Закону № 2074-IX у цьому контексті здатна мати лише перспективне значення, позаяк цей акт не введено в дію [1]; де-lege-lata статус віртуального активу як можливого предмета злочину має виводитися виключно через чинні приписи - Закон № 361-IX [12] та ст. 179-1 ЦК України [27].

Суб'єктивна сторона легалізації характеризується умисною формою вини: винний усвідомлює або, за обставинами, повинен усвідомлювати, що майно одержане злочинним шляхом [64; 170, с. 774]. Саме доказування цього інтелектуального моменту становить одну з найскладніших практичних проблем у провадженнях щодо віртуальних активів, оскільки анонімізаційний потенціал останніх ускладнює встановлення суб'єктивного ставлення особи до походження майна. Ця обставина закономірно зміщує практичний акцент із редакційного вдосконалення диспозиції на розбудову інструментів виявлення, фіксації та простеження операцій.

Типологія відмивання з використанням віртуальних активів демонструє якісну відмінність від «класичних» схем легалізації. Усталений поділ процесу на три етапи - розміщення (placement), розшарування / приховування (layering)

та інтеграцію (integration) - не може застосовуватися однаково до фіатних і віртуальних схем [171, с. 502; 172, с. 41, 44]. Як показують Д. В. Каменський і С. С. Титаренко, за системного використання криптовалют, криптобірж та електронних гаманців ідеться передусім про етапи розміщення й приховування, тоді як до третьої стадії - інтеграції - бенефіціар нерідко не вдається взагалі, оскільки його влаштовує «депозитний» характер криптоактиву як форми збереження раніше здобутого злочинним шляхом майна [172, с. 44-45]. Базова схема при цьому має вигляд ланцюга «інтернет-обмінник - підконтрольний крипто-гаманець - багаторазові перекази низької вартості й високої швидкості» [172, с. 45]. Конкретні способи крипто-легалізації систематизує М. О. Думчиков, виокремлюючи п'ять основних: сервіси конвертації віртуальних активів із дробленням сум задля уникнення інтересу фінансового моніторингу; P2P-обмін, зокрема через крипто-банкомати; сайти азартних ігор, через які, за наведеними оцінками, відмивається близько третини «брудних» віртуальних активів; програми-міксери; а також фіктивні інтернет-магазини цифрових товарів [173, с. 119-120]. Д. В. Каменський і О. О. Дудоров, своєю чергою, акцентують на двох найпоширеніших технологіях - монетах конфіденційності (privacy coins) та криптозмішувачах (crypto-mixers), що практично унеможливляють відстеження походження коштів [171, с. 502-503]. Методологічним каркасом для опису наведених схем слугує трифазна модель відмивання, рекомендована Групою з розроблення фінансових заходів боротьби з відмиванням коштів (ФАТФ) і докладно викладена Т. Л. Дмитренко, із суттєвим застереженням, що стадії розміщення, розшарування та інтеграції здатні накладатися одна на одну залежно від конкретного механізму легалізації [174, с. 117-118]. Водночас наведені емпіричні зрізи варто сприймати з урахуванням часу їх формування: систематизація способів за М. О. Думчиковим відображає стан 2022 р., а виклад трифазної моделі за Т. Л. Дмитренко - 2020 р., тож вони мають передусім типологічну, а не статистично-актуальну цінність.

Практичний вимір протидії крипто-легалізації у кіберпросторі розкривається насамперед через діяльність національних регуляторів і

правоохоронних органів. За даними річного звіту Державної служби фінансового моніторингу України (Держфінмоніторингу) за 2022 рік, відомство ідентифікувало російські біткоїн-обмінники, пов'язані з підсанкційними банками, запровадило у взаємодії з криптопровайдерами «механізм спонтанного блокування» гаманців походженням із держави-агресора та звернулося до біржі Binance, яка 20 березня 2022 р. виключила можливість P2P-транзакцій для низки російських банків і платіжних систем зі санкційного списку [172, с. 46-47; 175, с. 21-22]. С. О. Грицай документує інституційне поглиблення цієї практики у 2021-2022 рр.: Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА), налагодило співпрацю з низкою криптобірж - Binance, Coinbase, KuCoin, Kraken і WhiteBit - для обміну ідентифікаційними даними власників гаманців виключно в межах кримінальних проваджень, а Україна разом із Грузією та Молдовою долучилася до проєкту Організації з безпеки і співробітництва в Європі (ОБСЄ) та Управління ООН з наркотиків і злочинності (UNODC) «Інноваційні політичні рішення щодо зменшення ризиків з відмивання грошей, пов'язаних з віртуальними активами» в межах Спільного плану дій на 2022-2024 рр. [175, с. 20, 22-23]. Порівняльно-правовий досвід підтверджує цей вектор: у Сполучених Штатах Америки §§ 1956 і 1957 Кодексу, сформульовані достатньо широко, дозволяють застосовувати кримінальну відповідальність до новітніх діджитальних схем, що ілюструють як справа «Сполучені Штати проти Костанцо», у якій операції з біткоїном визнано такими, що впливають на торгівлю між штатами, так і санкції Управління контролю за іноземними активами (OFAC) проти Жданової за крипто-відмивання в інтересах російських еліт [171, с. 504-506].

Кримінально-правова складова протидії функціонує не ізольовано, а в межах міжнародно та європейсько узгодженої регуляторної рамки. Поширення антилегалізаційного режиму на сферу віртуальних активів відбулося передусім через стандарти ФАТФ - із включенням до Глосарію понять «віртуальний актив» і «постачальник послуг, пов'язаних з оборотом віртуальних активів» та

встановленням у Рекомендації 15 вимог щодо ліцензування, реєстрації й нагляду [77; 79] - а також через Директиву (ЄС) 2018/843, яка поширила обов'язки належної перевірки клієнтів на надавачів послуг обміну між віртуальними та фіатними валютами й адміністраторів електронних гаманців [46; 171, с. 503]. В основу цього режиму покладено ризик-орієнтований підхід, за яким, як підкреслює Т. Л. Дмитренко, головною ознакою для інструментів є вартість, а для учасників ринку - ведення бізнесу з віртуальними активами; вирішальне значення мають процедури «знай свого клієнта», моніторинг та звітування про підозрілі операції [174, с. 122-123]. Подальша еволюція європейського регулювання пов'язується з Регламентом (ЄС) 2023/1114 (MiCA) [2], до норм якого має бути адаптовано національне законодавство України про віртуальні активи [175, с. 18-19].

Сукупність наведених позицій формує центральну політико-кримінальну дилему підрозділу - про достатність наявного кримінально-правового інструментарію. Д. В. Каменський і С. С. Титаренко обстоюють тезу, згідно з якою вдосконалення вітчизняної моделі протидії має відбуватися не шляхом редакційного уточнення диспозиції ст. 209 КК, а через розбудову нормативної бази та системи організаційно-правових заходів з боку регуляторів - Національного банку України, Держфінмоніторингу й Національної комісії з цінних паперів та фондового ринку - та правоохоронних органів; за такого підходу кримінально-правова складова відіграє радше допоміжну, ніж провідну роль порівняно з моніторингово-регуляторною [172, с. 41, 49]. Близьку, хоч і не тотожну, позицію займають Д. В. Каменський і О. О. Дудоров, які визнають, що ст. 209 КК загалом дозволяє давати належну кримінально-правову оцінку випадкам крипто-відмивання й потребує уточнення хіба що в частині визнання криптовалюти предметом [171, с. 508-509]. Ці тези, однак, потребують критичного зважування: пропозиції щодо пріоритету регуляторного інструментарію мають характер *de lege ferenda* і не усувають потреби в чіткому визначенні предмета злочину, без якого, як показано вище, кваліфікація залишається вразливою до темпоральних і понятійних заперечень.

Підсумовуючи, можна стверджувати, що проблема кримінально-правової протидії легалізації майна з використанням віртуальних активів перебуває на перетині трьох площин - догматичної (визначеність предмета ст. 209 КК), типологічної (специфіка етапів крипто-легалізації, за якої стадія інтеграції нерідко відсутня) та інституційно-регуляторної (фінансовий моніторинг і міжнародна співпраця). Вузловим залишається питання предмета: попри аргументоване розширення його обсягу через ст. 179-1 ЦК України [27], доктрина не досягла консенсусу, а апеляція до нечинного Закону № 2074-IX [1] здатна лише позначити перспективу, але не розв'язати проблему *de lege lata*. З огляду на викладене оптимальним видається не протиставлення «криміналізація - регуляторика», а їх узгоджене поєднання: чітка кримінально-правова заборона з визначеним предметом, доповнена ефективною системою фінансового моніторингу обігу віртуальних активів, гармонізованою зі стандартами ФАТФ [77] та правом ЄС, зокрема Регламентом MiCA [2].

3.3.2. Фінансування тероризму із використанням віртуальних активів

Підрозділ продовжує аналіз кримінальних правопорушень, що вчиняються з використанням віртуальних активів, у площині, суміжній із легалізацією, проте відмінній за спрямованістю, - фінансування тероризму та обхід міжнародних санкцій. Якщо легалізація за ст. 209 КК України [64] передбачає надання правомірного вигляду вже здобутому злочинним шляхом майну, то фінансування тероризму за ст. 258-5 КК України [64] полягає в наданні чи зборі коштів або іншого майна з усвідомленням того, що їх буде використано для фінансування тероризму, а отже, має перспективну, цільову спрямованість. Спільним є те, що в обох випадках віртуальні активи виступають інструментом, привабливість якого зумовлена анонімізаційним потенціалом, транснаціональністю та цілодобовою доступністю переказів; саме тому протидія обом явищам спирається на спільну інфраструктуру фінансового моніторингу і значною мірою - на спільне законодавче забезпечення.

Законодавчу основу протидії відмиванню коштів та фінансуванню тероризму під час здійснення операцій з віртуальними активами в Україні

становить Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» № 361-IX [12]. Як показує О. І. Кулик, цей Закон визначає поняття «віртуальний актив» (п. 13 ч. 1 ст. 1), фактично відтворюючи дефініцію ФАТФ, і «постачальник послуг, пов'язаних з обігом віртуальних активів», наділяючи останнього повноваженнями суб'єкта первинного фінансового моніторингу (п. 8 ч. 2 ст. 6); закріплення цих норм відповідає євроінтеграційним зобов'язанням за ст. 20 Угоди про асоціацію та рекомендаціям ФАТФ, зокрема щодо порогового значення належної перевірки у 30 тис. грн і ризик-орієнтованого визначення обсягу заходів перевірки (ст. 11 Закону) [176, с. 45]. Водночас автор виявляє істотну прогалину: ч. 1 ст. 14 Закону, визначаючи обсяг інформації, що супроводжує переказ на суму понад 30 тис. грн, не згадує про віртуальні активи, унаслідок чого ця норма фактично позбавлена механізму застосування до переказів ВА понад порогове значення, що суперечить логіці Закону й рекомендаціям ФАТФ; звідси - пропозиції уточнити ч. 1 ст. 14 щодо її поширення на операції з ВА, а п. 51 ч. 1 ст. 1 - щодо визнання постачальників таких послуг суб'єктами підприємницької діяльності [176, с. 45-46].

У порівняльно-правовій площині О. І. Кулик зауважує, що на рівні *acquis communautaire* відповідні питання врегульовано Директивою (ЄС) 2018/843 [46], яка, однак, оперує вузьким поняттям «віртуальна валюта» і визнає обміном віртуальних активів лише їх обмін на фіатну валюту, але не на інші ВА, що не повною мірою відповідає рекомендаціям ФАТФ [176, с. 46-47]. На цьому тлі окремі норми українського законодавства є навіть суворішими за рівнозначні стандарти ЄС, позаяк об'єктом фінансового моніторингу в Україні є обмін ВА як на фіатну валюту, так і на інші ВА [176, с. 47]. Слід наголосити, що базовий профільний Закон № 2074-IX лишається нечинним [1]; у праці О. І. Кулика він фігурує лише як законопроект, прийнятий у першому читанні [176, с. 45].

Особливо загостреним унаслідок збройної агресії є вимір використання віртуальних активів для обходу міжнародних санкцій проти російської федерації. Т. Л. Дмитренко показує, що, попри обмежену ліквідність

криптоактивів, яка не дозволяє повністю замінити ними системи на кшталт SWIFT, підсанкційні російські суб'єкти системно вдаються до криптоінструментів і мережі позабіржових (OTC) провайдерів, що пропонують готівкові виплати поза процедурами ідентифікації клієнтів [137, с. 109, 112-113]. Авторка систематизує санкційний інструментарій - внесення осіб до списку спеціально позначених і заблокованих осіб (SDN) Управління контролю за іноземними активами (OFAC), обмеження п'ятого пакета санкцій ЄС щодо володіння криптоактивами сумою в 10 тис. євро, «правило подорожей» (Travel Rule) ФАТФ, - водночас вказуючи на обмежену ефективність цих заходів: станом на червень 2021 р. переглянуті стандарти ФАТФ запровадили лише 58 зі 128 звітних юрисдикцій, а самі рекомендації не мають юридично обов'язкової сили [137, с. 110-111, 117]. До типових способів ухилення віднесено виведення капіталу через невзаємозамінні токени, монети конфіденційності, міксери та децентралізовані біржі [137, с. 114-115].

Протидія цим практикам в Україні поєднує регуляторні та правоохоронні заходи: замороження банками активів за підозри щодо їх зв'язку з тероризмом із повідомленням Служби безпеки України в умовах воєнного стану, обмеження транскордонних переказів постановою Правління Національного банку України від 24.02.2022 № 18, ідентифікацію Держфінмоніторингом спільно з Міністерством цифрової трансформації російських криптообмінників, пов'язаних із підсанкційними банками, та механізм спонтанного блокування криптогаманців у взаємодії з криптопровайдерами [137, с. 118-121]. На цій підставі Т. Л. Дмитренко обстоює тезу, що акцент слід робити на нагляді, а не на зміні нормативної бази [137, с. 114]. Цю позицію варто сприймати критично й з урахуванням її *de lege ferenda* характеру: сама авторка визнає, що реалізації нагляду перешкоджає невизначеність із державним регуляторним органом - за чинним Законом № 361-IX [12] ним є Міністерство цифрової трансформації, а за нечинним профільним Законом № 2074-IX [1] - Національна комісія з цінних паперів та фондового ринку й Національний банк України, які не можуть здійснювати нагляд, позаяк цей Закон набере чинності лише після внесення

змін до Податкового кодексу України [137, с. 119-120]. Отже, навіть послідовно «наглядова» модель упирається в незавершеність законодавчого контуру.

Узагальнюючи, протидія фінансуванню тероризму та обходу санкцій із використанням віртуальних активів становить самостійний, хоча й тісно пов'язаний із легалізацією, напрям. Його кримінально-правовим стрижнем залишається ст. 258-5 КК України [64], дієвість якої прямо залежить від ефективності превентивного контуру - фінансового моніторингу операцій з ВА за Законом № 361-IX [12], який, за оцінкою О. І. Кулика, загалом відповідає рекомендаціям ФАТФ [77], але потребує усунення прогалин, передусім у ч. 1 ст. 14 [176, с. 45-47]. Санкційний вимір, проаналізований Т. Л. Дмитренко, демонструє двоїсту природу віртуальних активів: вони є водночас інструментом ухилення від санкцій і - завдяки відстежуваності публічного блокчейну - джерелом доказової бази [137, с. 113-114]. Вирішальною умовою результативності протидії є завершення законодавчого врегулювання ринку ВА, поєднане з ризик-орієнтованим фінансовим моніторингом і міжнародною співпрацею, гармонізованими зі стандартами ФАТФ [77] та правом ЄС, зокрема Регламентом MiCA [2].

3.3.3. Шахрайство та кримінальні правопорушення проти власності, предметом або засобом яких є віртуальні активи

Серед кримінальних правопорушень, у яких віртуальні активи виступають предметом або засобом учинення, окреме й чи не найпоширеніше місце посідають посягання на власність, передусім шахрайство (ст. 190 КК України [64]). Особливість цієї групи полягає у подвійній кримінально-правовій ролі віртуального активу: він може бути як предметом посягання - благом, на яке безпосередньо спрямований протиправний умисел (заволодіння криптовалютою потерпілого), так і засобом (знаряддям) учинення - інструментом обману та подальшого виведення майна. Така двоїстість, помножена на технологічні властивості активів, ускладнює і кваліфікацію діяння за чинними нормами розділу VI Особливої частини КК України, і доказування його обставин, адже ці норми формувалися щодо традиційних

об'єктів матеріального світу, тоді як віртуальний актив існує винятково у цифровій формі й не має речового субстрату у звичному розумінні.

Відправним для кваліфікації є з'ясування того, чи здатний віртуальний актив бути предметом злочину проти власності. О. Кришевич і І. Рощина обґрунтовують, що криптовалюта є одним із різновидів віртуальних фінансових інструментів, якому притаманні всі ознаки предмета такого посягання: економічна (курс до офіційних валют, мінова та споживча вартість), фізична (вираження у специфічній цифровій формі - програмному коді) та юридична (належність іншій особі, «чужість» майна для винного) [177, с. 172]. Водночас автори наголошують на ключовій передумові: перш ніж визнати криптовалюту предметом злочину проти власності, її потрібно легітимувати як «майно» в межах цивільного законодавства [177, с. 172]. Чинний ЦК України прямо не відносить віртуальні активи до окремо визначених об'єктів права власності [27], а профільний Закон України «Про віртуальні активи» від 17 лютого 2022 року № 2074-IX, який визначає віртуальний актив як нематеріальне благо - особливий об'єкт цивільних прав, станом на час дослідження так і не було введено в дію [1]. Інше визначення - «цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних чи інвестиційних цілей» - містить Закон України № 361-IX у сфері протидії відмиванню коштів [12], проте воно орієнтоване на фінансовий моніторинг і саме по собі не вирішує питання речово-правового статусу активу для кваліфікації посягань на власність.

Теза про спроможність віртуального активу бути предметом посягань на власність дістала розвиток у вітчизняній доктрині: Т. Овсійчук розглядає віртуальні активи саме крізь призму предмета злочинів проти власності [152, с. 137], а К. Черевко порушує питання про умови та межі визнання їх предметом відповідних правопорушень [153]. Спільним є висновок, що відсутність сталого нормативного статусу активу не усуває його майнової цінності й потреби в кримінально-правовій охороні, а лише зміщує невизначеність у площину правозастосування.

Доктрина та практика відносять до посягань на власність, предметом яких можуть бути віртуальні активи, насамперед крадіжку (ст. 185), вимагання (ст. 189) і шахрайство (ст. 190 КК України) [64]. О. Кришевич і І. Рощина звертають увагу на специфіку кожного складу стосовно криптовалюти: викрадення активу відбувається не таємним заволодінням річчю, а опосередковано - через доступ до приватного ключа; вимагання набуває нових форм з огляду на можливість непомітної конвертації активу у фіат; а шахрайство пов'язується з обманом під час продажу чи обміну активу або заволодіння реквізитами доступу до нього, найтипівіше - через фішинг криптовалютних бірж [177, с. 171-172].

Окремий зріз проблематики становить незаконне привласнення віртуальних активів, докладно проаналізоване Ш. Давлатовим і А. Подгорною. Дослідники акцентують на швидкому зростанні цінності активів (зокрема ігрових - акаунтів, ігрової валюти, предметів, артефактів) та на класифікації активів за критерієм забезпеченості на забезпечені й незабезпечені, що має значення для встановлення предмета посягання [178, с. 71]. У вітчизняному правозастосуванні такі діяння найчастіше кваліфікують як шахрайство, а також за нормами розділу XVI Особливої частини КК України про правопорушення у сфері використання електронно-обчислювальних машин, систем і мереж [178, с. 71]. Водночас автори визнають, що чинне законодавство хоч і охоплює основні різновиди таких діянь, потребує уточнення й конкретизації, а сам стан охорони активів від кіберзлочинності не відповідає сучасним викликам [178, с. 73]. Слід враховувати, що це дослідження значною мірою зосереджене на віртуальних ігрових активах, тож поширення його висновків на інші види активів потребує обачності.

Чи не найгострішою для цієї групи посягань Ш. Давлатов і А. Подгорна вважають проблему доказування та ідентифікації осіб. Перешкодами слугують самі властивості активів: анонімність учасників, використання VPN, чужих акаунтів і реквізитів, методів соціальної інженерії, легкість підроблення або знищення цифрових слідів, а також несинхронізованість правових систем держав і недостатня технічна готовність правоохоронних органів [178, с. 72].

Наведена авторами національна судова практика підтверджує це: в одній справі суд відмовив у задоволенні клопотання через відсутність доказів, в іншій - затвердив угоду про визнання винуватості з призначенням штрафу [178, с. 72].

Якщо віртуальний актив виступає засобом учинення шахрайства, ключового значення набуває аналіз способів злочинної діяльності у кіберпросторі. М. Думчиков, який спеціально досліджував кваліфікацію кібершахрайства, констатує, що приблизно половина кримінальних правопорушень у кіберпросторі припадає саме на шахрайство, основною формою якого є фішинг - отримання персональних даних потерпілого шляхом обману або методів соціальної інженерії для подальшого протиправного використання [179, с. 162]. Привабливість віртуальних активів для злочинців автор пояснює їх специфічними ознаками: анонімністю та конфіденційністю операцій, транснаціональністю й децентралізованістю обігу, високою швидкістю та незначною вартістю транзакцій, а також незворотністю переказів і відсутністю механізму повернення коштів (charge-back) [179, с. 160-161]. Саме поєднання цих властивостей робить розслідування таких діянь технічно складним, а самі діяння - високолатентними.

М. Думчиков виокремлює кілька типових різновидів шахрайства, засобом якого є віртуальні активи: цільовий фішинг із перенаправленням користувачів на фіктивні («клоновані») вебсайти бірж, обмінників і гаманців; шахрайство під час купівлі та обміну активів; інвестування у фіктивні активи [179, с. 162]. Найпоширенішими є схема з випуском фіктивного токена (за процедурою, аналогічною ICO) з подальшим обманом інвесторів і цільовий фішинг через клони популярних сервісів із майже ідентичними доменними назвами [179, с. 162-163]. Такі схеми засвідчують, що шкода завдається не безпосереднім «зломом», а введенням потерпілого в оману, - тож конструкція ст. 190 КК України загалом охоплює подібні діяння, проте їх кіберпросторовий характер потребує врахування під час кваліфікації.

Спільною та найскладнішою для всієї цієї групи посягань є проблема визначення розміру заподіяної шкоди. Оскільки для матеріальних складів розмір майнових наслідків є кваліфікувальною ознакою, відсутність єдиного

способу конвертації віртуального активу в грошовий еквівалент - з огляду на волатильність курсу та невизначеність правового статусу активу - ускладнює інкримінування відповідних частин статей [177, с. 172]. До цього додаються труднощі ідентифікації винного, фіксації цифрових доказів [178, с. 72] та встановлення сукупного обсягу збитків у масових схемах [179, с. 163]. Отже, навіть за наявності формальних підстав кваліфікація діяння за ст. 190 КК України на практиці залишається проблемною щодо доказування.

З огляду на виявлені прогалини в опрацьованих джерелах сформульовано пропозиції *de lege ferenda*, які слід оцінювати саме як авторські, а не як чинні приписи. Так, О. Кришевич і І. Рощина пропонують доповнити примітку до ст. 185 КК України положенням, за яким під «чужим майном» у статтях 185, 190 і 191 розуміється, зокрема, криптовалюта, а також викласти ч. 3 ст. 190 КК України в редакції, що прямо передбачає вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки, автоматизованих систем, комп'ютерних мереж або платіжних порталів [177, с. 172-173]. М. Думчиков, своєю чергою, обстоює віднесення до віртуальних активів не лише криптовалют, а й NFT, віртуальних цінних паперів, токенизованих акцій та віртуального майна, а повноваження з регулювання відповідного ринку пропонує покласти на Національний банк України, доповнивши їх створенням міжвідомчих робочих груп національного й міжнародного рівня [179, с. 163-164]. Ці пропозиції відображають доктринальний пошук, проте мають оцінюватися з урахуванням того, що профільний Закон № 2074-IX лишається нечинним [1], а перспективна модель регулювання нині пов'язується із законопроектом про ринки віртуальних активів за зразком Регламенту ЄС MiCA; тому зміни до КК України доцільно узгоджувати саме з майбутньою регуляторною рамкою, а не з нечинними чи застарілими редакціями.

