

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет цивільної та господарської юстиції
Кафедра приватного права
Кафедра права інтелектуальної власності та патентної юстиції**

ІТ-ПРАВО, КІБЕРБЕЗПЕКА ТА ШІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**МАТЕРІАЛИ
Всеукраїнської наукової конференції**

28 березня 2026 р.

Одеса
Фенікс
2026

За загальною редакцією

доктора юридичних наук, професора **Є. О. Харитонова**,
докторки юридичних наук, професорки **І. В. Давидової**

Упорядники-укладачі:

Давидова І. В. — доктор юридичних наук, професор, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Калітенко О. М. — кандидат юридичних наук, доцент, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Бобейко Н. І. — лаборантка кафедри приватного права Національного університету «Одеська юридична академія».

ІТ-право, кібербезпека та ШІ в умовах гібридної війни :
I-92 матеріали Всеукр. наук. конф. (Одеса, 28 берез. 2026 р.) / за заг. ред.: д-ра юрид. наук, проф. Є. О. Харитонова, д-ра юрид. наук, проф. І. В. Давидової. Одеса : Фенікс, 2026. 300 с. DOI: <https://doi.org/10.32837/11300.33701>

ISBN 978-617-8763-22-0

Збірник містить матеріали доповідей, присвячені актуальним проблемам ІТ-права, кібербезпеки, цифрової трансформації суспільних відносин, правового регулювання штучного інтелекту та захисту інформації в умовах гібридної війни, які були оприлюднені на Всеукраїнській науковій конференції 26 березня 2026 року в Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення науковців, викладачів, здобувачів освіти, практикуючих юристів, фахівців у сфері інформаційних технологій і кібербезпеки з результатами сучасних досліджень щодо правових, організаційних і технологічних аспектів функціонування цифрового середовища в умовах сучасних викликів. Матеріали видання можуть бути використані в науковій, освітній і практичній діяльності, а також під час подальшого вдосконалення правового регулювання цифрових відносин і забезпечення кібербезпеки України.

342.95 : 343.32 (477) : 351.863

Матеріали видано за авторською редакцією.

Повну відповідальність за достовірність і якість поданого матеріалу несуть учасники Всеукраїнської наукової конференції, їхні наукові керівники, рецензенти і структурні підрозділи вищих навчальних закладів та установ, які рекомендували ці матеріали до друку.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Всеукраїнської наукової конференції

Харитонов Є. О. – завідувач кафедри приватного права Національного університету «Одеська юридична академія», д-р юрид. наук, проф. (голова);

Федотов О. П. – начальник науково-дослідної частини, професор кафедри морського, митного та інформаційного права, д-р юрид. наук, проф. (заступник голови);

Харитонova О. І. – завідувачка кафедри права інтелектуальної власності і патентної юстиції, д-р юрид. наук, проф.;

Галупова Л. І. – доцентка кафедри права інтелектуальної власності і патентної юстиції, канд. юрид. наук, доц.;

Зубар В. М. – професор кафедри приватного права, канд. юрид. наук, проф.;

Калітенко О. М. – професорка кафедри приватного права, канд. юрид. наук, доц.;

Кривенко Ю. В. – доцентка кафедри приватного права, канд. юрид. наук, доц.;

Токарева В. О. – доцентка кафедри приватного права, д-р юрид. наук, доц.;

Бобейко Н. І. – лаборантка кафедри приватного права.

Орзiх Юрiй Геннадiйович

*кандидат юридичних наук, доцент, доцент кафедри приватного права Нацiонального унiверситету «Одеська юридична академiя»,
тaршиий викладач в Унiверситетi Еребру (Швецiя)*

**КРИПТОАКТИВИ ЯК ЦИФРОВА ВЛАСНIСТЬ
В УМОВАХ ГIБРИДНОЇ ВIЙНИ: ПРАВО ВЛАСНОСТI,
ДОКАЗУВАННЯ КОНТРОЛЮ ТА AML/CFT-РИЗИКИ**

Проблема криптоактивiв в умовах гiбридної вiйни виходить за межi дискусiї про цифровi фiнансовi iнструменти. Криптоактиви можуть бути засобом швидкого транскордонного перемiщення вартостi, iнвестицiйним активом, об'єктом спадкування, дарування чи внеску до статутного капiталу, а також iнструментом приховування походження майна. Тому вони одночасно належать до площини приватного права, фiнансового монiторингу, кiбербезпеки та правозастосування. Для України, яка перебуває в умовах вiйни та гiбридних загроз, iх правовий режим має не лише ринковий, а й безпековий вимiр.

