

УДК 347.73

DOI <https://doi.org/10.32782/apdp.v107.2025.14>*М. Г. Ільченко*

## **ЗАХИСТ ПРАВ УЧАСНИКІВ ПРАВОВІДНОСИН З ОБІГУ КРИПТОВАЛЮТ КРІЗЬ ПРИЗМУ УКРАЇНСЬКИХ РЕАЛІЙ ТА ЗАРУБІЖНОГО ДОСВІДУ**

**Постановка проблеми.** Особливістю механізму фінансово-правового забезпечення обігу криптовалют в Україні є та, що на сьогодні Закон України «Про віртуальні активи» від 17 лютого 2022 року № 2074-IX (далі – Закон № 2074-IX) [1] не набрав чинності. А це означає, що поки що передбаченого у ньому механізму захисту прав учасників правовідносин з обігу криптовалют як важливу складову фінансово-правового забезпечення такого захисту не запроваджено. Однак під час формування його національної моделі важливо також вивчити зарубіжний досвід та із метою визначення шляхів його використання в Україні проаналізувати законодавство Європейського Союзу (далі – ЄС) і окремих зарубіжних країн з цього питання.

**Метою статті** є визначити склад учасників і систему охоронюваних прав суб'єктів правовідносин із обігу криптовалют, ідентифікувати типові ризики їх порушень, проаналізувати засоби правового захисту за правом ЄС, зіставити їх із правовим регулюванням і судовою практикою в Україні.

**Аналіз останніх досліджень і публікацій.** Питанню захисту прав учасників правовідносин з обігу криптовалют наразі не приділено належної уваги з боку науковців та практиків. Проте, окремі аспекти зазначеного питання були висвітлені в працях таких авторів, як Бондаренко О.В., Логойда В.М., Овчаренко А.С. та інші.

**Виклад основного матеріалу.** Відповідно до документів ЄС суб'єктами правовідносин з обігу криптовалют є їх учасники, які володіють правами та обов'язками щодо створення, розміщення, обігу та зберігання криптоактивів. Їх система, на нашу думку, є такою:

- 1) споживачі та інвестори як кінцеві набувачі і користувачі криптоактивів;
- 2) емітенти asset-referenced tokens (ART) і e-money tokens (EMT);
- 3) провайдери послуг із віртуальними активами (криптоактивами) (VASPs (CASPs)), до яких належать оператори торговельних платформ (криптобіржі), посередники (брокери/дилери), кастодіальні сервіси, оператори on-/off-ramp та платіжні провайдери, а також провайдери стейкінгу/кредитування;
- 4) регулятори та інші органи нагляду.

Такий підхід корелюється із переліком видів послуг у Регламенті (ЄС) 2023/1114 (MiCA) (далі – MiCA) і визначає рамку для конкретизації змісту прав кожної групи, а саме: 1) «custody and administration of crypto-assets on behalf of clients» – «зберігання та адміністрування криптоактивів від імені клієнтів»; 2) «operation of a trading platform» – «функціонування (експлуатація) торговельної платформи для криптоактивів»; 3) «exchange of crypto-assets» – «обмін криптоактивів»; 4) «placing of crypto-assets» – «розміщення криптоактивів»; 5) «reception and transmission of orders» – «прийняття та передавання розпоряджень (доручень)

клієнтів щодо криптоактивів»; 6) «advice on crypto-assets» – «надання консультацій щодо криптоактивів» [2, ст. 3(1)(15)–(16), 59–63].

У питанні щодо прав учасників правовідносин з обігу криптовалют та моделей їх захисту нами проаналізовано положення законодавства ЄС (Регламенту (ЄС) 2023/1113 (TFR) (далі – TFR) та MiCA), Великої Британії, США.

Так, MiCA містить організаційні засади діяльності CASP, вимоги доступу до ринку (авторизація (ліцензія)), поведінкові та операційні стандарти захисту користувачів. Документ також визначає: обов'язки щодо структури управління та систем управління ризиками; вимоги до ІТ-безпеки (повідомлення про інциденти, надійне управління ключами тощо) [2, статті 59–63, 75–80]; порядок розгляду скарг і внутрішні процедури обробки звернень клієнтів, заборони конфліктів інтересів [2, статті 63, 68].

Для емітентів ART (Asset-Referenced Token) – токенів, забезпечених сировинними активами, нерухомістю або портфелем різних активів (далі – ART) та EMT (Electronic Money Token) – токенів, які підтримують стабільну вартість завдяки забезпеченню фіатними валютами і використовуються для платежів – далі EMT) передбачено вимоги до резервів (забезпечення), прозорості та погашення (викупу) [2, ст. 17–45], а для регуляторів й інших органів нагляду – повноваження щодо санкцій, приписів та відкликання дозволу за схемою «порушення – відновлення прав – санкція» [2, ст. 90–111].