Узагальнюючи, віртуальні активи здатні виступати як предметом злочинів проти власності, так і засобом учинення шахрайства в кіберпросторі, що зумовлює потребу диференційованого підходу до кваліфікації. Чинні норми розділу VI Особливої частини КК України, насамперед ст. 190, у поєднанні з

кіберскладами розділу XVI загалом дають змогу реагувати на такі посягання, проте їх ефективне застосування стримується невизначеністю речово-правового статусу активу, складністю обрахунку шкоди й доказування. Розв'язання цих питань потребує не лише вдосконалення кримінального закону, а й завершення формування цивільно-правового та регуляторного підґрунтя обігу віртуальних активів, узгодженого з європейською моделлю, що й визначає місце цього складу в системі кримінально-правової політики у сфері забезпечення охорони віртуальних активів.

3.3.4. Незаконне збагачення та корупційні правопорушення, пов'язані з віртуальними активами

Окреме місце серед типових кримінальних правопорушень, пов'язаних із віртуальними активами, посідають незаконне збагачення та суміжні корупційні діяння, у яких віртуальні активи виступають предметом одержання неправомірної вигоди або засобом приховування її дійсного розміру та джерела. Норму про кримінальну відповідальність за незаконне збагачення (статтю 368-5 КК України [64]) було повернуто до тексту кодексу Законом України «Про внесення змін до деяких законодавчих актів України щодо конфіскації незаконних активів осіб, уповноважених на виконання функцій держави або місцевого самоврядування, і покарання за набуття таких активів» від 31 жовтня 2019 року № 263-IX [180]. Повторна криміналізація стала наслідком того, що попередню редакцію відповідної норми Конституційний Суд України визнав такою, що суперечить Конституції України; з огляду на це законодавець прагнув максимально чітко окреслити склад діяння та його юридичні конструкції, щоб норма була водночас ефективною і не створювала підґрунтя для зловживань. Принципово важливо, що частина третя статті 368-5 КК України прямо відносить до активів, набуття яких здатне утворити незаконне збагачення, нематеріальні активи, у тому числі криптовалюти [64]. Тим самим криптовалюта (а ширше - віртуальний актив) набула значення предмета корупційного за своєю природою кримінального правопорушення.

Як зауважує Т. П. Овсійчук, на дату повернення «незаконного збагачення» до переліку кримінально караних діянь термін «віртуальні активи» в законодавстві ще фактично не використовувався: профільний для сфери запобігання та протидії відмиванню коштів акт - Закон України № 361-IX [12] - було ухвалено майже на два місяці пізніше, що дає підстави припускати вживання законодавцем понять «криптовалюти» і «віртуальні активи» як значною мірою тотожних [181, с. 158]. Така першооснова закладає термінологічну неузгодженість, яку дослідник простежує й далі: якщо частина третя статті 368-5 КК України оперує поняттям «криптовалюти», то Закон України «Про запобігання корупції» від 14 жовтня 2014 року № 1700-VII [182] для цілей фінансового контролю послуговується терміном «віртуальні активи». Відомості про наявні криптовалюти підлягають зазначенню суб'єктами декларування, а Національне агентство з питань запобігання корупції уповноважене додатково визначати у формі декларації дані для ідентифікації об'єктів декларування - віртуальних активів [182]. Співвідношення цих категорій (їх тотожність, синонімічність чи відмінність) на нормативному рівні не розкрито, що, як обґрунтовано наголошує Т. П. Овсійчук, лише посилює невизначеність та ускладнює правозастосування у справах про незаконне збагачення і декларування [181, с. 159].

З позицій вчення про склад кримінального правопорушення віртуальні активи (криптовалюти) логічно віднести до предмета, який є ознакою об'єкта посягання. Предметом прийнято вважати речі матеріального світу, з певними властивостями яких кримінальний закон пов'язує наявність ознак конкретного складу; водночас сучасне розуміння предмета охоплює не лише матеріальні об'єкти, а й явища дійсності, які можна контролювати та змінювати, хоча вони й не мають вираженої фізичної форми (як-от інформація чи енергія) [181, с. 159]. Предмет визначається за фізичними, соціальними та юридичними ознаками, причому до фізичних характеристик належать матеріальність, кількість, якість, форма, стан і структура [181, с. 159]. Застосування цього доктринального інструментарію до віртуальних активів засвідчує, що вони відповідають оновленому, «дематеріалізованому» розумінню предмета, а отже,

можуть повноцінно виступати предметом незаконного збагачення, попри відсутність речової форми.

Привабливість віртуальних активів для вчинення корупційних правопорушень зумовлена сукупністю їх властивостей. М. О. Думчиков і А. М. Куліш, відштовхуючись від закріпленого в Законі України «Про віртуальні активи» розуміння віртуального активу як нематеріального блага, що є об'єктом цивільних прав, має вартість і виражене сукупністю даних в електронній формі, виокремлюють такі ознаки, як анонімність, майновий характер, конфіденційність операцій, транснаціональний характер і децентралізованість [183, с. 3-4]. При цьому самі автори застерігають, що згаданий профільний закон станом на час дослідження чинності не набрав [183, с. 3]; це застереження є принциповим, оскільки Закон України № 2074-IX [1] досі лишається нечинним, а тому наведена в ньому дефініція може використовуватися лише як перспективна (*de lege ferenda*) модель, а не як чинне позитивне право. За оцінкою дослідників, саме анонімність дозволяє приховувати фінансові операції та уникати контролю з боку державних органів і фінансових установ, а в поєднанні з майновим характером, конфіденційністю, транснаціональністю та децентралізованістю - істотно підвищує суспільну небезпечність корупційних діянь, предметом яких є віртуальні активи: на відміну від традиційного хабарництва в готівковій чи безготівковій формі, цифровий характер активу майже повністю нівелює «сліди», придатні для подальшого розслідування [183, с. 4].

М. О. Думчиков і А. М. Куліш описують і конкретні форми використання віртуальних активів у корупційній діяльності: одержання неправомірної вигоди безпосередньо у криптовалюті чи на електронний гаманець; передавання невзаємозамінних токенів (NFT) із подальшим заниженням або, навпаки, завищенням їх вартості для прихованого перерозподілу вартості; вручення подарункових криптовалютних сертифікатів із наступним обміном на криптовалюту та фіатні кошти; а також внесення недостовірних відомостей до декларації - декларування віртуальних активів, якими особа насправді не володіє, що створює «маневр» для майбутньої легалізації майна, одержаного

злочинним шляхом, і фактично виступає предикатним діянням [183, с. 5]. Як ілюстрацію автори наводять відомі з практики випадки: повідомлення про підозру народному депутатові України у зв'язку з обіцянкою неправомірної вигоди у криптовалюті Bitcoin в еквіваленті близько 50 тис. доларів США, а також підозру в недостовірному декларуванні криптовалюти на суму близько 24 млн грн, що належала іншій особі [183, с. 5]. Найпоширенішою формою цифрової корупції автори вважають легалізацію майна, одержаного злочинним шляхом, із застосуванням нерегульованих платформ, міксерів і «тумблерів», множинних адрес, номінальних власників та розгалужених транскордонних схем обміну [183, с. 5-6].

У міжнародному та порівняльному вимірі зв'язок віртуальних активів із корупцією та організованою злочинністю докладно проаналізовано в аналітичній довідці U4 Anti-Corruption Resource Centre та Transparency International, підготовленій С. Ельсаєд [184]. У ній наголошено, що криптовалюти стають дедалі привабливішим інструментом для організованих злочинних угруповань завдяки псевдонімності й децентралізованій природі, а їх протиправне використання вже не обмежується кіберзлочинністю та охоплює всі види діянь, пов'язаних із переміщенням вартості [184, с. 4-5]. До властивостей, що приваблюють злочинців, віднесено анонімність та псевдонімність, механізми входу та виходу з ринку (on-ramp/off-ramp), регуляторну невизначеність і транскордонне охоплення [184, с. 5-7]. Стосовно корупції у довідці окремо розглянуто підкуп та розтрату: наведено дані Асоціації сертифікованих експертів з питань шахрайства, за якими у 2021 році 8 % світових випадків шахрайства були пов'язані з використанням криптовалют, із них 48 % стосувалися виплати хабарів і «відкатів», а 43 % - конвертації привласнених активів у криптовалюту [184, с. 8]; згадано й кореляцію, виявлену в дослідженні Міжнародного валютного фонду, між ширшим використанням криптовалют і вищим рівнем сприйняття корупції [184, с. 7]. Окрему увагу приділено використанню криптоактивів для ухилення від санкцій [184, с. 13].

Як шляхи мінімізації ризиків у довідці запропоновано посилення регуляторного середовища, гармонізацію національних і наднаціональних правових рамок, розвиток міжнародного співробітництва та механізмів повернення активів, а також підвищення спроможності правоохоронних органів [184, с. 14-15]. Зазначено, що Група з розроблення фінансових заходів боротьби з відмиванням коштів переглянула свої рекомендації, поширивши їх на операції з віртуальними активами і запровадивши визначення «віртуального активу» та «постачальника послуг, пов'язаних з обігом віртуальних активів» (VASP) [184, с. 15], а в межах Європейського Союзу П'ята директива про запобігання відмиванню коштів - Директива (ЄС) 2018/843 [46] - зобов'язала криптобіржі та постачальників послуг гарантувати ідентифікувати своїх клієнтів [184, с. 7]. Водночас цю довідку слід використовувати з певними застереженнями: вона відображає погляд сектору міжнародного розвитку та антикорупційних організацій, зосереджена переважно на криптовалютах (автор окремо зазначає, що фінансові злочини наразі становлять лише незначну частку операцій з NFT [184, с. 2]), а наведені кількісні показники запозичені з галузевих звітів і подаються в переказі. З урахуванням цього її доцільно залучати як джерело узагальнень щодо міжнародних тенденцій і типології, а не як підставу для висновків про чинне національне регулювання.

Самостійний блок проблем, що має безпосереднє кримінально-правове значення, становлять декларування віртуальних активів і оцінка їх вартості. Т. П. Овсійчук звертає увагу на те, що вартість окремих віртуальних активів можна визначити на криптобіржі, проте ринок залишається нестабільним, а поява невзаємозамінних токенів (NFT) узагалі унеможливорює їх оцінку біржовими механізмами через унікальність таких об'єктів, що вимагає розроблення альтернативних методик [181, с. 159]. Чинний національний стандарт оцінки об'єктів права інтелектуальної власності не задовольняє потреб оцінки криптоактивів, а отже, потребують ухвалення спеціальні правила (стандарт, методика) [181, с. 160]. Особливо показовою є ситуація, коли NFT створюється безпосередньо суб'єктом декларування: його вартість залишається невідомою, оскільки жодного правочину щодо нього не вчинялося, а подальше

відчуження такого активу здатне забезпечити легалізацію будь-якого незаконного доходу, - тому суспільний інтерес полягає в незалежній експертній оцінці реальної вартості активу [181, с. 160]. Дослідник окремо вказує на «мінімальну суму», за якої незаконне збагачення набуває кримінально караного характеру: відповідно до частини першої статті 368-5 КК України це перевищення законних доходів більш ніж на шість тисяч п'ятсот неоподатковуваних мінімумів доходів громадян [64], що, за обчисленням автора (з урахуванням прирівнювання неоподатковуваного мінімуму до податкової соціальної пільги, яка станом на 1 січня 2025 року становила 1514 грн), еквівалентне приблизно 9,84 млн грн [181, с. 159]. Додатковою перешкодою для протидії є дефіцит фахівців, здатних виступати спеціалістами у слідчих (розшукових) діях у відповідній категорії справ, на що звертають увагу й дослідники, на яких посиляється автор [181, с. 160].

Узагальнюючи, віртуальні активи є повноцінним предметом незаконного збагачення та інструментом учинення суміжних корупційних правопорушень, однак прогалини й термінологічні неузгодженості чинного законодавства створюють передумови для уникнення відповідальності. Ключовими напрямками вдосконалення видаються: розроблення уніфікованої термінології у сфері віртуальних активів, узгодженої з Регламентом (ЄС) 2023/1114 (MiCA) [2], та набрання чинності профільним законом, який наразі такої чинності не має [1]; формування справедливої методології визначення вартості віртуальних активів, у тому числі невзаємозамінних токенів, для цілей декларування і кримінально-правової кваліфікації; підвищення компетентності сторін кримінального провадження та суду щодо порядку створення, обміну й відчуження таких активів [181, с. 160]. Ці заходи органічно доповнюються запровадженням ефективного регулювання ринку та стандартів протидії відмиванню коштів і фінансуванню тероризму для постачальників послуг, пов'язаних з обігом віртуальних активів, а також забезпеченням міжнародної співпраці й обміну інформацією [183, с. 6], адже корупція, предметом якої є віртуальні активи, з огляду на свій транснаціональний і латентний характер

становить загрозу не лише фінансовій стабільності, а й національній безпеці держави [183, с. 5; 184, с. 14].

3.3.5. Кіберкримінальні правопорушення (Розділ XVI КК України) та кримінально-правова охорона безпеки інфраструктури ринку віртуальних активів

Віртуальні активи існують виключно в цифровому середовищі, а отже, їхня наявність, оборотоздатність і сама приналежність конкретному суб'єктові забезпечуються інформаційними системами, криптографічними механізмами та інтернет-інфраструктурою. Унаслідок цього надійність віртуальних активів є похідною від рівня кібербезпеки середовища, у якому вони обертаються: будь-яка вразливість програмного забезпечення, протоколів шифрування чи інфраструктури обміну безпосередньо позначається на цілісності, доступності та конфіденційності таких активів. Як наголошує колектив авторів (Ю. Юринець, Є. Криволап, Л. Белкін, М. Белкін), високий рівень кіберзахисту є не додатковою, а базовою умовою існування віртуальних активів, оскільки їх функціонування нерозривно пов'язане з кіберпростором [185, с. 1125]. Це твердження має пряме кримінально-правове значення: посягання на інформаційні системи, у яких «існують» віртуальні активи, водночас є посяганням на майнові інтереси їх володільців, а тому потребує оцінки за нормами розділу XVI Особливої частини КК України [64] у системному зв'язку з нормами про кримінальні правопорушення проти власності.

Нормативним підґрунтям для поширення на віртуальні активи режиму кіберзахисту є їх легальне визнання різновидом цифрової речі. Унаслідок доповнення Цивільного кодексу України статтею 179-1 (Закон України від 10.08.2023 № 3320-IX) [28] віртуальні активи прямо віднесено до цифрових речей - благ, що створюються та існують виключно у цифровому середовищі й мають майнову цінність [27]. На цю обставину звертають увагу й дослідники, які зазначають, що в силу законодавчого визначення віртуальних активів цифровою річчю на них поширюються способи та методи кібербезпеки і кіберзахисту [185, с. 1122-1123]. Об'єкти кібербезпеки та кіберзахисту

визначено статтею 4 Закону України «Про основні засади забезпечення кібербезпеки України» [188], відносячи до них, зокрема, конституційні права і свободи людини та сталий розвиток цифрового комунікативного середовища. Системне тлумачення наведених приписів дозволяє стверджувати, що інформаційна інфраструктура ринку віртуальних активів є самостійним об'єктом, безпека якого підлягає кримінально-правовій охороні.

З'ясування кола об'єктів такої охорони потребує звернення до поняття інфраструктури ринку віртуальних активів. У вітчизняній доктрині її визначено як сукупність елементів, що забезпечують, регулюють і створюють умови для нормального, ефективного та безперебійного функціонування цього ринку [186, с. 185]. До елементів спеціального призначення такої інфраструктури О. Кулик відносить постачальників послуг, пов'язаних з обігом віртуальних активів (зокрема криптобіржі та обмінні сервіси), емітентів (майнерів) і саморегулювні організації, водночас обґрунтовано не зараховуючи до них користувачів ринку [186, с. 188]. Слід урахувувати, що це дослідження виконане на основі законопроекту «Про віртуальні активи» від 11 червня 2020 р. № 3637, який не набув сили закону: запропонована класифікація елементів інфраструктури зберігає аналітичну цінність, проте відправним національним орієнтиром нині слугує (попри нечинність) Закон України № 2074-IX [1], а перспективним - наближена до Регламенту MiCA [2] модель регулювання. Саме перелічені елементи інфраструктури - насамперед криптобіржі, гаманцеві та кастодіальні сервіси - і виступають типовими цілями протиправних кіберпосягань, оскільки концентрують доступ до значних обсягів віртуальних активів.

Найбільш вразливим вузлом цієї інфраструктури є технічні засоби забезпечення доступу до активу - гаманці та ключі віртуальних активів. А. Донець обґрунтовано зауважує, що ключ віртуального активу має підвищену безпекову важливість, адже в більшості випадків він є єдиним зв'язком між власником і активом, а лише незначна частина постачальників послуг передбачає можливість відновлення доступу в разі його втрати [187, с. 49]. Звідси випливає, що сутність схоронності віртуального активу полягає не у збереженні його внутрішніх властивостей, а в недопущенні протиправних

посягань і забезпеченні гарантованого доступу володільця до активу [187, с. 56]. Дослідник систематизує і типові способи протиправного заволодіння: безпосередній злам онлайн-сервісу або протиправні дії його адміністратора, фішинг із отриманням доступу до персональних даних і ключів, а також отримання доступу до комп'ютера, смартфона чи матеріального носія, на яких зберігаються ключі [187, с. 56]. Окремої уваги заслуговує розмежування кастодіальних і некастодіальних гаманців: у першому випадку приватними ключами володіє та керує третя особа, тоді як у другому контроль над активами й ключами повністю належить користувачеві, який і несе ризик їх втрати [187, с. 54-55]. Це розмежування є визначальним для встановлення суб'єкта, чію інформаційну систему атаковано, та для відмежування несанкціонованого втручання ззовні від несанкціонованих дій особи, яка має право доступу.

Забезпечення безпеки обігу віртуальних активів утворює систему організаційних, правових і технічних заходів, спрямованих на запобігання, попередження та виявлення протиправних дій щодо фінансово-розрахункових операцій і пов'язаних з ними даних [189, с. 63-64]. У межах кіберзахисту таких відносин В. Добровольська виокремлює, зокрема, засоби автентифікації (у тому числі багатофакторної та біометричної), криптографічний захист інформації, антивірусні засоби, а також технологію блокчейн, що завдяки децентралізованості, прозорості та захищеності від несанкціонованого доступу здатна підвищити стійкість систем кіберзахисту [189, с. 62-63]. Дослідниця слушно акцентує, що частина 2 статті 9 Закону України «Про віртуальні активи» покладає на учасника ринку обов'язок до проведення операцій ознайомитися з особливостями функціонування систем забезпечення обороту віртуальних активів [189, с. 61]. Базовими складовими інформаційної безпеки, на захист яких спрямовано ці заходи, є цілісність, конфіденційність і доступність відповідних даних; саме ці три параметри безпосередньо страждають унаслідок кібератак на криптобіржі та гаманці, що призводить до втрати власником доступу до коштів [185, с. 1125-1126]. Водночас слід ураховувати, що Закон України № 2074-IX, на компетенційні приписи якого (статті 16, 17) посилаються дослідники, відносячи визначення вимог щодо

інформаційної безпеки та кібербезпеки постачальників послуг до повноважень НКЦПФР і НБУ [185, с. 1124], станом на час дослідження ще не введено в дію [1], а відтак ці вимоги мають перспективний (*de lege ferenda*) характер і фактично відсилаються до підзаконного рівня.

Кримінально-правова охорона безпеки інфраструктури ринку віртуальних активів забезпечується насамперед нормами розділу XVI Особливої частини КК України, що встановлюють відповідальність за кримінальні правопорушення у сфері використання інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем і мереж [64]. Несанкціоноване втручання в роботу таких систем криптобіржі, гаманцевого чи кастодіального сервісу, що призвело до витоку, спотворення або блокування інформації чи до перехоплення контролю над активами, охоплюється статтею 361 КК України. Створення з метою протиправного використання, розповсюдження чи збут шкідливих програмних або технічних засобів, призначених для несанкціонованого втручання (зокрема для викрадення ключів або компрометації гаманців), кваліфікується за статтею 361-1 КК України, а несанкціоновані дії з інформацією, яку оброблюють у відповідних системах, учинені особою, яка має право доступу до неї (наприклад, недобросовісним адміністратором кастодіального сервісу), - за статтею 362 КК України. Порушення правил експлуатації систем або порядку чи правил захисту інформації, що спричинило відповідні наслідки, охоплюється статтею 363, а перешкоджання роботі систем шляхом масового поширення повідомлень електрозв'язку (зокрема внаслідок DDoS-атак на біржі) - статтею 363-1 КК України [64].

Особливість посягань на інфраструктуру ринку віртуальних активів полягає в тому, що несанкціоноване втручання здебільшого є не самоціллю, а способом протиправного заволодіння активами. У таких випадках вчинене не вичерпується кіберскладом: якщо внаслідок втручання в роботу інформаційної системи відбувається заволодіння віртуальними активами, діяння потребує кваліфікації за сукупністю відповідного кіберправопорушення (розділ XVI КК України) і посягання проти власності - насамперед шахрайства (стаття 190 КК

України) або викрадення чи привласнення, докладно розглянутих у підрозділі 3.3.3 цієї роботи. Така сукупність відображає різноманітність об'єктів посягання: з одного боку - безпека інформаційних систем і встановлений порядок їх функціонування, з іншого - відносини власності щодо віртуального активу. Технічна природа віртуального активу як реєстрового запису, доступ до якого опосередковано ключем [187, с. 48-49], зумовлює те, що заволодіння активом фактично здійснюється через отримання неправомірного контролю над відповідною інформацією, що додатково підкреслює тісний зв'язок кіберскладів із майновими посяганнями.

Чинний стан правового регулювання у цій сфері характеризується фрагментарністю. Дослідники справедливо вказують на відсутність чітких стандартів кіберзахисту для постачальників послуг, пов'язаних з обігом віртуальних активів, неврегульованість питань відповідальності за втрату активів унаслідок кіберінцидентів, а також складність кваліфікації криптоактивів у кримінальному та цивільному процесі [185, с. 1127-1128]. Подолання цих прогалин потребує закріплення на законодавчому рівні мінімальних вимог кібербезпеки для суб'єктів ринку, визначення особливостей кримінальної відповідальності за порушення кібербезпеки у сфері віртуальних активів і вдосконалення процесуальних норм щодо доказування у відповідних провадженнях [185, с. 1128], а також гармонізації національного підходу з правом ЄС, яке поєднує фінансово-правове регулювання ринку криптоактивів (Регламент MiCA [2]) із вимогами цифрової операційної стійкості фінансового сектору. З огляду на викладене безпека інфраструктури ринку віртуальних активів - криптобірж, гаманцевих і кастодіальних сервісів - має розглядатися як самостійний об'єкт кримінально-правової охорони, а кіберсклади розділу XVI КК України - як основний, але не єдиний інструмент протидії посяганням на віртуальні активи, що вчиняються з використанням несанкціонованого втручання в роботу інформаційних систем.

3.3.6. Використання віртуальних активів в організації азартних та онлайн-ігор

Серед кримінальних правопорушень, що вчиняються з використанням віртуальних активів, окрему групу утворюють діяння, пов'язані з організацією та проведенням азартних і онлайн-ігор. Стрімка цифровізація сфери розваг, поширення інтернет-платформ для гри та формування навколо них самостійної віртуальної економіки призвели до того, що віртуальні активи дедалі частіше виступають інструментом, через який опосередковується як легальна, так і протиправна діяльність у цьому сегменті. Безпосереднім кримінально-правовим засобом охорони відповідних суспільних відносин в Україні виступає ст. 203-2 КК України [64], яка в чинній редакції встановлює відповідальність за незаконну діяльність з організації або проведення азартних ігор, лотерей.