Європейський пiдхiд поступово формує двi взаємопов'язанi логiки: регулювання ринку криптоактивiв i запобiгання iх використанню для вiдмивання коштів та фiнансування тероризму. Вiдповiдно до MiCA, криптоактивом є цифрове представлення вартостi або права, яке може передаватися i зберiгатися електронно з використанням технологiї розподiленого реєстру або подiбної технологiї [1, ст. 3]. AMLR використовує близьку дефiнiцiйну логiку i поширює AML/CFT-вимоги на ширше коло постачальникiв послуг [2].

Однак для приватного права центральним є питання, чи може криптоактив бути об'єктом майнових прав, передаватися, бути предметом забезпечення, спадкування, дарування, подiлу майна або примусового виконання i сьогодні можна це питання вiдповiсти з позитивно. CNUE Guide розрiзняє криптовалюту, stablecoins, security tokens, utility tokens та NFTs, пiдкреслюючи, що такi криптоактиви є найбільш розповсюдженими i можуть виконувати платiжну, iнвестицiйну, посвiдчувальну або сервісну

функцію [3, с. 7]. Отже, цифрова власність не є однорідною категорією. Її правовий режим залежить від функції активу, способу набуття, форми зберігання та можливості встановити фактичний і правовий контроль.

Ключовим є розмежування між фактичним контролем і правом власності. Приватний ключ або доступ до wallet забезпечує можливість розпорядження активом, але сам по собі не завжди доводить законне набуття активу або виключне право особи на нього. Без врегульованого правом порядку обліку та реєстрації таких активів доказування права власності на нього у певної особи зводить до фактичного володіння активом, а інколи навіть і не самим активом і його носієм. CNUE Guide прямо вказує, що доступ до гаманця може демонструвати контроль, але не є абсолютним доказом права власності водночас підтверджуючи обов'язок нотаріуса перевіряти законність походження активу та право власності на актив у особи [3, с. 23-24]. Тому «контроль» є важливим доказовим індикатором, але не повним юридичним еквівалентом права власності.

Саме тут зростає роль нотаріуса. У традиційному цивільному обороті нотаріус виконує функцію гаранта правової визначеності, перевірки волевиявлення, дієздатності, повноважень, належності документів та законності правочину. Поява криптоактивів не усуває цієї функції, а підвищує її значення. Якщо криптоактив використовується у правочині з нерухомістю, при внеску до статутного капіталу, договорі позики, даруванні, поділі майна подружжя або спадкуванні, нотаріус має встановити юридичну підставу участі цифрового активу в правочині та оцінити ризики його незаконного походження.

CNUE Guide наголошує, що нотаріуси як суб'єкти, на яких поширюються AML/CFT-вимоги, відіграють істотну роль у моніторингу законності правочинів, а включення криптоактивів у юридичні операції створює нові ризики у сфері відмивання коштів і фінансування тероризму [3, с. 19]. В умовах гібридної війни це має особливе значення, адже приватно-правові конструкції

можуть використовуватися для легалізації активів, приховування зв'язку з підсанкційними особами або переміщення вартості поза банківським контролем.

Практична роль нотаріуса не повинна зводитися до технічного спостереження за доступом до гаманця. Нотаріальна перевірка має охоплювати встановлення особи та кінцевого бенефіціарного власника, з'ясування економічної мети правочину, перевірку джерела походження активів, аналіз зв'язку з регульованими або нерегульованими постачальниками послуг, оцінку підозрілих ознак транзакції, документування доказів контролю і передачі. Для hosted wallets можливими доказами можуть бути довідки від regulated exchangers чи wallet providers. Для self-hosted wallets можуть використовуватися digital signatures, screenshots with metadata, signed wallets, transaction history та дані blockchain explorers [3, с. 23-24].