Зміст цієї норми зазнав принципового оновлення у зв'язку з ухваленням Закону України «Про державне регулювання діяльності щодо організації та проведення азартних ігор» [190], який легалізував гральний бізнес і запровадив ліцензійну модель його провадження. Якщо первісно ст. 203-2 КК України криміналізувала зайняття гральним бізнесом як таким - в умовах загальної заборони, то після набрання чинності зазначеним Законом її диспозицію було звужено й переорієнтовано: кримінально караними визнаються організація або проведення азартних ігор без ліцензії на провадження відповідного виду діяльності, випуск чи проведення лотерей особою, яка не має статусу оператора лотерей, а також організація чи функціонування закладів з метою надання доступу до азартних ігор або лотерей, що проводяться в мережі Інтернет [64]. Тим самим норма набула вираженого бланкетного характеру: висновок про злочинність діяння неможливий без звернення до приписів профільного законодавства про гральний бізнес, яке визначає, які саме види діяльності, за яких умов і на підставі якої ліцензії є дозволеними. Саме ця конструкція має ключове значення для оцінки операцій із віртуальними активами, оскільки переносить центр кваліфікації з виду майна, що використовується у грі, на додержання дозвільного порядку її організації.

Питання використання віртуальних активів у цій сфері предметно дослідив О. Кулик. Учений констатує, що поряд із розвитком ринків азартних ігор дедалі ширшого застосування набувають криптовалютні платежі, а в інтернет-середовищі поширилися платформи, що оперують віртуальними активами, - так звані «крипто казино» [191, с. 44]. Аналізуючи співвідношення віртуального активу з категоріями «ставка» та «виграш (приз)», дослідник доходить висновку, що умовою проведення азартних ігор із віртуальними активами у якості виграшу (призу) або ставки є відсутність у законодавстві заборон щодо використання таких активів для платіжних цілей чи як предмета обміну на майно (товари), роботи (послуги) [191, с. 45].

Ключову перешкоду для однозначної правової оцінки таких операцій О. Кулик вбачає у внутрішній суперечливості національного регулювання. З одного боку, ч. 7 ст. 4 Закону України «Про віртуальні активи» [1] встановлює, що віртуальні активи не є засобом платежу на території України та не можуть бути предметом обміну на майно (товари), роботи (послуги); з іншого - Регламент (ЄС) 2023/1114 (MiCA) [2] допускає використання криптоактивів із платіжною функцією. На цій підставі дослідник обґрунтовує, що відповідні заборонні положення національного закону потребують виключення, а віртуальним активам об'єктивно властиві платіжні функції, реалізація яких залежить лише від дозволу чи заборони законодавця [191, с. 45]. Водночас слід наголосити, що сам Закон України «Про віртуальні активи» [1] станом на цей час не набрав чинності, а тому окреслена суперечність наразі має радше потенційний характер і потребує усунення ще до запуску національного ринку віртуальних активів та приведення профільного закону у відповідність до Регламенту MiCA [2].

Спираючись на цивілістичну кваліфікацію віртуального активу як цифрової речі (ст. 179-1 ЦК України [27], запровадженої Законом України № 3320-IX [28]) та як майна (ст. 190 ЦК України [27]), О. Кулик доходить висновку, що віртуальний актив може охоплюватися поняттям «виграш (приз)», а за умови використання його як ставки - кваліфікуватися як електронний грошовий замінник, тобто ігровий замінник гривні [191, с. 46]. Принципово

важливим для кримінально-правової оцінки є висновок ученого про те, що використання віртуальних активів під час проведення азартних ігор не виводить суб'єкта господарювання з-під дії профільного законодавства, зокрема в частині необхідності отримання відповідної ліцензії [191, с. 46]. Це означає, що діяльність «крипто казино», яке організовує азартні ігри з віртуальними активами без ліцензії або забезпечує доступ до таких ігор у мережі Інтернет, за наявності всіх ознак складу підпадає під ознаки кримінального правопорушення, передбаченого ст. 203-2 КК України [64], незалежно від того, що ставки та виграші номіновані саме у віртуальних активах. Отже, спосіб номінування ставки чи виграшу у віртуальному активі сам по собі не декриміналізує діяння й не звільняє організатора від ліцензійних вимог.

Цей висновок узгоджується з міжнародними стандартами. У Рекомендаціях ФАТФ [77] та в Оновлених настановах щодо ризик-орієнтованого підходу до віртуальних активів і постачальників послуг, пов'язаних з їх обігом [79], діяльність із надання послуг, пов'язаних з обігом віртуальних активів, кваліфікується за функціональним критерієм - незалежно від того, як держава найменує чи маркує відповідного суб'єкта. За такого підходу оператор «крипто казино», що приймає та виплачує віртуальні активи, фактично виконує функції постачальника послуг, пов'язаних з обігом віртуальних активів (VASP), і підпадає під відповідні вимоги фінансового моніторингу. О. Кулик слушно зауважує наявну неузгодженість термінології Закону України «Про віртуальні активи» [1] із Законом України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [12] у частині видів діяльності постачальника послуг і пропонує доповнити п. 8 ч. 1 ст. 1 Закону № 2074-IX положенням про те, що участь і надання фінансових послуг, пов'язаних із пропозицією емітента та/або продажем віртуальних активів, є одним із видів діяльності такого постачальника [191, с. 47]. Ця пропозиція має характер *de lege ferenda* і спрямована на узгодження національного регулювання з

рекомендаціями ФАТФ; її реалізація сприятиме чіткішому окресленню кола суб'єктів, які несуть обов'язки у сфері протидії відмиванню коштів та фінансуванню тероризму, а отже, поліпшить передумови для виявлення та кваліфікації відповідних правопорушень.

Окремий, але тісно дотичний пласт проблем пов'язаний з онлайн-іграми, у межах яких обертаються віртуальні активи. О. Співак, аналізуючи правове регулювання та захист майнових прав на віртуальні активи споживачів онлайн-ігор, відзначає, що одними з найбільш популярних і комерційно успішних віртуальних просторів є масові багатокористувацькі рольові онлайн-ігри (MMORPG), у яких винагороди у вигляді ігрової валюти або внутрішньоігрових цінних предметів формують основу економічних відносин між учасниками, а вартість окремих об'єктів може сягати від кількох десятків до десятків тисяч доларів США [192, с. 418]. Дослідник звертає увагу, що розробники захищають свої права як власники ліцензій за допомогою ліцензійної угоди з кінцевим користувачем (EULA) та умов обслуговування (ToS), проте на практиці віртуальна власність продається між гравцями за реальні кошти - практика, що дістала назву торгівлі реальними грошима (RMT) [192, с. 418].

За методом обміну О. Співак розрізняє три моделі віртуальних валют в онлайн-іграх: систему із закритим потоком, за якої віртуальні кошти обмінюються лише на віртуальні товари чи послуги; систему з відкритим потоком, що допускає обмін на реальні гроші, товари та послуги; а також гібридну систему [192, с. 418]. Саме системи з відкритим і гібридним потоком, які уможливають конвертацію внутрішньоігрових цінностей у реальні кошти, набувають кримінально-правового значення, оскільки розмивають межу між ігровим розважальним контентом і фінансовою операцією. Підтримуючи позицію про ознаки об'єктів віртуального світу - нетілесний характер, незалежність, придатність до контролю, використання та цінність, дослідник доходить висновку, що віртуальними предметами, здатними бути віртуальним майном у грі, є артефакти (екіпірування персонажів), віртуальні простори та віртуальні персонажі (аватари) [192, с. 419].

Зіставлення наведених позицій дає підстави окреслити кілька значущих для кримінально-правової політики аспектів. По-перше, використання віртуальних активів в азартних іграх не утворює самостійного складу кримінального правопорушення, а лише ускладнює застосування вже наявної норми - ст. 203-2 КК України [64]: предметом ставки чи виграшу виступає актив, що не має офіційного курсу, характеризується відносною анонімністю та транскордонністю обігу, а це утруднює як виявлення протиправної діяльності, так і доказування та обчислення її масштабу. По-друге, дискусійним залишається розмежування власне азартних ігор та онлайн-ігор з елементами монетизації: якщо участь у грі передбачає внесення гравцем ставки (зокрема у вигляді віртуального активу), результат якої залежить від випадковості, а виграш має майнову цінність і може бути конвертований у реальні кошти (за класифікацією О. Співака - у системах з відкритим або гібридним потоком [192, с. 418]), то відповідна діяльність за своїми ознаками наближається до азартної гри й потенційно охоплюється профільним законодавством [190] та ст. 203-2 КК України [64]. По-третє, переважно офшорний характер значної частини «крипто казино» та відсутність їх прив'язки до української юрисдикції створюють практичні перешкоди для притягнення до відповідальності, що об'єктивно зміщує акцент кримінально-правової політики у бік превентивних і регуляторних механізмів - обмеження доступу, фінансового моніторингу та міжнародного співробітництва.

Викладене дозволяє констатувати, що чинна ст. 203-2 КК України [64] у системному поєднанні із Законом України «Про державне регулювання діяльності щодо організації та проведення азартних ігор» [190] у цілому здатна охопити випадки незаконної організації азартних та онлайн-ігор із використанням віртуальних активів, оскільки криміналізує саме недотримання ліцензійного (дозвільного) порядку, а не вид майна, що використовується як ставка чи виграш. Водночас ефективність такої охорони безпосередньо залежить від усунення суперечностей у регулюванні правового режиму віртуальних активів - насамперед від узгодження положень Закону України «Про віртуальні активи» [1], який ще не набрав чинності, із Регламентом МіСА

[2] щодо платіжної функції віртуальних активів, а також від гармонізації термінології цього Закону із Законом України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [12] і рекомендаціями ФАТФ [77; 79]. До моменту запуску національного ринку віртуальних активів і приведення законодавства у відповідність до європейських стандартів кримінально-правова політика у цьому сегменті має орієнтуватися переважно на бланкетне застосування ст. 203-2 КК України в системному зв'язку з регуляторними та фінансово-моніторинговими інструментами.

Висновки до розділу 3

Проведене в розділі дослідження кримінальних правопорушень, що вчиняються щодо віртуальних активів або з їх використанням, дозволяє сформулювати такі висновки.

1. Віртуальні активи посідають у системі об'єктів та предметів кримінальних правопорушень неоднозначне місце: залежно від обставин вони виступають предметом правопорушення (насамперед проти власності), засобом або знаряддям його вчинення, предметом незаконного збагачення та об'єктом фінансового моніторингу тощо. Така багатофункціональність вимагає попереднього розмежування ролей, оскільки помилкове ототожнення предмета посягання із засобом його вчинення спотворює юридичну оцінку діяння.

2. За чинним цивільним законодавством віртуальні активи визнаються майном і різновидом цифрової речі (стаття 179-1 ЦК України, запроваджена Законом № 3320-IX) і наділені всіма ознаками предмета злочинів проти власності - фізичною, економічною та юридичною; де-юре підставою такого визнання є саме стаття 179-1 ЦК України, а не нечинний Закон № 2074-IX. Контроль над приватним ключем і незворотність транзакцій ускладнюють встановлення власника та моменту вибуття активу, що позначається на доказуванні.

3. Обґрунтовано багатовимірну систематизацію правопорушень: за роллю активу у складі (предмет; засіб чи спосіб вчинення; об'єкт протиправного впливу), за технологічним критерієм (кіберуможливлені та кіберзалежні посягання) і за об'єктом охорони з прив'язкою до статей Кримінального кодексу України. Кримінологічно фіксується зростання абсолютного обсягу незаконного використання за зменшення його відносної частки, а методологічна нестабільність статистики обґрунтовує потребу систематизації для цілей кваліфікації та єдності практики.

4. Протидія легалізації (стаття 209 КК України) перебуває на перетині догматичної (визначеність предмета), типологічної (специфіка етапів крипто-легалізації, за якої стадія інтеграції нерідко відсутня) та інституційно-регуляторної площин. Вузловим залишається питання предмета, щодо якого доктрина консенсусу не досягла, а апеляція до нечинного № 2074-IX лише позначає перспективу; оптимальним є поєднання чіткої заборони з визначенням предметом та ефективного фінансового моніторингу, гармонізованого з ФАТФ і МіСА.

5. Протидія фінансуванню тероризму та обходу санкцій (стаття 258-5 КК України) становить самостійний напрям із перспективною, цільовою спрямованістю діяння, дієвість якого залежить від фінансового моніторингу за Законом № 361-IX, що загалом відповідає рекомендаціям ФАТФ, але потребує усунення прогалин. Санкційний вимір засвідчує двоїсту природу активів - інструмент ухилення і водночас джерело доказової бази завдяки відстежуваності блокчейну, - а результативність протидії впирається в незавершеність законодавчого контуру та невизначеність регулятора.

6. Віртуальні активи здатні бути і предметом, і засобом учинення шахрайства в кіберпросторі (стаття 190 КК України); чинні норми розділу VI у поєднанні з кіберскладами розділу XVI загалом дають змогу реагувати на такі посягання, проте їх застосування стримується невизначеністю речово-правового статусу активу, складністю обрахунку шкоди з огляду на волатильність і труднощами доказування. Розв'язання потребує не лише

вдосконалення кримінального закону, а й завершення цивільно-правового та регуляторного підґрунтя обігу активів.

7. Частина третя статті 368-5 КК України прямо відносить до відповідних активів нематеріальні активи, у тому числі криптовалюти, унаслідок чого віртуальний актив набуває значення повноцінного предмета корупційного правопорушення і засобу приховування неправомірної вигоди. Перешкодами для протидії є термінологічна неузгодженість законодавства («криптовалюти» в Кодексі і «віртуальні активи» в антикорупційному законодавстві) та брак методології визначення вартості активів, насамперед невзаємозамінних токенів, для цілей декларування і кваліфікації.

8. Безпека інформаційної інфраструктури ринку віртуальних активів - криптобірж, гаманцевих і кастодіальних сервісів - є самостійним об'єктом кримінально-правової охорони з найвразливішим вузлом у ключах і гаманцях. Несанкціоноване втручання здебільшого є способом протиправного заволодіння активом і потребує кваліфікації за сукупністю кіберскладу розділу XVI КК України та посягання проти власності, а фрагментарність регулювання зумовлює потребу закріплення мінімальних вимог кібербезпеки для постачальників послуг і гармонізації з правом ЄС (MiCA та вимоги цифрової операційної стійкості).

9. Стаття 203-2 КК України після легалізації грального бізнесу набула вираженого бланкетного характеру, криміналізуючи недотримання ліцензійного (дозвільного) порядку, а не вид майна, що використовується як ставка чи виграш. Діяльність «крипто казино» без ліцензії підпадає під ознаки цього складу незалежно від номінування ставок і виграшів у віртуальних активах; ефективність охорони залежить від усунення суперечностей правового режиму активів, насамперед від узгодження положень нечинного № 2074-IX із MiCA щодо їх платіжної функції.

РОЗДІЛ 4.

ВЗАЄМОЗВ'ЯЗОК КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ВІРТУАЛЬНИХ АКТИВІВ З КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОЮ ТА КРИМІНАЛЬНО-ВИКОНАВЧОЮ ПОЛІТИКОЮ

4.1. Особливості кримінального процесуального доказування, досудового розслідування та укладення угод у провадженнях, пов'язаних з віртуальними активами

Кримінально-правова політика у сфері забезпечення охорони віртуальних активів не вичерпується конструюванням складів правопорушень та визначенням меж караності. Її дієвість перевіряється насамперед у площині кримінального провадження, де охоронна функція держави реалізується через доказування обставин учиненого, досудове розслідування й застосування процесуальних механізмів повернення та вилучення активів. Саме тому взаємозв'язок матеріальної кримінально-правової політики з кримінальною процесуальною політикою має для віртуальних активів особливе, а подекуди й визначальне значення: матеріально-правова заборона, не забезпечена адекватними процесуальними інструментами виявлення, фіксації, доказування та повернення активу, залишається декларативною. Виклад у цьому підрозділі побудовано довкола трьох змістовно поєднаних вузлів - доказування у провадженнях, пов'язаних з віртуальними активами, проблем досудового розслідування таких правопорушень та особливостей укладення угод у кримінальному провадженні щодо незаконного заволодіння віртуальними активами, - кожен з яких розглядається крізь призму його дотичності до завдань охорони віртуальних активів засобами кримінального права.

Наскрізною для підрозділу є теза про те, що сама можливість процесуального доказування й розслідування у цій сфері значною мірою похідна від регуляторно-політичного вибору включити постачальників послуг,

пов'язаних з обігом віртуальних активів, до периметра протидії відмиванню коштів та фінансуванню тероризму відповідно до стандартів ФАТФ [77], п'ятої директиви ЄС про запобігання відмиванню коштів [46] та MiCA [2]: саме обов'язки таких постачальників щодо ідентифікації клієнтів і фіксації операцій перетворюють їх на ключове джерело верифікованих доказів.

Центральною проблемою доказування у провадженнях, пов'язаних з віртуальними активами, є відсутність у кримінальному процесуальному законі спеціального механізму використання таких активів у доказуванні та невизначеність їхнього процесуального статусу. Як обґрунтовано доводить О. Старенький, регулювання віртуальних активів є фрагментарним і нормативно неузгодженим між цивільним, фінансовим, антикорупційним, кримінальним та кримінальним процесуальним законодавством, унаслідок чого склалася «законодавчо сформована, проте фактично не імплементована модель», що породжує стан правової невизначеності [193, с. 247-249]. Єдина пряма згадка віртуальних активів у Кримінальному процесуальному кодексі України [144] міститься в частині десятій статті 170 і стосується можливості накладення на них арешту, тоді як спеціальних процедур пошуку, виявлення, вилучення та фіксації віртуальних активів кодекс не передбачає, що становить суттєву нормативну прогалину [193, с. 255-256]. Ця прогалина має не суто технічний, а політико-правовий характер: вона є показником незавершеності процесуальної складової кримінально-правової політики у сфері охорони віртуальних активів і прямо обумовлює потребу адаптації процесуального інструментарію до природи нового об'єкта.

Практичний вимір цієї невизначеності рельєфно ілюструють і галузеві дослідники. О. Кузьменко та П. Кравчук, аналізуючи віртуальні активи саме як предмет кримінального правопорушення, зазначають, що в чинному кримінальному законодавстві відсутні норми, які прямо згадували б віртуальні активи або криптовалюту, а тому слідчі та прокурори у провадженнях, пов'язаних із криптовалютами, діють фактично на власний розсуд, ухвалюючи процесуальні рішення, здійснюючи вилучення цифрових активів та організовуючи їх зберігання без чітко визначеного правового механізму, через

що питання подальшої правової долі вилучених криптоактивів залишається неврегульованим і вирішується ситуативно [194, с. 197]. Водночас ці автори обґрунтовано констатують, що за своєю правовою природою віртуальні активи можуть бути предметом багатьох кримінальних правопорушень - шахрайства, крадіжки, вимагання чи незаконного збагачення, - а основні труднощі доказування полягають у недостатньому законодавчому врегулюванні питань їх вилучення, зберігання та конфіскації, а також у необхідності встановлення власника активу, верифікації цифрових слідів у блокчейні, фіксації та збереження доказів і забезпечення допустимості інформації, отриманої з відкритих джерел чи закордонних платформ [194, с. 195, 197-198]. Прикметно, що ці автори, спираючись на висновки інших науковців, пов'язують перспективу подолання зазначених труднощів із виробленням уніфікованої термінології у сфері віртуальних активів відповідно до права ЄС та з набуттям чинності профільним законом, що узгоджується із загальною рамкою гармонізації національного регулювання з MiCA [2]; при цьому, відповідно до інтегративної настанови цього дослідження, згадуваний у цитованих працях Закон України «Про віртуальні активи» [1] послідовно тлумачиться як прийнятий, але такий, що не набрав чинності, а де-юре статус активу - за чинним функціональним визначенням [12].

Подолання процесуальної невизначеності потребує насамперед чіткого визначення того, чим саме є віртуальний актив у системі джерел доказів. Доктринальний висновок О. Старенького, до якого приєднується це дослідження, полягає в тому, що віртуальний актив не є речовим доказом у розумінні статті 98 Кримінального процесуального кодексу України [144], оскільки визначальною ознакою речового доказу є його матеріальна природа, тоді як віртуальний актив становить нематеріальне благо, що не локалізується в матеріальному об'єкті [193, с. 262-264]. Поширена практика визнання віртуальних активів речовими доказами «для збереження» помилково змішує майнову природу активу та можливість накладення на нього арешту з його доказовою природою, хоча накладення арешту на майно й речові докази є різними процесуальними інститутами [193, с. 264]. Так само віртуальний актив

не утворює й самостійного виду «електронних (цифрових) доказів», адже цифрова форма характеризує спосіб існування доказової інформації, а не її сутність, унаслідок чого коректніше вести мову про електронну (цифрову) форму доказу, а не про окремий його вид [193, с. 265-266]. Звідси випливає несучий для доказування висновок: доказове значення має не сам віртуальний актив, а належно зафіксована цифрова інформація про нього, відображена у протоколі слідчої (розшукової) дії, який і є самостійним процесуальним джерелом доказів, тоді як матеріальні носії - пристрої, апаратні гаманці, скріншоти, відеозаписи - долучаються як додатки без самостійного доказового значення [193, с. 265-267]. Таке тлумачення має пряме політико-правове значення: воно зміщує акцент із марних спроб «упредметнити» актив на забезпечення процесуальної форми його фіксації, що водночас уможливорює і доказування, і подальше вилучення та конфіскацію.

Із цього погляду набуває визначеності й питання про способи отримання відомостей про віртуальні активи у процесі провадження. За відсутності спеціальних норм віртуальні активи виявляються та вилучаються під час обшуку житла чи іншого володіння особи й під час огляду електронних носіїв інформації, мобільних телефонів і комп'ютерної техніки [193, с. 257]. При цьому розрізняють безпосередній механізм - фіксацію цифрових параметрів активу, як-от адреси, балансу та історії транзакцій через відкриті оглядачі блокчейну, із зазначенням ідентифікатора транзакції, відмітки часу та висоти блоку, - та опосередкований механізм, що полягає у встановленні контролю над засобами доступу до активу, тобто над приватними ключами, відновлювальними фразами та обліковими записами [193, с. 257-259]. Власне «вилучення» віртуального активу за такого підходу є не фізичним заволодінням, а ініціюванням транзакції на контрольований службовий гаманець органу досудового розслідування з документуванням технічних параметрів операції [193, с. 259-260]. Логічним завершенням цієї конструкції є запропонована система критеріїв допустимості відомостей про віртуальні активи, відповідно до якої допустимість визначається не цифровою природою інформації, а дотриманням процесуальної форми її отримання - здобуттям

уповноваженим суб'єктом у межах повноважень, належною фіксацією способу й джерела походження, забезпеченням цілісності та незмінності даних, можливістю незалежної технічної верифікації через відкриті оглядачі блокчейну, повнотою фіксації технічних параметрів та дотриманням процедури документування технічних дій із залученням спеціаліста [193, с. 267-268].

Прикладну деталізацію доказової бази, узгоджену з наведеними доктринальними засадами, пропонує методично-прикладний посібник М. Громека, підготовлений у межах діяльності Організації з безпеки і співробітництва в Європі; це джерело подається як авторський звіт кращих практик для правоохоронних органів, а не як офіційна позиція організації чи виклад чинного процесуального права України, тож його положення використовуються як порівняльно-стандартизаційний орієнтир. Посібник спростовує поширений міф про невловність криптоактивів, наголошуючи, що транзакції піддаються відстеженню, а точна фіксація даних «на вході» є передумовою поєднання цифрових і матеріальних доказів [195, с. 9]. Серед першочергових для фіксації відомостей виокремлено час операції, задіяну фінансову установу чи брокера, розмір транзакції та тип криптовалюти, а також підкреслено незворотність транзакцій після внесення до блокчейну, що визначає тактику дій і часову чутливість розслідування [195, с. 22]. Принципово важливими для доказування є застереження щодо достовірності та допустимості окремих категорій даних. Так, надійність мережевих адрес є сумнівною з огляду на спільне використання адрес, маскування з'єднання та неточність атрибуції, унаслідок чого мережева адреса сама по собі не ідентифікує користувача й може використовуватися лише в сукупності з іншими доказами [195, с. 31-32]; копії ідентифікаційних документів, отримані від постачальників послуг, уразливі до підробки, що зумовлює потребу окремої оцінки достовірності отриманих ідентифікаційних відомостей [195, с. 30, 34]; нарешті, дані аналітики блокчейну та відомості з відкритих джерел належить сприймати з обачністю й перевіряти перед формулюванням висновків [195, с. 48]. Ці застереження прямо корелюють із критерієм незалежної технічної верифікації, обґрунтованим у вітчизняній доктрині [193, с. 267-268], і разом

утворюють систему доказових стандартів вузла. Водночас посібник наочно демонструє наскрізну тезу підрозділу: обсяг відомостей, які централізований постачальник послуг надає за запитом правоохоронного органу, - ім'я, дата народження, копії документів, розмір і час транзакцій, хеші транзакцій та адреси гаманців - є можливим саме тому, що такі постачальники включені до периметра протидії відмиванню коштів і фінансуванню тероризму та зобов'язані виконувати відповідні обов'язки [195, с. 9, 29-30].

Найбільш чутливою для доказування є проблема доведення права власності на віртуальний актив та ідентифікації його власника. Тут особливу цінність має узагальнення національної практики, наведене в науково-методичних рекомендаціях для суддів, підготовлених Національною школою суддів України; це інституційне видання використовується як методично-практична позиція укладачів та узагальнення практики, тоді як правові позиції підкріплюються першоджерелами. Вихідною є теза про те, що попри псевдоанонімність публічний характер блокчейну залишає простежуваний «грошовий слід», унаслідок чого правоохоронні органи проводять криміналістичні дослідження блокчейну для відстеження потоків активів [196, § 1, с. 5-6]. Ключовим практичним стандартом доведення, що сформувався в національній судовій практиці, є використання публічної адреси (відкритого ключа) як унікального ідентифікатора належного особі активу: така адреса може бути оприлюднена без ризику для збереження активу, оскільки лише відображає його обсяг, не надаючи доступу до нього [196, § 6, с. 40-41, 44]. На цій підставі ненадання ідентифікатора гаманця під час перевірки як підтвердження факту набуття активу у власність розцінюється як декларування недостовірних відомостей, причому, за висновком судової експертизи, для дійсного власника втрата публічного ключа не є перешкодою для його відновлення, а тому відмова надати адресу з посиланням на «втрату» не може вважатися виправданою [196, § 6, с. 44-45]. Це узагальнення безпосередньо змикається з обґрунтованим у доктрині техніко-криптографічним підтвердженням володіння активом - через доступ до гаманця, ключі та зв'язок особи з публічною адресою [193, с. 253-254] - і набуває виразного політико-

правового змісту: за відсутності спеціального процесуального закону саме судова практика виробила робочий стандарт доведення належності віртуального активу.

Доведення обставин у цій сфері істотно спирається й на нормативну рамку Європейського Союзу, яка водночас є джерелом верифікованих доказів і орієнтиром гармонізації. Відповідно до Регламенту (ЄС) 2023/1113 [92] перекази віртуальних активів супроводжуються повною інформацією про ініціатора й одержувача, а постачальник послуг перевіряє правильність такої інформації на основі надійного незалежного джерела перед переказом і за наявності ознак недостовірності чи підозрілості повідомляє про це підрозділ фінансової розвідки відповідно до п'ятої директиви [46]; передбачене зберігання інформації протягом тривалого строку забезпечує доступ до доказів через місяці й навіть роки після здійснення операції [196, § 4, с. 24-27]. Набуття чинності Регламентом MiCA [2] формалізувало реєстрацію постачальників послуг у межах Європейського економічного простору, водночас значна частина обмінних операцій і досі здійснюється в третіх юрисдикціях, що окреслює об'єктивні межі доступності доказів [196, § 1, с. 7]. Емпіричним підтвердженням реалістичності доведення слугують вітчизняні кейси антикорупційних органів: задокументовані випадки одержання неправомірної вигоди у криптовалюті з подальшим переведенням у готівку через посередника, кваліфіковані за відповідними частинами статей 368 і 369 Кримінального кодексу України [64], причому щодо посередника було укладено угоду про визнання винуватості - обставина, що утворює змістовий місток до вузла угод [196, § 5, с. 35-36].

Перехід до вивчення проблем досудового розслідування доцільно розпочати з оцінки стану наукової розробленості проблеми, оскільки саме діагностований дефіцит криміналістичних напрацювань є одним із показників незавершеності розслідувальної складової кримінально-правової політики у досліджуваній сфері. Як зазначає В. Саєнко, попри те що перші ґрунтовні вітчизняні дослідження проблематики розпочалися ще близько десяти років тому, поза увагою науковців або висвітленими лише поверхово залишаються

питання сутності злочинної діяльності з віртуальними активами, віртуального активу як складової криміналістичної характеристики, обставин, що підлягають установленню, типових слідчих ситуацій і тактичних завдань, організації й тактики окремих слідчих (розшукових) дій, а також залучення спеціальних знань та експертиз [197, с. 280-281, 290]. Цю діагностику доповнює запропонована К. Мартиненком періодизація наукового дослідження, у межах якої виокремлено підготовчий етап, коли криміналістика ще не розглядала віртуальні активи як самостійний об'єкт, етап появи перших комплексних праць про правову природу блокчейну та доказування у відповідних провадженнях і сучасний прикладний етап, що супроводжується інституціоналізацією відносин на нормативному рівні [198, с. 140-143]. Особливе значення для системного розуміння предмета має обґрунтована цим автором комплексна криміналістична сутність віртуального активу, який одночасно може виступати засобом учинення правопорушення, його предметом, джерелом доказової інформації у вигляді сукупності цифрових слідів та наслідком злочинної діяльності, тобто активом, що підлягає встановленню, арешту й можливій спеціальній конфіскації [198, с. 142]. Ця чотиривимірна модель прямо змикається з доктриною доказування, оскільки роль активу як джерела доказової інформації потребує його фіксації, збереження та аналітичної обробки, а роль активу як наслідку утворює місток до питань арешту й конфіскації, що становлять предмет окремих підрозділів. Підсумовуючи, К. Мартиненко обґрунтовано наголошує на потребі цілісної криміналістичної концепції організації розслідування, що поєднувала б класичні підходи з цифровими інструментами та міждисциплінарними методами [198, с. 144-145].

Організаційно-інституційний вимір розслідування передбачає налагоджену взаємодію суб'єктів виявлення й розслідування. Т. Яцик і В. Шкелебей обґрунтовано наголошують, що в умовах збройної агресії проти України протидія обігу активів, одержаних злочинним шляхом і здатних фінансувати збройні угруповання, набуває політико-безпекового пріоритету, а ефективне розслідування потребує взаємодії правоохоронних органів із

Державною службою фінансового моніторингу України, Національним агентством України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, і Державною податковою службою України [199, с. 220, 222]. Автори виокремлюють форми співпраці правоохоронних органів із підрозділом фінансової розвідки - отримання узагальнених матеріалів, інформування про підозрілі операції та надання типологій таких операцій, - а також визначають ключові аспекти, що мають враховуватися під час розслідування: специфіку самих активів, особливості їх функціонування й обігу та технічні характеристики кіберпростору [199, с. 222]. Хоча виклад у цьому джерелі є переважно оглядово-описовим і використовується як опора на інституційну рамку, він має самостійну цінність, оскільки фіксує систему суб'єктів, через взаємодію яких політика охорони віртуальних активів реалізується у процесуальній площині, та виводить на роль Національного агентства з питань виявлення, розшуку та управління активами як інституції, що поєднує розслідування з подальшим розшуком і управлінням активами.

Технологічним ядром розслідування є аналіз руху віртуальних активів. В. Школьніков пропонує класифікацію етапів обробки й аналізу руху активів під час досудового розслідування, що охоплює отримання ідентифікатора транзакції чи адреси гаманця, визначення виду активу, вибір оглядача блокчейну або спеціалізованого програмного забезпечення, аналіз гаманця з вирішенням питання про доцільність подальшого відстеження та про спрямування запиту до сервісу обміну, встановлення сервісу-власника гаманця й надсилання запиту на розкриття даних про користувача, а також аналіз отриманих відповідей [200, с. 421-422]. Аналіз відповідей сервісу обміну дає змогу встановити персональні дані особи, відомості про використані пристрої, загальні суми отриманих і витрачених коштів та зв'язки користувача, а слідування за «цифровим слідом» - за адресами гаманців і супутніми даними на кшталт мережеских адрес входу, електронної пошти та прив'язаних номерів телефону - спрямоване на встановлення особи правопорушника й повернення викраденого активу законному власникові [200, с. 422]. Серед практичних

проблем обробки відповідей сервісів обміну автор слушно виокремлює неструктурований вигляд і значні обсяги даних, а також потребу конвертації віртуального активу у гривневий еквівалент за курсом на день транзакції - питання, що безпосередньо проєктується на визначення розміру шкоди й вартості активу для цілей кваліфікації та доказування [200, с. 422]. Інституційно-процесуальним підґрунтям цієї діяльності є створене в структурі кіберполіції управління протидії злочинам, пов'язаним з віртуальними активами, працівники якого проводять слідчі та негласні слідчі (розшукові) дії за дорученням слідчого, дізнавача чи прокурора [200, с. 419]. Згадувані в цьому джерелі та в практиці аналітики інструменти й програмні рішення наводяться нейтрально та ілюстративно, без оцінки їхніх переваг.

Окремої уваги заслуговує нормативний інструмент, що інституціоналізує розшукову складову в кожному «майновому» провадженні. Спільним наказом Офісу Генерального прокурора, Міністерства внутрішніх справ України, Служби безпеки України, Державного бюро розслідувань, Національного антикорупційного бюро України та Бюро економічної безпеки України від 28 жовтня 2024 року № 254/724/520/401/177/185 затверджено Порядок організації та забезпечення досудового розслідування злочинів, у результаті вчинення яких одержано майно (доходи) [201], відповідно до якого слідчий у кожному такому провадженні забезпечує визначення обсягу майна (доходів), одержаного злочинним шляхом, та його розшук [200, с. 420]. Цей акт має самостійне політико-правове значення: він переводить установку на розшук злочинних активів - а отже, і віртуальних активів як їх різновиду - із площини доктринальних рекомендацій у площину обов'язкового організаційного стандарту досудового розслідування, утворюючи місток до вузла арешту, управління та конфіскації активів і до ролі профільного агентства з управління активами.

Оперативно-розшуковий шар розслідування характеризується власною специфікою. А. Крижановський обґрунтовано виходить із того, що цифровізація фінансових потоків знижує застосовність традиційних методів і потребує нових алгоритмів оперативно-розшукової діяльності, а середовище

віртуальних активів завдяки прозорості блокчейну, незмінності транзакцій і псевдоанонімності водночас утворює стійкі цифрові сліди, які за коректної інтерпретації стають основою для встановлення причинно-наслідкових зв'язків та ідентифікації суб'єктів [202, с. 305-306]. Принципове значення має запропонована автором класифікація правопорушень за роллю активу, що розмежовує діяння, спрямовані на віртуальний актив як безпосередній предмет посягання, і діяння, у яких актив є інструментом реалізації протиправних цілей, адже від цієї категорії залежать тактика й джерела оперативної інформації [202, с. 306, 310]. Така класифікація узгоджується з чотиривимірною криміналістичною сутністю активу й безпосередньо проєктується на питання визначення предмета й засобу правопорушення. Серед джерел відомостей автор виокремлює опитування й наведення довідок із надсиланням запитів до бірж та обмінників для встановлення власників гаманців, до постачальників послуг доступу до мережі - для отримання технічних даних, а також до банків - для відстеження виведення активів у фіатні кошти [202, с. 307-308], а також дослідження предметів і документів та використання інструментів розвідки на основі відкритих джерел [202, с. 308-309]. Прикметно, що значна частина цих джерел знову виводить на залежність розслідування від доступу до постачальників послуг, бірж та обмінників, тобто від їх включення до регуляторного периметра, а порівняльним орієнтиром удосконалення оперативної роботи автор називає підхід «контролю на старті», за якого операції виявляються до їх внесення у блокчейн; цей підхід подається узагальнено, як ілюстрація європейського вектора, без приписування конкретній юрисдикції [202, с. 310]. Опис інструментарію розвідки на основі відкритих джерел та засобів обфускації походження коштів наводиться лише на рівні констатації проблеми для розслідування, без операційної деталізації способів деанонімізації чи ухилення.

Доволі гострим також є питання негласних заходів і пов'язаних із ними законодавчих прогалин. А. Ковальський, чия праця використовується насамперед для постановки проблеми та структурного переліку прогалин і особливостей, а не як джерело завершених доктринальних висновків,

систематизує дві принципові вади чинного регулювання. По-перше, стаття 6 Закону України «Про оперативно-розшукову діяльність» [204] не передбачає як підстави проведення оперативно-розшукової діяльності завдання розкриття вже вчинених правопорушень - установлення осіб, які їх учинили, та розшуку грошей, цінностей та іншого майна, одержаного злочинним шляхом, - що особливо відчутно за наявності віртуальних активів [203, с. 448]. По-друге, у Кримінальному процесуальному кодексі України [144] відсутній чіткий механізм використання засобів оперативно-розшукової діяльності під час досудового розслідування, а доручення слідчого на проведення негласних слідчих (розшукових) дій за статтею 40 кодексу не охоплює використання таких засобів, як спеціальні програмні рішення для виявлення й розшуку активів, унаслідок чого залучення не передбачених кодексом способів загрожує визнанням доказів недопустимими [203, с. 448-449]. Автор виокремлює й низку особливостей розшуку та виявлення віртуальних активів - технологічну складність, юридичні обмеження, міжнародний характер, труднощі ідентифікації суб'єктів та динамічність середовища, - а також констатує, що традиційні негласні слідчі (розшукові) дії, передбачені статтями 263 і 264 кодексу, виявляються малоефективними з огляду на технічну специфіку активів і децентралізований характер відповідних систем [203, с. 449]. Висновок про потребу вдосконалення законодавчої бази в частині засобів оперативно-розшукової діяльності та розширення підстав їх застосування для розкриття вчинених правопорушень [203, с. 449] прямо змикається з тезою про прогалину в кримінальному процесуальному законі [193, с. 255-256] та з критерієм здобуття доказів уповноваженим суб'єктом у межах повноважень [193, с. 267-268] і утворює один із найвагоміших аргументів *de lege ferenda* цього підрозділу.

Транскордонний характер обігу віртуальних активів закономірно виводить розслідування на рівень міжнародного співробітництва, що становить невід'ємну складову процесуальної реалізації політики охорони. Згадуваний посібник Організації з безпеки і співробітництва в Європі описує наявні канали взаємодії - від платформи для експертів та профільних структур Європолу до

спеціалізованого центру Інтерполу з протидії фінансовій злочинності й корупції, - а також механізм Інтерполу швидкого реагування на платежі, що дає змогу за умови своєчасності зупинити переказ до моменту його незворотного внесення у блокчейн [195, с. 22-23, 52-54]. Часова чутливість, на яку наголошує це джерело [195, с. 22], перетворює оперативність міжнародної взаємодії на самостійну вимогу процесуальної політики. Прикметно, що Україна виступає бенефіціаром відповідних міжнародних проєктів, спрямованих на приведення національної рамки обігу віртуальних активів у відповідність до Рекомендацій ФАТФ [77] та на інституційну розбудову правоохоронних органів, а серед національних учасників таких ініціатив - Національний банк України, Державна служба фінансового моніторингу України, Міністерство цифрової трансформації та Національна комісія з цінних паперів та фондового ринку [195, с. 11, 46]. Узагальнені типології злочинного використання віртуальних активів, що формуються в межах діяльності Європолу [161], так само слугують орієнтиром для організації розслідування й підтверджують наскрізну тезу про зв'язок процесуальних можливостей із міжнародними та європейськими стандартами.

Особливості укладення угод у кримінальному провадженні щодо незаконного заволодіння віртуальними активами можуть продемонструвати, як охоронна функція кримінально-правової політики реалізується через консенсуальні процесуальні механізми. А. Мовчан і В. Козій обґрунтовано констатують, що Кримінальний процесуальний кодекс України [144] не передбачає особливостей укладення угод у провадженнях про незаконне заволодіння криптовалютою, через що застосовуються загальні засади та глава 35 кодексу [205, с. 40]. На цьому тлі автори формулюють ключову умову угоди про визнання винуватості у таких провадженнях: згоду підозрюваного чи обвинуваченого на повернення віртуального активу, яким він незаконно заволодів, викриття співучасників і за потреби розкриття способу вчинення правопорушення, зокрема його технічної кіберскладової; без такої умови укладення угоди втрачає сенс [205, с. 40-41]. Угода про примирення, своєю чергою, має чітко визначати, яку кількість і якого саме активу належить

повернути, на які адреси гаманців та в який строк [205, с. 41]. Автори обґрунтовано окреслюють і ситуації, коли укладення угоди недоцільне, - за наявності достатньої доказової бази, у разі вже здобутого доступу до активу через відновлювальні фрази чи паролі або за достовірно відомого способу вчинення [205, с. 41]. Окремої уваги заслуговує запропонований підхід до розпорядження активом після одержання доступу: з огляду на волатильність ринку ризику зберігання й розпорядження переходять на сторону обвинувачення, тому доцільним визнається обмін активу на фіатні кошти з подальшим зарахуванням їх на спеціальні рахунки відповідного органу, а в разі примирення - потерпілому [205, с. 41-42]. Зміст угоди має охоплювати назву активу, кількість у кожній транзакції, за потреби - алгоритм хешування, а також розподіл комісій за транзакції, що перетворює технічну специфіку активу на самостійний предмет процесуальних домовленостей [205, с. 42-43]. Показовим індикатором ефективності політики є наведені авторами результати власного опитування процесуальних керівників, переважна більшість яких визнала угоди в цій категорії проваджень доцільними, погодившись із ключовою умовою про повернення активу, однак жоден з опитаних таких угод на практиці не укладав [205, с. 40-41]; цей розрив між визнаною доцільністю та фактичною незастосовуваністю є самостійним аргументом на користь адаптації глави 35 кодексу до специфіки віртуальних активів. Практичну реалізованість такого механізму підтверджує вже згадуваний кейс антикорупційних органів, у якому щодо посередника було укладено угоду про визнання винуватості [196, § 5, с. 35-36].

Узагальнення проведеного аналізу дає підстави для кількох висновків, що мають наскрізне значення для кримінально-правової політики у сфері забезпечення охорони віртуальних активів. По-перше, процесуальна складова цієї політики залишається незавершеною: єдина згадка віртуальних активів у кримінальному процесуальному законі [144] стосується лише накладення арешту, спеціальні процедури їх виявлення, фіксації та вилучення відсутні [193, с. 255-256], підстави оперативно-розшукової діяльності й механізм використання її засобів не пристосовані до розкриття правопорушень,

пов'язаних з активами [203, с. 448-449], а цілісна криміналістична концепція організації розслідування ще не сформована [198, с. 144-145]. По-друге, попри ці прогалини, доктрина й практика виробили робочі рішення - від визнання належно зафіксованої цифрової інформації у протоколі слідчої (розшукової) дії самостійним джерелом доказів [193, с. 265-267] і системи критеріїв допустимості [193, с. 267-268] до стандарту доведення власності через публічну адресу [196, § 6, с. 44-45] та консенсуального механізму повернення активу через угоди [205, с. 40-43]. По-третє, дієвість усіх цих рішень похідна від регуляторно-політичного вибору включити постачальників послуг, пов'язаних з обігом віртуальних активів, до периметра протидії відмиванню коштів і фінансуванню тероризму відповідно до стандартів ФАТФ [77], директив ЄС [46] та МіСА [2], оскільки саме обов'язки таких постачальників щодо ідентифікації клієнтів і фіксації операцій уможливають і доказування, і розслідування. Звідси впливає головний напрям удосконалення: адаптація Кримінального процесуального кодексу України та Закону України «Про оперативно-розшукову діяльність» до природи віртуального активу із синхронізацією цих змін із завершенням профільної реформи за моделлю МіСА [2] та з гармонізацією національних механізмів зі стандартами ФАТФ [77].

4.2. Арешт, спеціальна конфіскація та звернення стягнення на віртуальні активи; виконання судових рішень щодо їх конфіскації

Кримінально-правова політика також має свій відбиток і на завершальному відрізку кримінального провадження - у площині забезпечувальних, матеріально-правових і виконавчих механізмів, покликаних позбавити правопорушника протиправно набутого активу та повернути викрадене потерпілому або звернути актив у дохід держави. Саме тут охоронна функція кримінального права зазнає найсуворішої перевірки на дієвість: матеріально-правова заборона та процесуальна можливість вилучення активу залишаються неповними, якщо вони не завершуються реальним арештом, законною конфіскацією та її примусовим виконанням.

Чинна модель поводження з віртуальними активами у кримінальному провадженні фактично вичерпується можливістю накладення арешту, тоді як матеріально-правові підстави їх конфіскації та кримінально-виконавчі механізми реалізації залишаються непристосованими до природи нового об'єкта. Така незавершеність ризикує перетворити арешт на самоціль, неспроможну завершитися реальною конфіскацією, унаслідок чого арешт активу набуває рис «перманентного». Єдиною прямою нормативною підставою для поводження з віртуальними активами у кримінальному провадженні є частина десята статті 170 Кримінального процесуального кодексу України [144], яка передбачає можливість накладення на них арешту й зазнала відповідних змін у 2022 році; спеціальних же процедур арешту, конфіскації та реалізації, що враховували б цифрову природу активу, процесуальний і матеріальний закон не містять. Ця прогалина має не суто технічний, а політико-правовий характер, оскільки вона прямо обумовлює потребу синхронної адаптації забезпечувального, матеріального та виконавчого інструментарію кримінально-правової політики до особливостей віртуального активу.

Забезпечувальний вимір цієї проблематики предметно розкривають О. Шайтуро та Г. Рибалко, які обґрунтовано демонструють, що арешт віртуальних активів як захід забезпечення посідає ключове місце у виконанні завдань кримінального провадження, адже такий актив може одночасно виступати предметом, засобом і доходом від кримінального правопорушення, а також предметом подальшої конфіскації [206, с. 335-336]. Водночас автори справедливо наголошують, що у схемах відмивання коштів псевдоанонімність операцій і відсутність централізованого контролю істотно ускладнюють моніторинг руху активу, а право власності на віртуальний актив на технічному рівні підтверджується самим лише володінням ключем доступу до гаманця, тоді як відновлювальна фраза з дванадцяти, вісімнадцяти чи двадцяти чотирьох слів дає змогу відновити доступ до активу незалежно від конкретного пристрою [206, с. 337-338]. Ця технічна особливість має пряме процесуальне значення: вона визначає і предмет забезпечувального заходу, і коло осіб, здатних фактично розпоряджатися активом.

Спираючись на положення глави 17 Кримінального процесуального кодексу України [144], О. Шайтуро та Г. Рибалко пропонують поетапну модель накладення арешту на віртуальні активи, у межах якої підстави для арешту визначаються через наявні докази та об'єкти, що підлягають спеціальній конфіскації, а сама процедура охоплює подання відповідного клопотання згідно зі статтею 171 кодексу та врахування обставин, передбачених частиною другою статті 173, зокрема правової підстави, розумності й співмірності обмеження права власності [206, с. 339-341]. Окремої уваги в їхній конструкції потребує взаємодія з Національним агентством України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, до управління якого можуть передаватися арештовані віртуальні активи на підставі Закону України «Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів» [207]. Прикметно, що навіть у цій моделі чинна процесуальна конструкція щодо віртуальних активів фактично зводиться до арешту як інструмента забезпечення майбутньої конфіскації. Відповідно до інтегративної настанови цього дослідження, де-юре можливість арешту віртуальних активів ґрунтується на частині десятій статті 170 та нормах глави 17 кодексу зі змінами 2022 року, а не на Законі України «Про віртуальні активи» [1], який залишається нечинним; згадки про цей закон у цитованих працях стосуються прийнятого, але не введенного в дію акта.