Перевірка завершення передачі криптоактиву має окреме значення. Blockchain explorers дозволяють перевірити transaction ID або transaction hash, адреси учасників, суму, кількість підтверджень, дату, час і статус транзакції [3, с. 24]. У нотаріальному процесі це не перетворює блокчейн-дані на безспірний доказ права власності, але дає можливість фіксувати юридично значущі факти: наявність транзакції, її технічне завершення, відповідність заявлених адрес і часу, а також зв'язок між правочином і цифровим слідом. Окрім цього слід звернути увагу на необхідність приведення Закон України «Про нотаріат» у відповідність з потребами ринку криптоактивів.

Проблема примусового виконання щодо криптоактивів демонструє межі класичних правових інструментів. Якщо активи зберігаються у регульованого постачальника послуг, органи правозастосування можуть взаємодіяти з таким суб'єктом, отримувати інформацію, накладати обмеження або забезпечувати виконання рішення. Якщо активи зберігаються у self-hosted wallet, відсутній центральний адміністратор, який міг би виконати розпорядження державного органу. CNUE Guide зазначає, що в децентралізова-

них системах правоохоронним органам складно спрямувати дії на один центральний суб'єкт або місце для цілей розслідування чи арешту активів [3, с. 12].

AMLR виходить із того, що розвиток технологій створює нові продукти й системи обміну коштів або вартості, однак водночас породжує нові ризики ML/TF [2, п. 7 преамбули]. Для криптоактивів такими ризиками є псевдоанонімність, транскордонність, використання mixers, privacy coins, peer-to-peer transfers, self-hosted wallets та юрисдикцій зі слабким контролем. FATF також підкреслює необхідність risk-based approach, ліцензування або реєстрації VASPs, нагляду з боку компетентних органів та застосування до них релевантних AML/CFT-заходів [4].

У гібридній війні AML/CFT-ризики криптоактивів мають додатковий вимір: фінансування терористичної діяльності, обхід санкцій, приховування активів осіб, пов'язаних з агресором, кіберзлочини, ransomware-платежі, фінансування дезінформаційних або підривних мереж. Тому правове регулювання цифрової власності не може бути ізольованим від режимів фінансового моніторингу, санкційного контролю, кібербезпеки і доказового права. Нотаріус у такій моделі має виступати як gatekeeper правової довіри, який не допускає надання формальної легальності сумнівним цифровим активам через нотаріально посвідчений правочин.

Додатковою правовою невизначеності в українському контексті додає Закон України «Про віртуальні активи» від 17 лютого 2022 року № 2074-IX, який прийнятий, але офіційно не набрав чинності [5]. Водночас чинним залишається Закон України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [6].

З огляду на актуальну ситуацію, доцільно розглядати криптоактиви не лише як об'єкти ринку, а як цифрові майнові об'єкти, які потребують особливого режиму доказування. Такий режим має включати: встановлення виду криптоактиву; перевірку способу набуття; доказування контролю над wallet/private key або

обліковим записом у постачальника послуг; перевірку законності походження джерела доходу; документування цифрового сліду транзакції. Для нотаріальної практики це означає потребу у стандартах обережності, які дозволяють відрізнити технічний доступ від права власності та фіксувати межі нотаріальної відповідальності.

Отже, криптоактиви в умовах гібридної війни мають розглядатися як складна форма цифрової власності, що поєднує приватно-правову, доказову, AML/CFT та кібербезпекову проблематику. Контроль над ключем не дорівнює автоматично праву власності; blockchain record не замінює правочин; нотаріальне посвідчення не повинно легалізувати сумнівне походження активу; AML/CFT-перевірка має враховувати технологічні особливості цифрової власності. Для українського правопорядку перспективною є інтегрована модель яка повинна надавати можливість нотаріусу виконати свої обов'язки суб'єкта первинного фінансового моніторингу та не допустити проведення незаконних правочинів.

ЛІТЕРАТУРА:

1. Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets. OJ EU. 2023. L 150. P. 40-205. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>
2. Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for money laundering or terrorist financing. OJ EU. 2024.
3. CNUE. Crypto Assets: Characteristics, risks and best practices. Council of the Notariats of the European Union.
4. FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021.
5. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. <https://zakon.rada.gov.ua/laws/main/2074-20>
6. 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. <https://zakon.rada.gov.ua/laws/show/361-20#Text>