Поглиблений критичний аналіз забезпечувально-конфіскаційної проблематики пропонують О. Капліна та І. Парфіло, які виокремлюють три ключові проблеми поводження з криптоактивами у кримінальному провадженні: ідентифікацію власника активу, порядок його тимчасового вилучення та арешту, а також можливість конфіскації криптоактиву як виду покарання [208, с. 91-93]. Автори прямо констатують, що Закон України «Про віртуальні активи» так і не набрав чинності, однак на практиці залишається чи не єдиним джерелом, до якого звертаються правозастосовники за відсутності адекватного чинного регулювання, - обставина, що сама по собі засвідчує незавершеність матеріальної складової кримінально-правової політики у цій

сфері [208, с. 92]. Це спостереження прямо узгоджується із застосованою в дослідженні рамкою, за якою згаданий закон послідовно тлумачиться як прийнятий, але такий, що не набрав чинності, а де-юре статус активу визначається чинним функціональним визначенням [12].

Щодо ідентифікації власника О. Капліна та І. Парфило обґрунтовано звертають увагу на те, що за частинами п'ятою і шостою статті 170 Кримінального процесуального кодексу України [144] арешт майна з метою його подальшої конфіскації як виду покарання може бути накладено лише на майно підозрюваного, обвинуваченого або засудженого, на відміну від арешту з метою збереження речових доказів, де визначальною є об'єктивна пов'язаність майна з кримінальним правопорушенням незалежно від його власника [208, с. 94-96]. Модельне правило, запозичене з нечинного Закону України «Про віртуальні активи» [1], визнає власником віртуального активу володільця ключа з окремими винятками для зберігання активу третьою особою; проте, як справедливо зауважують автори, це правило не може слугувати чинною юридичною підставою, а на практиці анонімність розподіленого реєстру й можливість перебування відновлювальної фрази в розпорядженні кількох осіб роблять саме лише виявлення ключа недостатнім для достовірного встановлення власника [208, с. 96-98]. Замість спрощеного ототожнення «власник - володільця ключа» автори обґрунтовано пропонують встановлювати фактичний контроль над активом і реальну можливість розпоряджатися ним, проводячи аналогію з підходами, виробленими для інституту необґрунтованих активів. Для кримінально-правової політики цей висновок має принципове значення: достовірне встановлення належності активу є матеріальною передумовою законності арешту, що накладається з конфіскаційною метою.

Не менш гострою є друга з виокремлених авторами проблем - порядок тимчасового вилучення та арешту віртуальних активів. О. Капліна та І. Парфило слушно вказують, що процесуальний закон не містить спеціального регулювання накладення арешту на активи, що перебувають на конкретних гаманцях, а поширена на практиці модель переведення активів на гаманець правоохоронного органу породжує колізії з вимогою статті 19 Конституції

України [68], згідно з якою органи державної влади діють лише на підставі, у межах повноважень та у спосіб, що передбачені законом, а також із приписами частини другої статті 167 і частини п'ятої статті 237 Кримінального процесуального кодексу України [144], а отже, і ризик визнання отриманих у такий спосіб доказів недопустимими [208, с. 99-102]. За цією логікою вилучення й арешт віртуальних активів технічно можливі двома способами: через блокування активу криптобіржею або емітентом за запитом органу досудового розслідування й через переведення активів на службовий гаманець правоохоронного органу, - однак другий спосіб потребує спеціального процесуального порядку, який ще має бути встановлений законом. Брак такого порядку перетворює технічно здійсненну дію на джерело процесуальних ризиків і знов-таки відсилає до незавершеності процесуальної складової політики охорони віртуальних активів.

Третя проблема, на якій наголошують О. Капліна та І. Парфіло, безпосередньо виводить аналіз на матеріально-правовий і кримінально-виконавчий рівні: чинне законодавство не містить працездатного механізму примусової реалізації рішень про конфіскацію віртуальних активів або звернення стягнення на них [208, с. 102-103]. Без такої процедури арешт віртуальних активів ризикує перетворитися на «перманентний арешт», що суперечить самій природі забезпечувальних заходів, адже за пунктом третім частини третьої статті 132 Кримінального процесуального кодексу України [144] застосування заходів забезпечення не допускається, якщо завдання, для якого слідчий чи прокурор звертається до суду, може бути виконане іншим способом, а захід не здатний це завдання виконати. Заблокований або арештований актив, який неможливо реалізувати, цього завдання не виконує - і цим відкриває перехід до матеріально-правового та кримінально-виконавчого виміру конфіскації, що становить предмет подальшого аналізу.

Матеріально-правовий вимір конфіскації віртуальних активів найбільш повно опрацьовано у дослідженні В. Козія, який послідовно розмежовує наявні в національному праві типи конфіскації та оцінює придатність кожного з них до криптоактивів. Автор виокремлює конфіскацію майна як додаткове покарання,

передбачену статтею 59 Кримінального кодексу України [64], спеціальну конфіскацію за статтями 96-1 та 96-2 цього кодексу в поєднанні із санкціями його Особливої частини, конфіскацію як захід кримінально-правового характеру щодо юридичних осіб, а також, поряд із суто кримінально-правовими інститутами, цивільну конфіскацію за наявності відповідних підстав [209, с. 74-75]. Таке розмежування має не лише класифікаційне, а й політико-правове значення, адже від обраного типу конфіскації залежить і коло активів, що можуть бути звернені в дохід держави, і процедура, у якій це відбувається.

Центральною в аналізі В. Козія є виявлена ним матеріально-правова прогалина. Як зазначає автор, цивільна конфіскація, запроваджена Законом України № 263-IX [180], спирається на процесуальне поняття «активи», яке за пунктом першим частини восьмої статті 290 Цивільного процесуального кодексу України [210] прямо охоплює криптовалюти, унаслідок чого звернути криптовалюту в дохід держави наразі видається можливим переважно саме через механізм цивільної конфіскації [209, с. 75]. Водночас тут постає ключова матеріально-правова колізія: процесуальний закон оперує поняттям «нематеріальні активи, у тому числі криптовалюти», тоді як профільна термінологія послуговується поняттям «віртуальні активи», і жоден чинний акт прямо не ототожнює ці поняття, а Кримінальний кодекс України [64] у статті 59 використовує поняття «майно», до якого віртуальні активи як нематеріальні блага за чинним цивільним законодавством [27] прямо не належать [209, с. 75-77]. Звідси впливає несучий для матеріальної кримінально-правової політики висновок: за чинної конструкції бракує однозначних законних підстав для конфіскації криптовалют як виду покарання у кримінальному судочинстві, що зумовлює потребу доповнити статтю 59 Кримінального кодексу України прямими положеннями про підстави та порядок конфіскації криптовалют, а так само адаптувати до неї норми про спеціальну конфіскацію.

Навіть тоді, коли матеріально-правова підстава для конфіскації існує, її реалізація, як показує В. Козій, натрапляє на перешкоди в кримінально-виконавчому механізмі, не розрахованому на цифрові активи. Відповідно до частини другої статті 48 Кримінально-виконавчого кодексу України [211]

покарання у виді конфіскації майна виконується Державною виконавчою службою в порядку виконавчого провадження, а за статтею 48 Закону України «Про виконавче провадження» [212] звернення стягнення на майно боржника охоплює його арешт, вилучення та примусову реалізацію, технічний порядок якої деталізовано в Порядку реалізації арештованого майна, затвердженому наказом Міністерства юстиції України [213]. Сукупний аналіз цих актів дає В. Козію підстави для висновку про те, що державний виконавець не має ні юридичних підстав, ні технічних можливостей звернути стягнення на криптоактив, через що арештований актив потрапляє у стан фактично безстрокового арешту без реальної перспективи реалізації [209, с. 78-80]. Цей висновок наочно демонструє, що та сама виконавча машинерія, якою реалізується кримінальна конфіскація, виявляється непридатною до віртуальних активів.

Технічна реалізація конфіскованих криптоактивів, як обґрунтовано показує В. Козій, потребує спеціальних процедур, що принципово відрізняються від реалізації матеріального майна, - створення службових гаманців, відновлення доступу через ключі, обміну активу та виведення коштів на державні рахунки, - жодна з яких чинним порядком виконавчого провадження не передбачена [209, с. 80-82]. Як ілюстрацію можливих інституційних рішень автор наводить досвід Сполучених Штатів Америки, де конфісковані цифрові активи реалізуються спеціально уповноваженою службою через поступовий продаж або спеціалізовані аукціони, проте розглядає цей досвід саме як орієнтир, а не як модель для прямого перенесення [209, с. 82-83]. Основна проблема, діагностована автором, полягає в розриві між процесуальною можливістю арешту віртуального активу та матеріально-виконавчою неможливістю його конфіскувати й реалізувати, - і саме цей розрив утворює один із центральних аргументів на користь взаємозв'язку кримінально-правової політики з кримінально-виконавчою.

Виконавчо-реалізаційний вимір проблеми, але вже крізь призму звернення стягнення у виконавчому провадженні, докладно розглядає О. Гайдучок, виявляючи колізію між визнанням віртуальних активів об'єктом

цивільних прав і потенційним об'єктом стягнення, з одного боку, та практичною відсутністю процедур їх ідентифікації, арешту, оцінки й реалізації - з іншого [214, с. 336-337]. Для оцінки масштабу проблеми автор наводить контекст поширеності криптоактивів в Україні: за відповідними індексами держава стабільно потрапляє до першої десятки глобального рейтингу використання криптоактивів, значна частина населення володіє такими активами, а на державному рівні вони використовувалися навіть для збору коштів на потреби оборони, хоча конкретні статистичні показники різняться залежно від джерела [214, с. 338]. Ця поширеність надає проблемі звернення стягнення на віртуальні активи самотійного суспільного значення й підсилює потребу в адекватному виконавчому інструментарії.

Аналізуючи чинний інструментарій, О. Гайдучок слушно зауважує, що Закон України «Про виконавче провадження» [212] дає стягувачеві право зазначити відомості про електронний гаманець боржника, однак це поняття охоплює також банківські облікові записи, а тому норма не має практичного впливу на можливість арешту чи стягнення віртуальних активів, що перебувають на криптобіржах, унаслідок чого чітко регламентованого механізму звернення стягнення саме на віртуальні активи в Україні досі немає [214, с. 339]. За таких умов фактично єдиним доступним інструментом залишається блокування активу, що здійснюється самими біржами в межах їхніх внутрішніх процедур моніторингу та ідентифікації клієнта на виконання рішень регуляторів або суду; проте, як наголошує авторка, таке блокування не забезпечує передачі активу стягувачеві й реального звернення його в дохід держави в разі конфіскації [214, с. 339]. Як орієнтир для подолання цієї прогалини О. Гайдучок звертається до Глобального кодексу цифрового виконання [215], розробленого Міжнародним союзом судових виконавців, що формулює універсальні принципи цифрового примусового виконання, зокрема потребу створити умови для арешту віртуальних активів судовими виконавцями, передбачити реєстр криптоактивів або обов'язкове їх декларування за відсутності такого реєстру та забезпечити доступ виконавців до систем, де зберігається інформація про криптоактиви.

Окремий зріз тієї самої проблеми - реалізація віртуальних активів у процедурах банкрутства, що також безпосередньо змикається з виконанням рішень про звернення стягнення. О. Гайдучок звертає увагу на те, що Кодекс України з процедур банкрутства [216] не містить механізмів реалізації віртуальних активів, унаслідок чого ці активи фактично випадають із сфери дії процедур, призначених для задоволення вимог кредиторів [214, с. 339]. Цю проблематику предметно опрацьовують А. Ткаченко та О. Пожуєв, які досліджують механізм звернення стягнення на віртуальні активи боржника в разі оголошення його банкрутом і обґрунтовують потребу в окремій процедурі оцінки таких активів, що враховувала б їхню високу волатильність [217, с. 279-282]. Питання оцінки має пряме кримінально-правове значення, оскільки саме від достовірного визначення вартості активу на відповідний момент залежать і розмір конфіскації, і обсяг відшкодування завданої кримінальним правопорушенням шкоди.

Дослідження О. Гайдучок містить і запобіжно-кримінологічний зріз, дотичний до кримінально-правової політики: відсутність належного регулювання обігу віртуальних активів створює сприятливі передумови для шахрайських схем, замаскованих під фінансові послуги з криптоактивами [214, с. 340]. Цей зріз утворює змістовий місток до проблематики Розділу 3 цього дослідження, присвяченого окремим складам кримінальних правопорушень, зокрема шахрайству за статтею 190 Кримінального кодексу України [64], а в межах цього підрозділу згадується стримано - лише як свідчення криміногенності нерегульованого обігу, без переказу фактичних обставин конкретних епізодів. Водночас, відповідно до настанови щодо інтегративного використання джерел, окремі датування й формулювання цитованої праці стосовно профільного закону тут не відтворюються; правовий статус активу послідовно прив'язується до чинного функціонального визначення [12], а реформаторська перспектива - до моделі MiCA [2] та відповідного законопроекту [106].

Технічний канал реалізації віртуальних активів, що має визначальне значення для кримінально-виконавчого аспекту, розкриває С. Грицай,

аналізуючи порядок реалізації віртуальних активів в Україні. Запропонована автором конструкція передбачає, що реалізація віртуального активу в правовому полі відбувається не безпосередньо, а через уповноваженого посередника - постачальника відповідних послуг - шляхом прямого продажу або обміну на інші активи чи на гривню [218, с. 18-20]. Сам автор наголошує, що впровадження цієї моделі залежить від унесення змін до податкового законодавства та створення відповідного державного реєстру, що вкотре підтверджує наявний розрив між формальним і фактичним правовим статусом активу; з огляду на це й відповідно до інтегративної настанови описана конструкція тлумачиться як модельна, побудована на положеннях нечинного Закону України «Про віртуальні активи» [1], а не як виклад чинного права [218, с. 20-22]. Попри модельний характер, для кримінально-правової політики ця конструкція має точкове, але принципове значення: якщо будь-яка легальна реалізація віртуального активу передбачає посередництво уповноваженого суб'єкта, то й реалізація конфіскованого державою активу мусить здійснюватися через біржу чи обмінник, а не напряду. Тим самим конкретизується технічний механізм виконання конфіскації й пояснюється, чому конфіскація віртуальних активів залишатиметься без легального каналу реалізації до запуску інфраструктури постачальників послуг та їхнього авторизаційного режиму, прив'язаного до завершення профільної реформи за моделлю MiCA [2] на основі відповідного законопроекту [106].

Найповніший порівняльно-правовий аналіз порядку звернення стягнення на віртуальні активи у примусовому виконанні судових рішень пропонує І. Гринь, чиє дослідження водночас підтверджує де-юре анкер усієї конструкції. Авторка констатує, що, попри ухвалення профільного закону, останній так і не набрав чинності через відсутність податкових змін, а тому чинне визначення віртуального активу залишається функціональним за антилегалізаційним законом [12], при цьому Україна посідає одне з провідних місць у глобальному індексі впровадження криптовалют [219, с. 193-194]. Особливе значення для теми має зафіксована авторкою позиція фінансових регуляторів: вони не визнають криптовалют ні законним платіжним засобом, ні електронними

грошима, ні цінними паперами, а Національний банк України кваліфікує їх як цифрові речі в розумінні статті 179-1 Цивільного кодексу України [27], що не є платіжним засобом, валютою чи грошовим сурогатом [219, с. 194-195]. Ця кваліфікація, наведена за викладом І. Гринь, повністю узгоджується із застосованою в дослідженні рамкою й додатково посилює тезу про зазор між де-факто поширеністю та де-юре статусом віртуальних активів.

Систематизований каталог викликів, що постають під час звернення стягнення на віртуальні активи, наводять С. Щербак та Д. Репін, на яких спирається у своєму аналізі І. Гринь. До таких викликів належать відсутність гарантованого доступу до активів і ключів, складність доведення належності активу конкретній особі, неможливість централізованого зупинення операцій і примусового списання, проблема холодних гаманців, що перебувають поза сферою досяжності, та потреба конвертації активу у грошовий еквівалент [220, с. 403-405; 219, с. 195]. Принципово важливо, що ці самі бар'єри - доступ до ключів, доведення належності та неможливість примусової реалізації - однаково паралізують і цивільне звернення стягнення, і кримінально-виконавчу реалізацію конфіскованих криптоактивів, унаслідок чого проблеми, описані в контексті виконавчого провадження, виявляються тотожними тим, на які вже вказували О. Капліна та І. Парфило [208] і В. Козій [209] стосовно кримінальної конфіскації. Ця тотожність підтверджує, що йдеться не про розрізнені галузеві труднощі, а про єдину системну прогалину, яка наскрізно зачіпає матеріальну, процесуальну та виконавчу складові політики охорони віртуальних активів.

Порівняльно-правовий матеріал, наведений І. Гринь, дає змогу окреслити можливі орієнтири для вдосконалення національного порядку звернення стягнення, водночас наочно засвідчуючи відсутність єдиного підходу. Регуляторні рамки на кшталт MiCA [2] упорядковують діяльність постачальників послуг і забезпечують інформування про власників активів, проте самі собою не запроваджують механізму автоматичного звернення стягнення [219, с. 196]. Естонія, що ще з 2017 року має легальне визначення віртуальної валюти й легалізований обмін на фіат, демонструє підхід, за якого віртуальний актив може бути лише арештований як еквівалент фіатних коштів,

тоді як його безпосереднє списання та перерахування стягувачеві залишаються неможливими через брак відповідного механізму; Франція, за наведеним авторкою рішенням комерційного суду, звертає стягнення на криптоактиви в порядку арешту грошових вимог до третьої особи - біржі, але лише за умови, що така біржа зареєстрована в національній юрисдикції; подібним шляхом - через стягнення як на кошти чи вимоги, що перебувають у третіх осіб, - рухається й Федеративна Республіка Німеччина, водночас проблема холодних гаманців залишається неврегульованою в усіх розглянутих правопорядках [219, с. 196-198]. Цей порівняльний зріз використовується тут вузько - на механіці виконання та стягнення, без переходу до регуляторних моделей як таких, - і подається через вторинні джерела, що цитуються авторкою, тоді як самі зарубіжні акти та судові рішення до списку джерел не вносяться, оскільки прямо не цитуються.

Ключовою для кримінально-правової політики є експліцитна теза І. Гринь про те, що недостатність механізмів примусового виконання щодо віртуальних активів створює можливості для ухилення від виконання судових рішень, зокрема рішень про конфіскацію майна та відшкодування завданої кримінальним правопорушенням шкоди [219, с. 198]. У такому формулюванні виконавча прогалина перестає бути суто процедурною вадою й перетворюється на самостійний криміногенний чинник: можливість заховати активи від звернення стягнення знижує невідворотність майнових наслідків правопорушення та підриває превентивний потенціал кримінального закону. Саме тому вдосконалення виконавчого порядку щодо віртуальних активів обґрунтовано розглядається як невід'ємна частина кримінально-правової політики у сфері їх охорони, а не як периферійне питання виконавчого провадження.

Узагальнення проведеного аналізу дає підстави для кількох взаємопов'язаних висновків, що окреслюють дотичні точки досліджуваної проблематики до кримінально-правової політики. По-перше, чинна модель поведінки з віртуальними активами у кримінальному провадженні фактично обмежується можливістю накладення арешту за частиною десятою статті 170

Кримінального процесуального кодексу України [144], тоді як процедура арешту спирається на загальні норми глави 17, не пристосовані до цифрової природи активу. По-друге, законність конфіскації прямо залежить від достовірного встановлення належності активу, однак анонімність технології розподіленого реєстру та модельне правило «власник - володілець ключа» ускладнюють ідентифікацію власника, що зумовлює потребу переходу до підходу, заснованого на встановленні фактичного контролю над активом. По-третє, на матеріально-правовому рівні бракує однозначних підстав для конфіскації віртуальних активів як виду покарання, оскільки вони не охоплюються поняттям «майно» в розумінні статті 59 Кримінального кодексу України [64], а звернення їх у дохід держави наразі можливе переважно через цивільну конфіскацію [180] із опорою на поняття «активи» за статтею 290 Цивільного процесуального кодексу України [210]. По-четверте, навіть за наявності підстави реалізація конфіскації блокується кримінально-виконавчим механізмом, оскільки Державна виконавча служба не має ні правових підстав, ні технічних можливостей звернути стягнення на криптоактив, через що арешт ризикує набути «перманентного» характеру всупереч пункту третьому частини третьої статті 132 цього кодексу. По-п'яте, віртуальні активи дедалі активніше використовуються для ухилення від виконання судових рішень, зокрема про конфіскацію та відшкодування шкоди, що перетворює виявлену прогалину на самостійний криміногенний чинник.

Із наведеного випливає, що основним напрямом удосконалення є синхронна адаптація матеріального, процесуального та кримінально-виконавчого законодавства до природи віртуальних активів - із запровадженням дієвої та технічно реалізовної процедури їх ідентифікації, арешту, оцінки, конфіскації й реалізації через авторизованих посередників, що відповідає й модельній конструкції реалізації через постачальників послуг [218], і логіці виконання конфіскації державою. Така адаптація має відбуватися паралельно з профільною реформою за моделлю Регламенту (ЄС) 2023/1114 (MiCA) [2] на основі відповідного законопроєкту [106] та в гармонії зі стандартами Групи з розробки фінансових заходів боротьби з відмиванням

грошей [77], що забезпечують ідентифікацію учасників операцій і простежуваність руху активів. Проведений у цьому підрозділі аналіз засвідчує, що ефективність охоронної функції кримінального права у сфері віртуальних активів визначається не окремо взятою матеріальною заборонаю, а узгодженістю матеріальної, процесуальної та виконавчої складових.

Висновки до розділу 4

Проведене в розділі дослідження взаємозв'язку кримінально-правової політики у сфері забезпечення охорони віртуальних активів із кримінальною процесуальною та кримінально-виконавчою політикою дозволяє сформулювати такі висновки.

1. Дієвість матеріальної кримінально-правової політики перевіряється у площині кримінального провадження: заборона, не забезпечена адекватними процесуальними та виконавчими інструментами виявлення, фіксації, доказування й конфіскації активу, залишається декларативною. Наскрізним є дуалізм статусу віртуального активу - чинний функціональний за Законом № 361-IX і нечинна цивілістична модель Закону № 2074-IX, - який безпосередньо переноситься у процесуальну та виконавчу площини.

2. У системі джерел доказів віртуальний актив не є речовим доказом у розумінні статті 98 Кримінального процесуального кодексу України з огляду на його нематеріальну природу і не утворює окремого виду «електронних доказів»; доказове значення має належно зафіксована у протоколі слідчої (розшукової) дії цифрова інформація про актив, тоді як матеріальні носії долучаються як додатки. Обґрунтовано систему критеріїв допустимості таких відомостей, а національна судова практика виробила стандарт доведення належності активу через публічну адресу (відкритий ключ).

3. За відсутності спеціальних норм віртуальні активи виявляються під час обшуку й огляду електронних носіїв; розрізняють безпосередній механізм - фіксацію параметрів активу через відкриті оглядачі блокчейну - і опосередкований, що полягає у встановленні контролю над засобами доступу (приватними ключами, відновлювальними фразами). Власне «вилучення»

активу є не фізичним заволодінням, а ініціюванням транзакції на контрольований службовий гаманець органу з документуванням її технічних параметрів.

4. Досудове розслідування характеризується дефіцитом криміналістичних напрацювань і відсутністю цілісної концепції організації розслідування; обґрунтовано чотиривимірну криміналістичну сутність активу, який одночасно може бути засобом учинення правопорушення, його предметом, джерелом доказової інформації та наслідком злочинної діяльності. Розслідування спирається на інституційну взаємодію правоохоронних органів із Державною службою фінансового моніторингу, профільним агентством з управління активами та податковою службою і на спеціалізований підрозділ кіберполіції, а нормативним стандартом розшуку майна в кожному «майновому» провадженні став відповідний міжвідомчий Порядок 2024 року.

5. У сфері оперативно-розшукової діяльності та негласних заходів виявлено дві принципові вади: стаття 6 Закону України «Про оперативно-розшукову діяльність» не передбачає як підстави завдання розкриття вже вчинених правопорушень і розшуку одержаного злочинним шляхом майна, а Кримінальний процесуальний кодекс України не містить чіткого механізму використання засобів оперативно-розшукової діяльності під час розслідування. Унаслідок цього традиційні негласні слідчі (розшукові) дії виявляються малоефективними, а залучення непередбачених кодексом засобів загрожує недопустимістю доказів, що утворює вагомий аргумент *de lege ferenda*.

6. Кримінальний процесуальний кодекс України не передбачає особливостей укладення угод у провадженнях про незаконне заволодіння віртуальними активами; ключовою умовою такої угоди має бути згода на повернення активу із зазначенням його кількості, адрес гаманців і строку, викриття співучасників і за потреби розкриття технічного способу, а з огляду на волатильність - обмін активу на фіатні кошти з переходом ризиків на сторону обвинувачення. Розрив між визнаною процесуальними керівниками доцільністю таких угод і їх фактичною незастосовуваністю є самостійним аргументом на користь адаптації відповідних норм.

7. Єдиною прямою нормативною підставою поводження з віртуальними активами у кримінальному провадженні є частина десята статті 170 Кримінального процесуального кодексу України (можливість арешту), тоді як сама процедура спирається на не пристосовані до цифрової природи активу загальні норми глави 17. Законність арешту з конфіскаційною метою прямо залежить від достовірного встановлення належності активу, що зумовлює перехід від спрощеного ототожнення «власник - володілець ключа» до встановлення фактичного контролю над ним; незавершеність механізму реалізації загрожує перетворенням арешту на «перманентний».

8. На матеріально-правовому рівні віртуальні активи як нематеріальні блага прямо не охоплюються поняттям «майно» у статті 59 Кримінального кодексу України, унаслідок чого бракує однозначних підстав для їх конфіскації як виду покарання, а звернення активів у дохід держави наразі можливе переважно через цивільну конфіскацію - з опорою на поняття «активи», яке прямо охоплює криптовалюти, за статтею 290 Цивільного процесуального кодексу України. Це зумовлює потребу доповнити статтю 59 Кримінального кодексу України прямими положеннями про конфіскацію криптовалюти й адаптувати норми про спеціальну конфіскацію.

9. Технічні бар'єри однаково паралізують цивільне звернення стягнення й кримінально-виконавчу реалізацію конфіскованих активів, а недостатність примусового виконання створює можливості для ухилення від виконання судових рішень про конфіскацію та відшкодування шкоди, перетворюючи виконавчу прогалину на самостійний криміногенний чинник.

ВИСНОВКИ

У результаті проведеного дослідження кримінально-правової політики у сфері забезпечення охорони віртуальних активів можна сформулювати наступні загальні висновки.

1. Віртуальні активи постали на перетині економічних, технологічних і світоглядних передумов — ідей денаціоналізації грошей, криптоанархічного руху та еволюції технологій цифрових грошей, що завершилася появою біткоїна і технології блокчейн. Децентралізований і псевдонімний характер обігу, відсутність єдиного емітента та незворотність трансакцій визначають специфіку віртуальних активів водночас як предмета кримінальних правопорушень, засобу їх учинення й об'єкта доказування. Сформульовано визначення віртуального активу як майна особливого роду, основою якого є сама інформація, а не носій права вимоги. Чинною легальною дефініцією залишається функціональне визначення Закону № 361-IX, тоді як профільний Закон № 2074-IX лишається нечинним, а орієнтиром майбутньої моделі регулювання виступає Регламент (ЄС) 2023/1114 (MiCA).

2. Понятійний апарат у досліджуваній сфері залишається неусталеним. У дослідженні вибудовано ланцюг «цифрові речі (цифрові активи) — віртуальні активи — криптоактиви — криптовалюта» та відмежовано віртуальні активи від нематеріальних благ та інформації, грошей і засобів платежу, цінних паперів і фінансових інструментів, робіт і послуг. За чинним цивільним законодавством (ст. 179-1 ЦК України) віртуальні активи належать до цифрових речей, а отже до майна, що підтверджує їх придатність бути предметом злочинів проти власності.

3. Єдиного підходу до класифікації віртуальних активів немає ні в доктрині, ні в законодавстві; найбільше прикладне значення мають поділ за критерієм забезпеченості, характерний для законодавства України, і видова типологія MiCA (токени електронних грошей, токени з прив'язкою до активів, інші криптоактиви). Уперше обґрунтовано самостійне кримінально-правове

значення класифікації віртуальних активів: вид активу безпосередньо впливає на встановлення предмета та кваліфікацію правопорушень — забезпечений актив тяжіє до предмета злочинів проти власності; незабезпечений породжує проблему визначення предмета й доказування вартості; фінансові активи окреслюють сферу посягань, пов'язаних із ринками капіталу; платіжні та анонімні активи становлять підвищений ризик використання як засобу легалізації (відмивання) доходів і фінансування тероризму; поділ на централізовані та децентралізовані активи визначає коло суб'єктів фінансового моніторингу й реальні межі кримінально-правової охорони.

4. Стан наукової розробленості проблеми є нерівномірним: понятійно-класифікаційні аспекти опрацьовані достатньо, тоді як власне кримінально-правовий і політико-правовий виміри досліджені фрагментарно. Відтак, уперше сформульовано поняття *кримінально-правової політики у сфері забезпечення охорони віртуальних активів як системної діяльності уповноважених суб'єктів щодо формування і реалізації стратегії кримінально-правової охорони відносин, що виникають у зв'язку зі створенням, обігом та використанням таких активів*, і розкрито її структуру. Її ознаками є подвійна родова належність, похідний (субсидіарний) характер щодо регулятивного законодавства з переважно бланкетною природою заборон, міжнародна та європейська зумовленість, технологічна складність об'єкта й динамічність; суб'єктом формування є Верховна Рада України (ст. 92 Конституції України), суб'єктами реалізації — органи досудового розслідування, прокуратура, суд та органи виявлення, розшуку й управління активами. Систему принципів утворюють законність криміналізації, юридична визначеність, пропорційність і гуманність та невідворотність відповідальності.

6. Система міжнародних стандартів регулювання й охорони віртуальних активів є багаторівневою: її ядро утворюють Рекомендації ФАТФ (насамперед 15 і 16), макрофінансовий контур — рекомендації FSB та елементи політики МВФ, а регіональну гармонізацію забезпечує право Європейського Союзу на чолі з Регламентом MiCA. Обґрунтовано, що, на відміну від традиційних сфер охорони, де визначальними є внутрішні соціально-економічні чинники й

національна правова традиція, у сфері віртуальних активів первинним джерелом політики виступає зовнішній — наднаціональний — нормативний і досвідний масив, що зумовлено транскордонною природою активів і задає зміст бланкетних заборон, межі допустимої криміналізації та орієнтири гармонізації. Досвід держав поза ЄС (зокрема Гонконгу, де провадження діяльності оператора без ліцензії визнане кримінальним правопорушенням) підтверджує передбачуваність кримінально-правового захисту дозвільного режиму.

7. Національне регулювання обігу віртуальних активів має перехідний характер: профільний Закон № 2074-IX ухвалено, але не введено в дію (його введення поставлено в залежність від змін до податкового законодавства), а де-юре статус активів визначається функціональним підходом Закону № 361-IX. Реформа просувається через перехід до моделі ринків віртуальних активів за зразком Регламенту (ЄС) 2023/1114 (MiCA) на основі законопроекту № 10225-д, що зміщує акцент із дозвільної на реєстраційно-наглядову конструкцію. Основним напрямом удосконалення є синхронізація профільної реформи з гармонізацією термінології та завершенням законодавчого контуру обігу віртуальних активів.

8. Кримінально-правові засоби посідають субсидіарне місце в механізмі охорони обігу віртуальних активів, доповнюючи регулятивні й фінансово-моніторингові інструменти, а не замінюючи їх. Запобіжно-ризиковий вимір політики (ризик-орієнтований контроль, співрегулювання, саморегулювнi організації) має бути збалансований презумпцією добросовісності (ч. 5 ст. 12 ЦК України), покладенням тягара доказування правомірності рішень на регулятора (ч. 2 ст. 77 КАС України), правом особи на інформацію та пропорційністю криміналізації, оскільки межа добросовісної поведінки збігається з межею поведінки, що не суперечить законодавству про кримінальну відповідальність. З огляду на нечинність Закону № 2074-IX цей вимір є перспективним складником політики, зорієнтованим на поступовий перехід до європейської моделі регулювання.

9. Віртуальні активи посідають у системі об'єктів та предметів кримінальних правопорушень неоднозначне місце: залежно від обставин вони

виступають предметом правопорушення (насамперед проти власності), засобом або знаряддям його вчинення, предметом незаконного збагачення та об'єктом фінансового моніторингу, що вимагає попереднього розмежування ролей. За чинним цивільним законодавством (ст. 179-1 ЦК України, запроваджена Законом № 3320-IX) віртуальні активи визнаються майном і різновидом цифрової речі та наділені всіма ознаками предмета злочинів проти власності — фізичною, економічною та юридичною; де-юре підставою такого визнання є саме ст. 179-1 ЦК України, а не нечинний Закон № 2074-IX. Контроль над приватним ключем і незворотність транзакцій ускладнюють встановлення власника та моменту вибуття активу.

10. Обґрунтовано багатовимірну систематизацію кримінальних правопорушень у сфері віртуальних активів: за роллю активу у складі (предмет; засіб чи спосіб учинення; об'єкт протиправного впливу), за технологічним критерієм (кіберуможливлені та кіберзалежні посягання) і за об'єктом охорони з прив'язкою до статей Кримінального кодексу України.

11. Розкрито особливості кваліфікації типових кримінальних правопорушень: при легалізації (ст. 209 КК України) вузловим є питання визначення предмета та специфіка етапів крипто-легалізації; протидія фінансуванню тероризму й обходу санкцій (ст. 258-5 КК України) спирається на двоїсту природу активу — інструмент ухилення і водночас джерело доказів завдяки відстежуваності блокчейну; шахрайство (ст. 190 КК України) охоплює актив як предмет і засіб, але стримується невизначеністю речово-правового статусу й волатильністю; незаконне збагачення (ч. 3 ст. 368-5 КК України прямо охоплює криптовалюти) ускладнене термінологічною неузгодженістю та браком методології визначення вартості активів, насамперед невзаємозамінних токенів; кіберправопорушення (Розділ XVI КК України) забезпечують охорону безпеки інфраструктури ринку; незаконні азартні ігри (ст. 203-2 КК України) криміналізують недотримання дозвільного порядку, а не вид майна.

12. Процесуальна складова кримінально-правової політики залишається незавершеною: єдина згадка віртуальних активів у Кримінальному процесуальному кодексі України стосується лише накладення арешту, а

спеціальні процедури їх виявлення, фіксації та вилучення відсутні. Віртуальний актив не є речовим доказом у розумінні ст. 98 КПК України з огляду на його нематеріальну природу і не утворює окремого виду «електронних доказів»; доказове значення має належно зафіксована у протоколі слідчої (розшукової) дії цифрова інформація про актив, а національна практика виробила стандарт доведення належності активу через публічну адресу (відкритий ключ). Підтримано чотиривимірну криміналістичну сутність активу, який одночасно може бути засобом учинення правопорушення, його предметом, джерелом доказової інформації та наслідком злочинної діяльності; дієвість цих рішень похідна від включення постачальників послуг до периметра протидії відмиванню коштів за стандартами ФАТФ, директивами ЄС та МіСА.

13. На завершальному відрізку провадження чинна модель обмежується накладенням арешту за ч. 10 ст. 170 КПК України на загальних нормах, не пристосованих до цифрової природи активу. На матеріально-правовому рівні бракує однозначних підстав для конфіскації віртуальних активів як виду покарання, оскільки вони не охоплюються поняттям «майно» в розумінні ст. 59 КК України, а звернення їх у дохід держави наразі можливе переважно через цивільну конфіскацію; навіть за наявності підстави реалізація блокується на етапі реалізації кримінально-виконавчої політики. На цій підставі комплексно підтверджено положення про нерозривний взаємозв'язок матеріальної, процесуальної та кримінально-виконавчої складових політики. Основним напрямом удосконалення є синхронна адаптація матеріального, процесуального і кримінально-виконавчого законодавства із запровадженням технічно реалізовної процедури ідентифікації, арешту, оцінки, конфіскації й реалізації активу через авторизованих посередників.

14. Узагальнюючи, ефективність охоронної функції кримінального права у сфері віртуальних активів визначається не окремо взятою матеріальною заборonoю, а узгодженістю матеріальної, процесуальної та виконавчої складових політики в сфері боротьби з злочинністю, синхронізованою із завершенням профільної реформи за моделлю Регламенту (ЄС) 2023/1114 (МіСА) та гармонізацією національних механізмів зі стандартами ФАТФ.

Наскрізний дуалізм правового статусу віртуального активу — чинний функціональний за Законом № 361-IX і нечинна цивілістична модель Закону № 2074-IX — має бути усунутий уведенням профільного закону в гармонії з правом Європейського Союзу; до того кримінально-правова політика спирається на бланкетне застосування чинних норм Кримінального кодексу України у системному зв'язку з регуляторними та фінансово-моніторинговими інструментами. Реалізація сформульованих пропозицій дає змогу перейти від фрагментарної охорони до цілісної, зорієнтованої на ЄС та технічно забезпеченої системи кримінально-правової охорони віртуальних активів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX (не набрав чинності). Голос України. 2022. 16 берез. № 57. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (дата звернення: 14.02.2026).
2. 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. Official Journal of the European Union. L 150, 9.6.2023. P. 40-205. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj> (дата звернення: 14.02.2026).
3. Школьний В. Онтологічні засади та генезис віртуальних активів (криптовалюти) в сучасних умовах розвитку соціально-правової системи. Слово Національної школи суддів України. 2021. № 3 (36). С. 58-66. DOI: [https://doi.org/10.37566/2707-6849-2021-3\(36\)-5](https://doi.org/10.37566/2707-6849-2021-3(36)-5).
4. Савчук В. К., Собченко Т. С., Бойченко В. Т. Віртуальні активи - пізнання сутності, облікове відображення, аналітична оцінка. Економіка і управління бізнесом. 2023. Т. 14, № 1. С. 38-53. DOI: [https://doi.org/10.31548/economics14\(1\).2023.003](https://doi.org/10.31548/economics14(1).2023.003).
5. Погрібний Д. І. Тенденції правового забезпечення використання технології блокчейн та віртуальних активів. Теорія і практика правознавства. 2020. Вип. 2 (18). DOI: <https://doi.org/10.21564/2225-6555.2020.18.216789>.
6. Гончаренко С. Ю. Інновації в фінансовій сфері: віртуальні активи — поява, розвиток і тенденції правового регулювання. Держава та регіони. Серія: Право. 2021. № 2 (72). С. 152-157. DOI: <https://doi.org/10.32840/1813-338X-2021.2.25>.
7. Панасюк В. М., Гальчак Х. Р., Босий В. А. Особливості обліку розрахунків у сфері е-комерції віртуальними активами (криптовалютою): міжнародний та вітчизняний досвід. Бізнес Інформ. 2023. № 2. С. 222-228. DOI: <https://doi.org/10.32983/2222-4459-2023-2-222-228>.

8. Самсін Р. І. Еволюція термінів «криптовалюта», «віртуальні активи» та «криптоактиви» у сучасній правовій площині. Київський часопис права. 2024. № 2. С. 213-221. DOI: <https://doi.org/10.32782/klj/2024.2.31>.
9. Кудь А. А. Феномен віртуальних активів: економіко-правовий аспект. International Journal of Education and Science. 2020. Vol. 3, No. 3. Р. 30-42. DOI: <https://doi.org/10.26697/ijes.2020.3.3>.
10. Цукан С. В. Поняття, правова природа та класифікація віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 80, ч. 1. С. 613-618. DOI: <https://doi.org/10.24144/2307-3322.2023.80.1.94>.
11. Самсін Р. І. Генезис визначення віртуальних активів у правовому полі України: від грошового сурогату до цифрового вираження вартості. Правові новели. 2021. № 15. С. 210-216. DOI: <https://doi.org/10.32847/ln.2021.15.26>.
12. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. Відомості Верховної Ради України. 2020. № 25. Ст. 171. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text> (дата звернення: 14.02.2026).
13. Ушинкіна О. А. Концептуальні підходи до визначення поняття «віртуальні активи» в Україні та у світі. Юридичний вісник. 2022. № 3 (64). С. 70-76. DOI: <https://doi.org/10.18372/2307-9061.64.16880>.
14. Могил Л. С. Порядок обліку операцій з криптовалютою як різновидом віртуальних активів. Аналітично-порівняльне правознавство. 2023. № 2. С. 168-174. DOI: <https://doi.org/10.24144/2788-6018.2023.02.28>.
15. Ковальова Т. В., Хорошилова І. О. Про облік віртуальних активів в Україні. Економіка. Фінанси. Право. 2022. № 10/1. С. 37-40. DOI: [https://doi.org/10.37634/efp.2022.10\(1\).8](https://doi.org/10.37634/efp.2022.10(1).8).
16. Мілаш В. С. Деякі аспекти правової природи віртуальних активів/криптовалюти в умовах глобальної цифровізації. Право та інновації. 2020. № 2 (30). С. 7-16. DOI: [https://doi.org/10.37772/2518-1718-2020-2\(30\)-1](https://doi.org/10.37772/2518-1718-2020-2(30)-1).

17. Аксюков С. М. Поняття та природа віртуальних активів як об'єкту правового регулювання в господарській діяльності в Україні. Аналітично-порівняльне правознавство. 2024. № 1. С. 258-263. DOI: <https://doi.org/10.24144/2788-6018.2024.01.45>.
18. Дмитренко Т. Визначення сутності віртуальних активів як чинник формування методологічних підходів до оподаткування їх обороту. Вісник Чернівецького торговельно-економічного інституту. 2024. Вип. IV (96). С. 121-143. DOI: <https://doi.org/10.34025/2310-8185-2024-4.96.08>.
19. Савенкова В. Г., Вихристенко Б. О. Теоретико-правові підходи та практичні аспекти визначення віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 87, ч. 3. С. 137-144. DOI: <https://doi.org/10.24144/2307-3322.2025.87.3.20>.
20. Грицай С. О. Поняттєвий ряд — віртуальні активи. Науковий вісник Ужгородського національного університету. Серія: Право. 2022. Вип. 70. С. 313-318. DOI: <https://doi.org/10.24144/2307-3322.2022.70.49>.
21. Грицай С. О. Правова сутність дефініції «віртуальні активи» у Законі України «Про віртуальні активи». Аналітично-порівняльне правознавство. 2022. № 1. С. 244-248. DOI: <https://doi.org/10.24144/2788-6018.2022.01.45>.
22. Гавриленко В., Крот Ю., Ткаченко А., Міщенко А. Фінансовий та податковий облік і контроль віртуальних активів: новітні міжнародні практики та шляхи їх імплементації в Україні. Економічний вісник Черкаського державного технологічного університету. 2025. Т. 26, вип. 2 (75). С. 154-171. DOI: [https://doi.org/10.24025/2306-4420.75\(2\).2025.338803](https://doi.org/10.24025/2306-4420.75(2).2025.338803).
23. Нікітін В. В. Місце і роль віртуальних активів в фінансовій системі України. Право і суспільство. 2025. № 3, ч. 2. С. 493-499. DOI: <https://doi.org/10.32842/2078-3736/2025.3.2.67>.
24. Щеглаков І. Е. Проблеми розмежування «криптермінів» при кваліфікації кримінальних правопорушень проти власності. Вісник Асоціації кримінального права України. 2025. № 1 (23). С. 225-246. DOI: <https://doi.org/10.21564/2311-9640.2025.23.331560>.

25. Дмитрик О. О. Віртуальні активи і цифрові активи: до питання про співвідношення понять. *Право та інноваційне суспільство*. 2021. № 2 (17). С. 248-254. DOI: [https://doi.org/10.37772/2309-9275-2021-2\(17\)-33](https://doi.org/10.37772/2309-9275-2021-2(17)-33).
26. Савченко Є. Ю. Цифрові речі, цифрові активи, віртуальні активи та цифрові токени: розмежувати не можна консолідувати. *Київський часопис права*. 2024. № 3. С. 87-95. DOI: <https://doi.org/10.32782/klj/2024.3.13>.
27. Цивільний кодекс України: Кодекс України від 16.01.2003 № 435-IV. *Відомості Верховної Ради України*. 2003. №№ 40-44. Ст. 356. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 15.02.2026).
28. Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав: Закон України від 10.08.2023 № 3320-IX (чинний з 03.09.2023). URL: <https://zakon.rada.gov.ua/laws/show/3320-20#Text> (дата звернення: 15.02.2026).
29. Некіт К. Г. Віртуальні активи як різновид цифрових речей. *Часопис цивілістики*. 2022. Вип. 45. С. 53-57. DOI: <https://doi.org/10.32837/chc.v0i45.466>.
30. Савченко Є. Ю. Віртуальні активи: нематеріальні блага чи окремі об'єкти цивільних прав? *Юридичний вісник*. 2023. № 6. С. 301-310. DOI: <https://doi.org/10.32782/yuv.v6.2023.37>.
31. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 15.02.2026).
32. Легенько В. Ю. Порівняльна характеристика віртуальних активів та інших об'єктів приватноправових відносин. *Аналітично-порівняльне правознавство*. 2024. № 4. С. 129-133. DOI: <https://doi.org/10.24144/2788-6018.2024.04.21>.
33. Грицай С. О. Віртуальний актив в Україні є засобом платежу? *Актуальні проблеми політики*. 2022. Вип. 70. С. 131-137. DOI: <https://doi.org/10.32782/app.v70.2022.21>.
34. Музика Л. А. Позика віртуальних активів: правовий вимір. *Юридичний вісник*. 2025. № 3. С. 73-80. DOI: <https://doi.org/10.32782/yuv.v3.2025.9>.

35. Про платіжні послуги: Закон України від 30.06.2021 № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text> (дата звернення: 15.02.2026).
36. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III. Відомості Верховної Ради України. 2001. № 5-6. Ст. 30. URL: <https://zakon.rada.gov.ua/laws/show/2121-14#Text> (дата звернення: 15.02.2026).
37. Про валюту і валютні операції: Закон України від 21.06.2018 № 2473-VIII. Відомості Верховної Ради України. 2018. № 30. Ст. 239. URL: <https://zakon.rada.gov.ua/laws/show/2473-19#Text> (дата звернення: 15.02.2026).
38. Про ринки капіталу та організовані товарні ринки: Закон України від 23.02.2006 № 3480-IV. Відомості Верховної Ради України. 2006. № 31. Ст. 268. URL: <https://zakon.rada.gov.ua/laws/show/3480-15#Text> (дата звернення: 15.02.2026).
39. Савченко Є. Ю. Використання віртуальних активів за договорами міни. Наукові записки НаУКМА. Юридичні науки. 2024. Т. 14. С. 66-75. DOI: <https://doi.org/10.18523/2617-2607.2024.14.66-75>.
40. Арзянцева Д. А., Захаркевич Н. П. Проблеми використання цифрових активів у діяльності віртуальних організацій. Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. 2019. Т. 1, № 1. С. 1-7. DOI: <https://doi.org/10.23939/smeu2019.01.001>.
41. Самсін Р. І. Класифікація віртуальних активів. Центральнотукаїнський вісник права та публічного управління. 2024. Вип. 2 (6). С. 90-98. DOI: <https://doi.org/10.32782/cuj-2024-2-12>.
42. Яроцький В. О. Поняття та види віртуальних активів, що можуть перебувати в обігу за законодавством України. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки. 2023. Т. 34 (73), № 4. С. 101-107. DOI: <https://doi.org/10.32782/TNU-2707-0581/2023.4/15>.
43. Грицай С. О. Перспективи оподаткування операцій з забезпеченими віртуальними активами в Україні. Науковий вісник публічного та приватного права. 2022. Вип. 2. С. 68-73. DOI: <https://doi.org/10.32844/2618-1258.2022.2.11>.

44. Невмержицький Є. І., Єщенко М. С. Технологічна характеристика ф'ючерсів на віртуальних активах. Наукові записки НаУКМА. Комп'ютерні науки. 2021. Т. 4. С. 113-116. DOI: <https://doi.org/10.18523/2617-3808.2021.4.113-116>.
45. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Official Journal of the European Union. L 267, 10.10.2009. P. 7-17. URL: <https://eur-lex.europa.eu/eli/dir/2009/110/oj> (дата звернення: 05.03.2026).
46. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Official Journal of the European Union. L 156, 19.6.2018. P. 43-74. URL: <https://eur-lex.europa.eu/eli/dir/2018/843/oj> (дата звернення: 05.03.2026).
47. Фріс П. Л. Кримінально-правова політика Української держави: теоретичні, історичні та правові проблеми : монографія. Київ : Атіка, 2005. 332 с.
48. Фріс П. Л. Політика у сфері боротьби зі злочинністю і права людини : монографія. Івано-Франківськ ; Надвірна : Надвірнянська друкарня, 2009. 169 с.
49. Борисов В. І. Державна політика у сфері боротьби зі злочинністю та її напрямки. Проблеми законності. 2009. Вип. 100. С. 305-312.
50. Козич І. В. Кримінально-правова політика: функції та функціонування : монографія / наук. ред. П. Л. Фріс. Івано-Франківськ : Супрун В. П., 2020. 296 с.
51. Микитин Ю. І. Кримінальна процесуальна політика Європейського Союзу як частина політики Європейського Союзу у сфері боротьби зі злочинністю. Аналітично-порівняльне правознавство. 2021. № 3. С. 185-189. DOI: <https://doi.org/10.24144/2788-6018.2021.03.35>.

52. Кернякевич-Танасійчук Ю. В. Кримінально-виконавча політика України : монографія. Івано-Франківськ : Прикарпатський національний університет імені Василя Стефаника, 2019. 336 с.
53. Кучерявий А. О. Інституціональне забезпечення регулювання віртуальних активів: аналіз розкриття в літературі. Міжнародний науковий журнал «Інтернаука». Серія: Економічні науки. 2024. № 8 (88), т. 2. С. 123-130. DOI: <https://doi.org/10.25313/2520-2294-2024-8-10250>.
54. Khan D., Farman H., Hassan S., Seelro M., Mughal M. H. Cryptocurrency Crimes: A Systematic Literature Review of Bitcoin's Role in Illicit Activities. Pakistan Journal of Engineering Technology and Science (PJETS). 2024. Vol. 12, Issue 1. P. 12-25. DOI: <https://doi.org/10.22555/pjets.v12I1.1121>.
55. Navani S., Cirella G. T. Cybercrimes in the Cryptocurrency Domain: Identifying Types, Understanding Motives and Techniques, and Exploring Future Directions for Technology and Regulation. Journal of Geography, Politics and Society. 2024. Vol. 14, No. 2. P. 1-22. DOI: <https://doi.org/10.26881/jpgs.2024.2.01>.
56. Guidara A. Cryptocurrency and money laundering: a literature review. Corporate Law & Governance Review. 2022. Vol. 4, Issue 2. P. 36-41. DOI: <https://doi.org/10.22495/clgrv4i2p4>.
57. Collins J. A. Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti-Money Laundering Regulations. University of Miami Business Law Review. 2025. Vol. 34, Issue 1. P. 71-103. URL: <https://repository.law.miami.edu/umbl/vol34/iss1/5> (дата звернення: 10.04.2026).
58. Karchevskyi M., Kovalenko A., Matviichuk A., Zavalnyi M. V. Legal aspects of cryptocurrency's circulation: international experience and possibilities of its application in Ukraine. Cuestiones Políticas. 2021. Vol. 39, No. 70. P. 153-164. DOI: <https://doi.org/10.46398/cuestpol.3970.09>.
59. Газдайка-Василишин І. Переосмислення ознак об'єкта кримінального правопорушення у цифрову епоху. Соціально-правові студії. 2026. Т. 9, № 1. С. 9-16. DOI: <https://doi.org/10.32518/sals1.2026.09>.

60. Карчевський М. В. Blockchain та Bitcoin: що це таке та «як працює»? Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2018. Вип. 4 (84). С. 108-117. DOI: <https://doi.org/10.33766/2524-0323.84.108-117>.
61. Грунь О. В. Окремі аспекти методології дослідження правової регламентації відносин у сфері віртуальної реальності. Київський часопис права. 2024. № 3. С. 21-27. DOI: <https://doi.org/10.32782/klj/2024.3.3>.
62. Мічурін Є. О. Об'єкти цифрових технологій та їхнє правове регулювання. Copernicus Political and Legal Studies. 2022. Vol. 1, Issue 3. P. 22-29. DOI: <https://doi.org/10.15804/CPLS.20223.03>.
63. Олійник Д. М. Поняття адміністративно-правового забезпечення державної політики щодо розвитку і функціонування ринку віртуальних активів в Україні. Вісник Кримінологічної асоціації України. 2024. № 3 (33). С. 668-676. DOI: <https://doi.org/10.32631/vca.2024.3.62>.
64. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України. 2001. № 25-26. Ст. 131. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 14.02.2026).
65. Кулик О. І. Ринок віртуальних активів як об'єкт правового регулювання. Форум права. 2020. Т. 63, № 4. С. 56-63. DOI: <https://doi.org/10.5281/zenodo.4249276>.
66. Починок О. Структура правових відносин, пов'язаних з обігом віртуальних активів. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2023. № 4 (40). С. 219-231. DOI: <https://doi.org/10.23939/law2023.40.219>.
67. Бондаренко О. В. Суб'єкти забезпечення обігу віртуальних активів. Держава та регіони. Серія: Право. 2023. № 1 (79). С. 242-246. DOI: <https://doi.org/10.32840/1813-338X-2023.1.39>.
68. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 14.02.2026).

69. Ушинкіна О. А. Правова характеристика суб'єктного складу правовідносин, що виникають у зв'язку з обігом віртуальних активів. Юридичний вісник. 2023. № 1 (66). С. 97-104. DOI: <https://doi.org/10.18372/2307-9061.66.17423>.

70. Грицай С. О. Учасники ринку віртуальних активів в Україні. Дніпровський науковий часопис публічного управління, психології, права. 2022. Вип. 3. С. 152-157. DOI: <https://doi.org/10.51547/ppp.dp.ua/2022.3.25>.

71. Цукан С. В. Поняття та правова природа принципів державного регулювання обороту віртуальних активів. Аналітично-порівняльне правознавство. 2024. № 6. С. 674-678. DOI: <https://doi.org/10.24144/2788-6018.2024.06.111>.

72. Бондаренко О. В. Принципи забезпечення обігу віртуальних активів. Наукові праці Міжрегіональної академії управління персоналом. Юридичні науки. 2022. Вип. 2 (62). С. 86-91. DOI: <https://doi.org/10.32689/2522-4603.2022.2.13>.

73. Цукан С. В. Типологізація принципів державного регулювання обороту віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 87, ч. 3. С. 196-201. DOI: <https://doi.org/10.24144/2307-3322.2025.87.3.28>.

74. Олійник Д. М. Особливості адміністративно-правового впливу на ринок віртуальних активів. Вісник Кримінологічної асоціації України. 2024. № 2 (32). С. 917-926. DOI: <https://doi.org/10.32631/vca.2024.2.71>.

75. Цукан С. В. Міжнародне регулювання обороту віртуальних активів: основні положення та принципи. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 81, ч. 2. С. 228-233. DOI: <https://doi.org/10.24144/2307-3322.2024.81.2.35>.

76. Пазюк А. В. Міжнародно-правові стандарти регулювання віртуальних активів у кіберпросторі: баланс між цифровим суверенітетом та глобальними зобов'язаннями держав. Право і суспільство. 2025. № 3, ч. 2. С. 363-368. DOI: <https://doi.org/10.32842/2078-3736/2025.3.2.49>.

77. The FATF Recommendations. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation / Financial Action Task Force. Paris : FATF, 2012 (updated October 2025). URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> (дата звернення: 15.04.2026).

78. Гончаренко С. Ю. Рекомендації ФАТФ з урегулювання обміну віртуальних активів як протидія загрозам глобальній фінансовій системі. Право і суспільство. 2020. № 3, ч. 2. С. 127-132. DOI: <https://doi.org/10.32842/2078-3736/2020.3-2.20>.

79. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers / Financial Action Task Force. Paris : FATF, 2021. 111 р. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (дата звернення: 15.04.2026).

80. Дмитренко Т. Л., Любіч О. О., Пархоменко Ю. В. Регулювання ринку віртуальних активів: глобальний та національний рівні імплементації міжнародних стандартів ПВК/ФТ. Фінанси України. 2021. № 7. С. 31-52. DOI: <https://doi.org/10.33763/finukr2021.07.031>.

81. Дмитренко Т. Л., Любіч О. О. Упровадження міжнародних стандартів регулювання ринку віртуальних активів в Україні. Фінанси України. 2020. № 9. С. 65-79. DOI: <https://doi.org/10.33763/finukr2020.09.065>.

82. High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets : Final Report / Financial Stability Board. Basel : FSB, 2023. URL: <https://www.fsb.org/uploads/P170723-2.pdf> (дата звернення: 15.04.2026).

83. Elements of Effective Policies for Crypto Assets / International Monetary Fund. IMF Policy Paper No. 2023/004. Washington, D.C. : IMF, 2023. URL: <https://www.imf.org/-/media/files/publications/pp/2023/english/ppea2023004.pdf> (дата звернення: 15.04.2026).

84. Кудь А. А. Сучасні підходи глобального та державного регулювання обігу віртуальних активів: що обрати для підтримки цифрових інновацій? Актуальні проблеми державного управління. 2023. № 1 (62). С. 59-82. DOI: <https://doi.org/10.26565/1684-8489-2023-1-04>.

85. Музика-Стефанчук О. А., Мохнєв С. С. Генеза становлення правового статусу постачальників послуг, пов'язаних з оборотом віртуальних активів, в ЄС. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 85, ч. 3. С. 35-41. DOI: <https://doi.org/10.24144/2307-3322.2024.85.3.5>.

86. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012, and repealing Directive 2005/60/EC and Commission Directive 2006/70/EC. Official Journal of the European Union. L 141, 5.6.2015. P. 73-117. URL: <https://eur-lex.europa.eu/eli/dir/2015/849/oj> (дата звернення: 20.03.2026).

87. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2). Official Journal of the European Union. L 337, 23.12.2015. P. 35-127. URL: <https://eur-lex.europa.eu/eli/dir/2015/2366/oj> (дата звернення: 20.03.2026).

88. Дмитренко Т. Л. Особливості імплементації європейських директив щодо обігу віртуальних активів у національне законодавство України. Фінанси України. 2022. № 12. С. 55-72. DOI: <https://doi.org/10.33763/finukr2022.12.055>.

89. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLR). Official Journal of the European Union. L, 2024/1624, 19.6.2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1624/oj> (дата звернення: 20.03.2026).

90. Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD6). Official Journal of the European Union.

L, 2024/1640, 19.6.2024. URL: <https://eur-lex.europa.eu/eli/dir/2024/1640/oj> (дата звернення: 20.03.2026).

91. Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). Official Journal of the European Union. L, 2024/1620, 19.6.2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1620/oj> (дата звернення: 20.03.2026).

92. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets (Travel Rule). Official Journal of the European Union. L 150, 9.6.2023. P. 1-39. URL: <https://eur-lex.europa.eu/eli/reg/2023/1113/oj> (дата звернення: 20.03.2026).

93. Огляд законодавства щодо регулювання віртуальних активів у сфері боротьби з відмиванням коштів та фінансуванням тероризму. Київ, 2022. 587 с. URL: <https://fiu.gov.ua/assets/userfiles/310/Pizne/VirtualAssets.pdf> (дата звернення: 20.03.2026).

94. Воєводіна Г. І. Формування правових стандартів віртуальних активів в Європейському Союзі: визначення та реалізація : дис. ... д-ра філософії : 293 / Державний університет «Київський авіаційний інститут». Київ, 2026. 244 с. URL: <https://nrat.ukrintei.ua/searchdoc/0826U001053/>.

95. Кулик О. І. Правові засади впливу Європейського Союзу на ринок віртуальних активів. Економіка та право. 2021. № 1. С. 71-79. DOI: <https://doi.org/10.15407/econlaw.2021.01.071>.

96. Устименко В. А., Джабраїлов Р. А., Гудіма Т. С. Правове регулювання ринку віртуальних активів в Україні та Європейському Союзі: порівняльне дослідження. Право України. 2022. № 8. С. 48-61. DOI: <https://doi.org/10.33498/louu-2022-08-048>.

97. Воєводіна Г. І. Європейська система наднаціональних і державних органів, що регулюють обіг віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 84, ч. 4. С. 246-251. DOI: <https://doi.org/10.24144/2307-3322.2024.84.4.34>.

98. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. L 333, 27.12.2022. P. 1-79. URL: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj> (дата звернення: 20.03.2026).

99. Воєводіна Г. Визначення поняття «віртуальні активи»: порівняльний аналіз законодавства і судової практики країн Європейського Союзу. Слово Національної школи суддів України. 2024. № 1 (46). С. 72-80. DOI: [https://doi.org/10.37566/2707-6849-2024-1\(46\)-7](https://doi.org/10.37566/2707-6849-2024-1(46)-7).

100. Judgment of the Court (Fifth Chamber) of 22 October 2015. Skatteverket v David Hedqvist. Case C-264/14. ECLI:EU:C:2015:718. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0264> (дата звернення: 20.03.2026).

101. Ганган В. Г. Правове регулювання інсайдерської інформації на ринку віртуальних активів в Україні та ЄС. Європейський правничий часопис. 2024. Вип. 5. С. 47-55. URL: https://cms.legal-journal.e-u.edu.ua/uploads/5_8_09e1f729a4.pdf (дата звернення: 20.03.2026).

102. Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation, MAR) and repealing Directive 2003/6/EC and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC. Official Journal of the European Union. L 173, 12.6.2014. P. 1-61. URL: <https://eur-lex.europa.eu/eli/reg/2014/596/oj> (дата звернення: 20.03.2026).

103. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II) (recast). Official Journal of the European Union. L 173, 12.6.2014. P. 349-496. URL: <https://eur-lex.europa.eu/eli/dir/2014/65/oj> (дата звернення: 20.03.2026).

104. Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive, CSMAD). Official Journal of the European Union. L 173, 12.6.2014. P. 179-189. URL: <https://eur-lex.europa.eu/eli/dir/2014/57/oj> (дата звернення: 20.03.2026).

105. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. Official Journal of the European Union. L 284, 12.11.2018. P. 22-30. URL: <https://eur-lex.europa.eu/eli/dir/2018/1673/oj> (дата звернення: 20.03.2026).

106. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні : проєкт Закону України від 07.11.2023 № 10225. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/43123> (дата звернення: 20.03.2026).

107. Judgment of the Court (Second Chamber) of 11 March 2015. Jean-Bernard Lafonta v Autorité des marchés financiers (AMF). Case C-628/13. ECLI:EU:C:2015:162. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0628> (дата звернення: 20.03.2026).

108. Грицай С. О. Зміна профільного закону про віртуальні активи: імплементація європейського регламенту MiCA. Юридичний вісник. 2023. № 1 (66). С. 72-82. DOI: <https://doi.org/10.18372/2307-9061.66.17420>.

109. Овсійчук Т. П. Порівняльна характеристика основних категорій, запропонованих у проєкті Закону про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні, з чинним законодавством та Регламентом № 2020/0265. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки. 2023. Т. 34 (73), № 6. С. 68-73. DOI: <https://doi.org/10.32782/TNU-2707-0581/2023.6/11>.

110. Воєводіна Г. І. Майбутні міркування щодо загальноєвропейського регулювання віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 84, ч. 4. С. 239-245. DOI: <https://doi.org/10.24144/2307-3322.2024.84.4.33>.

111. Матвієнко В. В., Котенко А. М. До питання правового режиму віртуальних активів в Україні та світі. Економіка. Фінанси. Право. 2020. № 12/2. С. 18-23. DOI: [https://doi.org/10.37634/efp.2020.12\(2\).4](https://doi.org/10.37634/efp.2020.12(2).4).

112. Кулик О. І. Правове регулювання ринку віртуальних активів: досвід Швейцарської Конфедерації. Актуальні проблеми держави і права. 2021. Вип. 92. С. 44-51. DOI: <https://doi.org/10.32837/apdp.v0i92.3260>.
113. Самсін Р. І. Державне регулювання у сфері обігу віртуальних активів: світовий досвід. Правова позиція. 2020. № 3 (28). С. 137-141. DOI: <https://doi.org/10.32836/2521-6473.2020-3.27>.
114. Яроцький В. О. Зарубіжний досвід регулювання обігу віртуальних активів та можливість його імплементації в Україні. Успіхи і досягнення у науці. 2025. № 12 (22). С. 618-628. DOI: [https://doi.org/10.52058/3041-1254-2025-12\(22\)-618-628](https://doi.org/10.52058/3041-1254-2025-12(22)-618-628).
115. Легенько В. Ю. Правове регулювання віртуальних активів у Спеціальному адміністративному районі КНР Гонконг. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 79, ч. 1. С. 206-210. DOI: <https://doi.org/10.24144/2307-3322.2023.79.1.35>.
116. Попов Р. В. Віртуальні активи: особливості державного механізму регулювання та міжнародний досвід. Право і суспільство. 2024. № 5. С. 693-699. DOI: <https://doi.org/10.32842/2078-3736/2024.5.100>.
117. Доляновська І. М., Кривенко К. О. Світовий досвід протидії кримінальним правопорушенням, пов'язаним з обігом віртуальних активів. Legal Bulletin. 2024. № 2 (12). С. 79-86. DOI: <https://doi.org/10.31732/2708-339X-2024-12-A12>.
118. Гудіма Т. С., Устименко В. А., Джабраїлов Р. А., Черних О. Г. Особливості правового регулювання обігу віртуальних активів в Україні: де-факто vs де-юре. Financial and Credit Activity: Problems of Theory and Practice. 2022. Vol. 5 (46). Р. 137-148. DOI: <https://doi.org/10.55643/fcaptp.5.46.2022.3844>.
119. Грицай С. О. Правовий режим віртуальних активів в Україні. Juris Europensis Scientia. 2022. Вип. 2. С. 65-68. DOI: <https://doi.org/10.32837/chern.v0i2.349>.
120. Верес І. Я. Правовий режим віртуальних активів. Часопис цивілістики. 2025. Вип. 57. С. 103-108. DOI: <https://doi.org/10.32782/chc.v057.2025.15>.

121. Грицай С. О. Сфера застосування законодавства України про віртуальні активи. Актуальні проблеми вітчизняної юриспруденції. 2022. № 2. С. 54-59. DOI: <https://doi.org/10.32782/392278>.
122. Самсін Р. І. Державне регулювання у сфері обігу віртуальних активів в Україні. Право та інновації. 2022. № 4 (40). С. 69-74. DOI: [https://doi.org/10.37772/2518-1718-2022-4\(40\)-10](https://doi.org/10.37772/2518-1718-2022-4(40)-10).
123. Грицай С. О. Національна комісія з цінних паперів та фондового ринку як суб'єкт адміністрування віртуальних активів в Україні. Науковий вісник публічного та приватного права. 2022. Вип. 1. С. 86-92. DOI: <https://doi.org/10.32844/2618-1258.2022.1.14>.
124. Волинець В. В. Державний контроль за обігом віртуальних активів в Україні. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 88, ч. 2. С. 26-32. DOI: <https://doi.org/10.24144/2307-3322.2025.88.2.3>.
125. Добровольська В. В. Державний контроль щодо застосування та обігу цифрових (віртуальних) активів. Актуальні проблеми вітчизняної юриспруденції. 2023. № 2. С. 57-62. DOI: <https://doi.org/10.32782/39221470>.
126. Рядінська В. О. Напрями реформування правового регулювання у сфері обороту віртуальних активів в Україні. Наука і правоохорона. 2024. № 1 (63). С. 99-110. DOI: [https://doi.org/10.36486/np.2024.1\(63\).10](https://doi.org/10.36486/np.2024.1(63).10).
127. Чернов Л. О. Актуальні проблеми та перспективи розвитку правового регулювання віртуальних активів. Актуальні проблеми держави і права. 2024. Вип. 102. С. 125-132. DOI: <https://doi.org/10.32782/apdp.v102.2024.17>.
128. Миронов О. Г. Регулювання віртуальних активів в Україні: поточний стан та перспективи. Інвестиції: практика та досвід. 2024. № 9. С. 80-86. DOI: <https://doi.org/10.32702/2306-6814.2024.9.80>.
129. Федоренко Т. В. Правове регулювання віртуальних активів в Україні: перспективи розвитку. Сучасний науковий журнал. 2024. № 3 (1). С. 47-53. DOI: <https://doi.org/10.36994/2786-9008-2024-3-6>.

130. Шемет Д. С. Правове регулювання віртуальних активів: виклики легалізації та інституційного впровадження в Україні. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 87, ч. 3. С. 236-241. DOI: <https://doi.org/10.24144/2307-3322.2025.87.3.35>.
131. Стеблянко А. В., Шевцов Я. А. Легалізація віртуальних активів в Україні: правовий аспект і загальна концепція. Форум права. 2021. № 4 (69). С. 29-36. DOI: <https://doi.org/10.5281/zenodo.5075714>.
132. Некіт К. Г. Розвиток правового регулювання обігу віртуальних активів (криптовалют) в Україні. Часопис цивілістики. 2022. Вип. 44. С. 45-50. DOI: <https://doi.org/10.32837/chc.v0i44.455>.
133. Грудницький В. М. Правове регулювання обігу віртуальних (цифрових) активів в Україні. Київський часопис права. 2023. № 2. С. 43-49. DOI: <https://doi.org/10.32782/klj/2023.2.6>.
134. Лагунов К. В., Кузьмінська О. Е. Нормативно-правове забезпечення операцій з віртуальними активами в Україні. Фінанси України. 2025. № 2. С. 116-124. DOI: <https://doi.org/10.33763/finukr2025.02.116>.
135. Нагнибіда В. І. Реалізація положень законодавства про віртуальні активи у світлі політики діджиталізації. Наукові записки Інституту законодавства Верховної Ради України. 2021. № 5. С. 45-52. URL: http://nbuv.gov.ua/j-pdf/Nzizvru_2021_5_7.pdf (дата звернення: 10.03.2026)
136. Любіч О. О., Волкова В. М., Гавриленко С. В., Пархоменко Ю. В. Вплив воєнного стану в Україні на легалізацію і розвиток ринку віртуальних активів. Наукові праці НДФІ. 2022. № 4 (101). С. 41-51. DOI: <https://doi.org/10.33763/npndfi2022.04.041>.
137. Дмитренко Т. Л. Регулювання ринку віртуальних активів як інструмент протидії уникненню міжнародних санкцій проти рф. Фінанси України. 2022. № 4. С. 107-128. DOI: <https://doi.org/10.33763/finukr2022.04.107>.
138. Грицай С. О. Порядок отримання дозволу на надання послуг, пов'язаних з віртуальними активами в Україні. Наукові праці Міжрегіональної академії управління персоналом. Юридичні науки. 2022. Вип. 2 (62). С. 11-17. DOI: <https://doi.org/10.32689/2522-4603.2022.2.2>.

139. Кулик О. І. Поняття і елементи господарської правосуб'єктності постачальників послуг, пов'язаних з оборотом віртуальних активів. Аналітично-порівняльне правознавство. 2024. № 5. С. 282-287. DOI: <https://doi.org/10.24144/2788-6018.2024.05.45>.

140. Про особливості регулювання діяльності юридичних осіб окремих організаційно-правових форм у перехідний період та об'єднань юридичних осіб: Закон України від 09.01.2025 № 4196-IX. URL: <https://zakon.rada.gov.ua/laws/show/4196-20#Text> (дата звернення: 10.03.2026).

141. Грицай С. О. Відповідальність за порушення вимог щодо обігу віртуальних активів в Україні. Нове українське право. 2022. Вип. 3. С. 60-67. DOI: <https://doi.org/10.51989/NUL.2022.3.9>.

142. Кулик О. І. Удосконалення правового регулювання посередницької діяльності на ринку віртуальних активів. ScienceRise: Juridical Science. 2021. № 2 (16). С. 58-64. DOI: <https://doi.org/10.15587/2523-4153.2021.234724>.

143. Худик А. М. Правове регулювання обігу віртуальних активів та їх використання в кримінальному праві і процесі. Академічні візії. 2025. Вип. 42. DOI: <https://doi.org/10.5281/zenodo.15343342>.

144. Кримінальний процесуальний кодекс України: Кодекс України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України. 2013. № 9-10, № 11-12, № 13. Ст. 88. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 10.03.2026).

145. Вереша Р. В., Карпунцов В. В. Правове забезпечення та фактори ризику обігу віртуальних активів: національний та міжнародно-правовий аспекти. Вісник Національної академії правових наук України. 2025. Т. 32, № 1. С. 66-85. DOI: <https://doi.org/10.31359/1993-0909-2025-32-1-66>.

146. Зянько В. В., Нечипоренко Т. Д. Віртуальні активи крізь призму вітчизняної практики: ризикоорієнтованість та імплементація. Фінанси України. 2022. № 3. С. 88-106. DOI: <https://doi.org/10.33763/finukr2022.03.088>.

147. Кибиш І. В., Лугіна Н. А. Запобігання кримінальним правопорушенням, пов'язаним із використанням криптовалюти. Аналітично-

порівняльне правознавство. 2022. № 4. С. 287-292. DOI: <https://doi.org/10.24144/2788-6018.2022.04.52>.

148. Кулик О. І. Впровадження презумпції добросовісності учасників ринку віртуальних активів. Часопис цивілістики. 2024. Вип. 54. С. 17-22. URL: <https://clj.nuoua.od.ua/archive/54/4.pdf> (дата звернення: 10.03.2026).

149. Кодекс адміністративного судочинства України: Кодекс України від 06.07.2005 № 2747-IV. Відомості Верховної Ради України. 2005. № 35-36, № 37. Ст. 446. URL: <https://zakon.rada.gov.ua/laws/show/2747-15#Text> (дата звернення: 10.03.2026).

150. Кулик О. І. Саморегулювання ринку віртуальних активів: поняття та форми. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2020. Вип. 4 (48). С. 99-104.

151. Кузьменко О. В., Кравчук П. Ю. Віртуальні активи як предмет кримінального правопорушення: проблеми визначення та доказування. Аналітично-порівняльне правознавство. 2025. № 6. С. 194-198. DOI: <https://doi.org/10.24144/2788-6018.2025.06.3.29>.

152. Овсійчук Т. П. Віртуальні активи як предмет злочинів проти власності. Європейський правничий часопис. 2025. Вип. 8. С. 137-142. DOI: [https://doi.org/10.36919/3041-1149\(Print\).8.2025.137-142](https://doi.org/10.36919/3041-1149(Print).8.2025.137-142).

153. Черевко К. О. Щодо питання віртуальних активів як предмету кримінальних правопорушень проти власності. Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук: матеріали міжнародної конференції (Харків — Рига, 2022). Харків; Рига, 2022. С. 227-228. URL: <https://dspace.univd.edu.ua/entities/publication/ab20c366-a54e-476a-ad51-108d2e4379f1> (дата звернення: 10.03.2026).

154. Кулик О. І. Віртуальні активи у складі майна суб'єктів господарювання. Правничий часопис Донецького національного університету імені Василя Стуса. 2024. № 2. С. 106-115. DOI: <https://doi.org/10.31558/2786-5835.2024.2.11>.

155. Савченко Є. Ю. Правовий режим власності на віртуальні активи. Нове українське право. 2024. Вип. 6. С. 165-181. DOI: <https://doi.org/10.51989/NUL.2024.6.24>.

156. Посполітак В. В., Савченко Є. Ю. Момент набуття права власності на віртуальні активи за цивільно-правовим договором. Київський часопис права. 2025. № 4. С. 57-63. DOI: <https://doi.org/10.32782/klj/2025.4.8>.

157. Іванський А. Й. Фінансово-правові аспекти кваліфікації віртуальних активів в Україні у порівнянні з досвідом Європейського Союзу та інших зарубіжних країн. Право і суспільство. 2024. № 1, т. 2. С. 163-169. DOI: <https://doi.org/10.32842/2078-3736/2024.1.2.24>.

158. Юсупов В. В., Марчук Р. П. Протидія незаконному обігу віртуальних активів в Україні: питання правового регулювання. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90, ч. 4. С. 367-373. DOI: <https://doi.org/10.24144/2307-3322.2025.90.4.53>.

159. Дмитренко Т. Л., Волкова В. М. Особливості регулювання операцій із віртуальними активами щодо діяльності у сфері майнінгу. Наукові праці НДФІ. 2021. № 2 (95). С. 85-95. URL: http://npndfi.org.ua/docs/NP_21_02_085_uk.pdf (дата звернення: 10.04.2026).

160. Подолян Ю. О., Романенко О. В. Питання правового регулювання генерування віртуальних активів як виду підприємницької діяльності. Dictum Factum. 2021. № 2 (10). С. 64-72. DOI: <https://doi.org/10.32703/2663-6352/2021-2-10-64-72>.

161. Europol. Cryptocurrencies — Tracing the evolution of criminal finances. Europol Spotlight Report series. Luxembourg : Publications Office of the European Union, 2021. 20 p. DOI: <https://doi.org/10.2813/75468>. URL: <https://www.europol.europa.eu> (дата звернення: 10.04.2026).

162. Arnone G., Scirè G., Bivona E. The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review. Digital Finance. 2025. Vol. 7, Issue 4. P. 815-851. DOI: <https://doi.org/10.1007/s42521-025-00148-1>.

163. Казначеева Д. В., Дорош А. О. Кримінальні правопорушення у сфері обігу криптовалюти. Вісник Кримінологічної асоціації України. 2021. № 2

(25). С. 149-157. URL: <https://dspace.univd.edu.ua/bitstreams/882dbcb7-bd33-412f-8a0c-94491e535d4d/download> (дата звернення: 12.04.2026)

164. Саєнко В. В. Виокремлення видів злочинної діяльності, у яких віртуальні активи є засобом вчинення кримінальних правопорушень, як підстава формування окремих криміналістичних методик розслідування. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 92, ч. 4. С. 409-421. DOI: <https://doi.org/10.24144/2307-3322.2025.92.4.57>.

165. 2026 Crypto Crime Report / TRM Labs. San Francisco, CA : TRM Labs, 2026. 60 p. URL: <https://www.trmlabs.com> (дата звернення: 12.04.2026).

166. Trozze A., Kamps J., Akartuna E. A. та ін. Cryptocurrencies and future financial crime. Crime Science. 2022. Vol. 11. Art. 1. 35 p. DOI: <https://doi.org/10.1186/s40163-021-00163-8>.

167. Карчевський М. В. Кримінальне право в умовах цифрової трансформації. Від несанкціонованого доступу до «jailbreak» штучного інтелекту : монографія / Ун-т Короля Данила ; Ін-т інформації, безпеки і права Нац. акад. прав. наук України. Харків : Право, 2025. 176 с. ISBN 978-617-8617-41-7.

168. The Little Book of Crypto Crime / Metropolitan Police Service. London : Mayor's Office for Policing and Crime ; The Crown, 2025. 56 p. (Little Media Series). URL: <https://www.met.police.uk/littlemedia> (дата звернення: 11.04.2026).

169. Політова А. С. Стан наукової розробки проблем кримінально-правової протидії легалізації (відмиванню) майна, одержаного злочинним шляхом, за допомогою віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90, ч. 4. С. 123-129. DOI: <https://doi.org/10.24144/2307-3322.2025.90.4.17>.

170. Самойлов Є. Ю. Деякі проблеми експліцитних ознак легалізації (відмивання) майна, одержаного злочинним шляхом, вчинюваної з використанням віртуальних активів. Вісник Кримінологічної асоціації України. 2024. Т. 33, № 3. С. 772-781. DOI: <https://doi.org/10.32631/vca.2024.3.73>.

171. Каменський Д. В., Дудоров О. О. Відмивання злочинних доходів через операції з віртуальними валютами: нова загроза економічній безпеці. Аналітично-порівняльне правознавство. 2024. № 1. С. 500-509. DOI: <https://doi.org/10.24144/2788-6018.2024.01.88>.

172. Каменський Д. В., Титаренко С. С. Віртуальні активи як інструмент легалізації майна, одержаного злочинним шляхом: порівняльно-правовий аспект. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 80, ч. 2. С. 41-50. DOI: <https://doi.org/10.24144/2307-3322.2023.80.2.6>.

173. Думчиков М. Особливості протидії легалізації злочинних доходів за допомогою віртуальних активів у кіберпросторі: практичний вимір. Law. State. Technology. 2022. Вип. 1. С. 117-122. DOI: <https://doi.org/10.32782/LST/2022-1-18>.

174. Дмитренко Т. Л. Особливості регулювання операцій із віртуальними активами щодо протидії легалізації доходів, отриманих злочинним шляхом. Фінанси України. 2020. № 3. С. 112-126. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Fu_2020_3_9.pdf (дата звернення: 15.02.2026).

175. Грицай С. О. Тенденції протидії відмиванню доходів отриманих злочином шляхом: віртуальні активи. Міжнародний науковий журнал «Інтернаука». Серія: Юридичні науки. 2024. № 1 (71). С. 17-27. DOI: <https://doi.org/10.25313/2520-2308-2024-1-9602>.

176. Кулик О. І. Законодавче забезпечення протидії відмиванню коштів та фінансуванню тероризму під час здійснення операцій із віртуальними активами. Juris Europensis Scientia. 2021. Вип. 3. С. 43-48. DOI: <https://doi.org/10.32837/chern.v0i3.227>.

177. Кришевич О. В., Рощина І. О. Криптовалюта як предмет кримінального правопорушення проти власності: національне та міжнародне законодавство. Вісник Маріупольського державного університету. Серія:

Право. 2022. Вип. 23-24. С. 168-175. DOI: <https://doi.org/10.34079/2226-3047-2022-12-23-24-168-175>.

178. Давлатов Ш. Б., Подгорна А. В. Кримінальна відповідальність за незаконне привласнення віртуальних активів. Правова позиція. 2024. № 3 (44). С. 69-74. DOI: <https://doi.org/10.32782/2521-6473.2024-3.12>.

179. Думчиков М. О. Особливості кваліфікації шахрайства в кіберпросторі, засобом вчинення якого є віртуальні активи. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право. 2022. Вип. 14 (26). С. 159-165. DOI: <https://doi.org/10.33098/2078-6670.2022.14.26.149-155>.

180. Про внесення змін до деяких законодавчих актів України щодо конфіскації незаконних активів осіб, уповноважених на виконання функцій держави або місцевого самоврядування, і покарання за набуття таких активів: Закон України від 31.10.2019 № 263-IX. Відомості Верховної Ради України. 2020. № 2. Ст. 5. URL: <https://zakon.rada.gov.ua/laws/show/263-20#Text> (дата звернення: 15.02.2026).

181. Овсійчук Т. П. Теоретико-правові аспекти визначення віртуальних активів як предмета незаконного збагачення. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 88, ч. 3. С. 157—161. DOI: <https://doi.org/10.24144/2307-3322.2025.88.3.23>.

182. Про запобігання корупції: Закон України від 14.10.2014 № 1700-VII. Відомості Верховної Ради України. 2014. № 49. Ст. 2056. URL: <https://zakon.rada.gov.ua/laws/show/1700-18#Text> (дата звернення: 15.02.2026).

183. Думчиков М. О., Куліш А. М. Характеристика ознак віртуальних активів, що роблять їх привабливими для вчинення корупційних правопорушень: виклики національної безпеки. Академічні візії. 2024. Вип. 28. URL: <https://academy-vision.org/index.php/av/article/view/917/821> (дата звернення: 15.02.2026).

184. Elsayed S. Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption. Bergen : U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute,

2023. 21 р. (U4 Helpdesk Answer 2023:8). URL: <https://www.u4.no/publications/cryptocurrencies-corruption-and-organised-crime> (дата звернення: 10.04.2026).

185. Юринець Ю. Л., Криволап Є. В., Белкін Л. М., Белкін М. Л. Захист надійності віртуальних активів в системі кібербезпеки та кіберзахисту. Актуальні питання у сучасній науці. 2026. № 1 (43). С. 1120-1129. DOI: [https://doi.org/10.52058/2786-6300-2026-1\(43\)-1120-1129](https://doi.org/10.52058/2786-6300-2026-1(43)-1120-1129).

186. Кулик О. І. Інфраструктура ринку віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Вип. 63. С. 183-189. URL: <https://scispace.com/pdf/infrastruktura-rinku-virtualnikh-aktiviv-9869vd9lxl.pdf> (дата звернення: 10.04.2026).

187. Донець А. Г. Договір зберігання віртуальних активів (Crypto Custody) за законодавством України. Теорія і практика правознавства. 2022. Вип. 2 (22). С. 40-63. DOI: <https://doi.org/10.21564/2225-6555.2022.2.267943>.

188. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 12.04.2026).

189. Добровольська В. В. Правовий аспект безпеки віртуальних активів. Часопис цивілістики. 2023. Вип. 48. С. 60-64. DOI: <https://doi.org/10.32782/chc.v048.2023.8>.

190. Про державне регулювання діяльності щодо організації та проведення азартних ігор: Закон України від 14.07.2020 № 768-IX. Голос України. 2020. 12 серп. № 141-142. URL: <https://zakon.rada.gov.ua/laws/show/768-20#Text> (дата звернення: 14.02.2026).

191. Кулик О. І. Правове регулювання проведення азартних ігор з використанням віртуальних активів. Вісник Львівського торговельно-економічного університету. Юридичні науки. 2023. № 14. С. 43-49. DOI: <https://doi.org/10.32782/2616-7611-2023-14-07>.

192. Співак О. М. Віртуальні активи та он-лайн ігри: правове регулювання та питання захисту. *Право і суспільство*. 2024. № 2. С. 416-419. DOI: <https://doi.org/10.32842/2078-3736/2024.2.58>.

193. Старенький О. С. Використання віртуальних активів у кримінальному процесуальному доказуванні: проблеми правової визначеності та критерії допустимості. *Вісник кримінального судочинства*. 2026. № 1. С. 247-273. DOI: <https://doi.org/10.59835/2413-5372.2026.1/247-273>.

194. Кузьменко О. В., Кравчук П. Ю. Віртуальні активи як предмет кримінального правопорушення: проблеми визначення та доказування. *Аналітично-порівняльне правознавство*. 2025. № 6, ч. 3. С. 194-198. DOI: <https://doi.org/10.24144/2788-6018.2025.06.3.29>.

195. Gromek M. *Decoding Crypto Crime: A Guide for Law Enforcement*. Vienna : OSCE, Office of the Co-ordinator of OSCE Economic and Environmental Activities, 2025. 64 p. URL: <https://www.osce.org/occea/587475> (дата звернення: 12.04.2026).

196. Віртуальні активи у правосудді: національна практика та європейська перспектива : наук.-метод. рек. для суддів / уклад.: Н. Ахтирська, Л. Паршикова, Б. Остудімов. Київ : Національна школа суддів України, 2025. URL: <https://nsj.gov.ua/files/1767784436virtualni-actyvy2025.pdf> (дата звернення: 12.04.2026).

197. Саєнко В. В. Аналіз стану наукового дослідження проблем розслідування кримінальних правопорушень, пов'язаних з використанням віртуальних активів. *Аналітично-порівняльне правознавство*. 2025. № 4, ч. 3. С. 280-294. DOI: <https://doi.org/10.24144/2788-6018.2025.04.3.41>.

198. Мартиненко К. В. Організація розслідування кримінальних правопорушень, пов'язаних із використанням віртуальних активів: проблеми та стан наукових досліджень. *Аналітично-порівняльне правознавство*. 2026. № 2, ч. 3. С. 138-147. DOI: <https://doi.org/10.24144/2788-6018.2026.02.3.19>.

199. Яцик Т. П., Шкелебей В. А. Розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів. *Науковий вісник*

Ужгородського національного університету. Серія: Право. 2023. Вип. 80, ч. 2. С. 219-223. DOI: <https://doi.org/10.24144/2307-3322.2023.80.2.34>.

200. Школьніков В. І. Технології обробки та аналізу руху віртуальних активів під час досудового розслідування. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 87, ч. 4. С. 418-424. DOI: <https://doi.org/10.24144/2307-3322.2025.87.4.65>.

201. Про затвердження Порядку організації та забезпечення досудового розслідування злочинів, у результаті вчинення яких одержано майно (доходи) : наказ Офісу Генерального прокурора, Міністерства внутрішніх справ України, Служби безпеки України, Державного бюро розслідувань, Національного антикорупційного бюро України, Бюро економічної безпеки України від 28.10.2024 № 254/724/520/401/177/185. URL: https://zakon.rada.gov.ua/laws/show/v254_905-24#Text (дата звернення: 12.04.2026).

202. Крижановський А. С. Особливості проведення оперативно-розшукових заходів при розкритті кримінальних правопорушень, що вчиняються у сфері віртуальних активів. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 92, ч. 4. С. 305-311. DOI: <https://doi.org/10.24144/2307-3322.2025.92.4.41>.

203. Ковальський А. В. Проблемні аспекти негласних заходів оперативних підрозділів під час виявлення та розшуку віртуальних активів, пов'язаних із кримінальними правопорушеннями. Юридичний науковий електронний журнал. 2024. № 10. С. 447-450. DOI: <https://doi.org/10.32782/2524-0374/2024-10/103>.

204. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text> (дата звернення: 12.04.2026).

205. Мовчан А. В., Козій В. В. Укладення угод у кримінальному провадженні про незаконне заволодіння криптовалютою (віртуальними

активами). Галицькі студії. Юридичні науки. 2024. № 5. С. 37-44. DOI: https://doi.org/10.32782/galician_studies/law-2024-5-6.

206. Шайтуро О. П., Рибалко Г. С. Накладення арешту на віртуальні активи у кримінальному провадженні. Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Право. 2025. Вип. 39. С. 335-342. DOI: <https://doi.org/10.26565/2075-1834-2025-39-37>.

207. Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів: Закон України від 10.11.2015 № 772-VIII. Відомості Верховної Ради України. 2016. № 1. Ст. 2. URL: <https://zakon.rada.gov.ua/laws/show/772-19#Text> (дата звернення: 12.04.2026).

208. Капліна О. В., Парфило І. В. Проблеми тимчасового вилучення та арешту криптоактивів у кримінальному провадженні. Право України. 2025. № 9. С. 90-107. DOI: <https://doi.org/10.33498/louu-2025-09-090>.

209. Козій В. В. Конфіскація криптовалюти (віртуальних активів) під час виконання судових рішень у кримінальному провадженні. Криміналістика і судова експертиза. 2024. Вип. 69. С. 72-84. DOI: <https://doi.org/10.33994/kndise.2024.69.06>.

210. Цивільний процесуальний кодекс України: Кодекс України від 18.03.2004 № 1618-IV. Відомості Верховної Ради України. 2004. № 40-41, 42. Ст. 492. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text> (дата звернення: 12.04.2026).

211. Кримінально-виконавчий кодекс України: Кодекс України від 11.07.2003 № 1129-IV. Відомості Верховної Ради України. 2004. № 3-4. Ст. 21. URL: <https://zakon.rada.gov.ua/laws/show/1129-15#Text> (дата звернення: 12.04.2026).

212. Про виконавче провадження: Закон України від 02.06.2016 № 1404-VIII. Відомості Верховної Ради України. 2016. № 30. Ст. 542. URL: <https://zakon.rada.gov.ua/laws/show/1404-19#Text> (дата звернення: 12.04.2026).

213. Про затвердження Порядку реалізації арештованого майна: наказ Міністерства юстиції України від 29.09.2016 № 2831/5; зареєстровано в

Міністерстві юстиції України 30.09.2016 за № 1301/29431. URL: <https://zakon.rada.gov.ua/laws/show/z1301-16#Text> (дата звернення: 12.04.2026).

214. Гайдучок О. О. Особливості віртуальних активів як об'єкта звернення стягнення у виконавчому провадженні. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 88, ч. 2. С. 336-342. DOI: <https://doi.org/10.24144/2307-3322.2025.88.2.45>.

215. Global Code of Digital Enforcement / International Union of Judicial Officers (UIHJ). Brussels: Bruylant, 2021. URL: <https://www.uihj.com/> (дата звернення: 12.04.2026).

216. Кодекс України з процедур банкрутства: Кодекс України від 18.10.2018 № 2597-VIII. Відомості Верховної Ради України. 2019. № 19. Ст. 74. URL: <https://zakon.rada.gov.ua/laws/show/2597-19#Text> (дата звернення: 12.04.2026).

217. Ткаченко А., Пожуєв О. Механізм звернення стягнення на віртуальні активи боржника у разі оголошення його банкрутом. Економічний аналіз. 2024. Т. 34, № 1. С. 279-291. DOI: <https://doi.org/10.35774/econa2024.01.279>.

218. Грицай С. О. Порядок реалізації віртуальних активів в Україні. Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки. 2022. Вип. 1 (61). С. 18-23. DOI: <https://doi.org/10.32689/2522-4603.2022.1.3>.

219. Гринь І. О. Правове регулювання порядку звернення стягнення на віртуальні активи у межах примусового виконання судових рішень в Україні та країнах ЄС. Наукові записки. Серія: Право. 2025. Вип. 19. С. 193-199. DOI: <https://doi.org/10.36550/2522-9230-2025-19-193-199>.

220. Щербак С., Рєпін Д. Електронні гроші та віртуальні активи в умовах цифровізації виконавчого провадження. Теоретичні та прикладні питання державотворення. 2025. № 33. С. 403-416. DOI: <https://doi.org/10.35432/tisb332025333264>.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України (категорія «Б»):

1. Ногін В.В. Генеза поняття віртуальних активів та предмет кримінально-правової охорони. *Актуальні проблеми вдосконалення чинного законодавства України. Випуск 60, 2022. С.293-301*

DOI: <https://doi.org/10.15330/apiclu.60.293-301>

URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10750/10367>

2. Ногін В.В. Легальні дефініції віртуального актива та їх значення для кримінально-правової охорони. *Актуальні проблеми вдосконалення чинного законодавства України. Випуск 61, 2023. С.1.72-1.79*

DOI: <https://doi.org/10.15330/apiclu.61.1.72-1.79>

URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10751/10368>

3. Ногін В.В. Зарубіжний досвід правового регулювання віртуальних активів у сфері протидії відмиванню коштів і фінансуванню тероризму та орієнтири для кримінально-правової політики України. *Актуальні проблеми вдосконалення чинного законодавства України. Випуск 65, 2024. С.1.149-1.158*

DOI: <https://doi.org/10.15330/apiclu.65.1.149-1.158>

URL: <https://journals.pnu.edu.ua/index.php/apiclu/article/view/10752/10369>

Праці, що засвідчують апробацію матеріалів дисертації:

4. Ногін В.В. Кримінально-правова політика у сфері захисту віртуальних активів: виклики та перспективи. *Вдосконалення правового регулювання: погляд молодих науковців [Текст] : Матеріали щорічної Всеукраїнської науково-*

практичної конференції здобувачів освіти та молодих вчених (9 травня 2025 року). Івано-Франківськ, 2025.с. 319-321.

URL:

<https://law.cnu.edu.ua/wp-content/uploads/sites/100/2025/12/youth2025.pdf>

5. Ногін В.В. Цивільно-правовий договір щодо віртуальних активів у механізмі кримінально-правової охорони. *Договір як універсальна форма правового регулювання: Матеріали Всеукраїнської науково-практичної конференції, присвяченої пам'яті академіка Національної академії правових наук України, заслуженого діяча науки і техніки України, доктора юридичних наук, професора Володимира Васильовича Луця (1933-2021) (м. Івано-Франківськ, 17 квітня 2026р.). Івано-Франківськ: Карпатський національний університет імені Василя Стефаника, 2026. Івано-Франківськ, 2025.с. 268-271.*

URL:

https://kcp.cnu.edu.ua/wp-content/uploads/sites/82/2026/06/zbirnyk_dohovir_2026-2.pdf