Зауважимо, що нормами TFR на перекази криптоактивів поширено «travel rule» – міжнародний стандарт регулювання передачі криптовалют між користувачами із встановленням обов'язку супроводжувати транзакції ідентифікаційними даними відправника й одержувача та порогів верифікації для операцій між CASP і «само-кастоді» (self-hosted) [2, ст. 14–16, 28; преамбула]. Вимоги MiCA і TFR про управління ризиками деталізуються через настанови Європейської бізнес-асамблеї (Europe Business Assembly (EBA) щодо факторів ризику для CASP [3].

До майнових прав інвестора також належить право власності на криптоактив як об'єкт, здатний бути предметом речово-правових і забезпечувальних заходів: у common law (загальному праві) це прямо визнано High Court у справі «AA v Persons Unknown», де суд підтвердив можливість застосування proprietary injunction щодо біткоїнів як «форми майна» [4, §59]. Для інвесторів (споживачів) підставою для захисту може бути настання таких ризиків: шахрайство та «піраміди»; некоректна комунікація; маніпулювання ринком; замороження (втрата доступу) до активів унаслідок кастодіальних збоїв або втрати приватних ключів; недобросовісні практики лістингу; залучення кредиту для придбання високоризикових активів; прямі матеріальні втрати, упущена вигода.

Якщо мову вести про права та обов'язки емітентів токенів (у тому числі емітентів ART (EMT)), то вони мають право доступу до публічного ринку на умовах рівного ставлення, на захист ділової репутації. Водночас на них покладаються обов'язки щодо достовірних розкриттів (white paper (маркетингові матеріали)), корпоративного управління ризиками (у тому числі ІТ-ризиками), безпечного механізму викупу (погашення) для EMT і стабілізаційних резервів для ART та заборона вводити в оману інвесторів [2, ст. 5, 17–22, 30–45].

Правовий статус провайдерів послуг із віртуальними криптоактивами (VASPs та CASPs) і мінімальні стандарти організації їх діяльності, управління ризиками, IT-безпеки та роботи зі скаргами визначені у MiCA. Так для кастодіальної діяльності встановлені окремі вимоги щодо сегрегації клієнтських активів, обліку та своєчасного доступу, включно з розмежуванням власних і клієнтських правомочностей та з обов'язком негайного інформування про інциденти, що загрожують доступності активів [2, ст. 59–63, 75–80].

Для провайдерів переказів діє режим TFR, який імперативно встановлює супровідні дані, пороги, винятки для P2P-переказів без провайдера та обмін інформацією між залученими CASP [2, ст. 14–16, 28]. Це зобов'язує провайдера супроводжувати перекази криптоактивів інформацією про відправника (одержувача), у тому числі для цілей превенції шахрайства та полегшення подальшого відновлення прав [2, ст. 5, 63, 68; 2, ст. 14–16].

Відповідно до проаналізованих нами положень права ЄС система охоронюваних прав вказаних суб'єктів охоплює:

1) право на правдиві розкриття та коректний маркетинг (споживач/інвестор) та обов'язок провайдера забезпечити зрозумілі комунікації та заборону вводити в оману [5, п. 1.11–1.14; 6];

2) майнові права на криптоактив як об'єкт власності, з можливістю захисту речово-правовими й забезпечувальними інструментами (арешт активів, розкриття інформації) [4, §59];

3) право на збереження, сегрегацію та своєчасний доступ (повернення) клієнтських активів (кастоді) з покладенням відповідальності за операційні збої [2, ст. 75–80];

4) право на приватність і захист персональних даних у межах AML і сервісної взаємодії [2, ст. 14–16; 7, ст. 8, 24];

5) право на ефективні засоби правового захисту (судові (ін'юнкції, арешт активів, розкриття інформації), позасудові (регуляторні скарги, ADR (alternative dispute resolution) – «альтернативне врегулювання спорів»), компенсаційні механізми) з публічно-правовими інструментами нагляду, приписів і санкцій у регулятора [2, ст. 90–111].

Зазначений аналіз показує, що наслідком порушення системи охоронюваних прав учасників правовідносин з обігу криптовалюти є настання майнових та (або) процесуальних наслідків та потреба у застосуванні визначених механізмів відновлення. Механізмів відновлення порушених прав за законодавством ЄС, Великої Британії та США є декілька: 1) регуляторні скарги та дії нагляду; 2) блокування незаконних промоцій і запровадження стандартних попереджень про ризики та «період охолодження» для нових клієнтів (Велика Британія) [5, п. 1.11–1.14; 6]; звернення до національного компетентного органу щодо CASP з подальшим застосуванням інструментів VI розділу MiCA (штрафи, приписи, відкликання дозволу) – у ЄС [2, ст. 90–111]; 2) судові засоби [4, §59; 8, с. 1–3; 9]; вжиття тимчасових заходів щодо учасників шахрайських схем [10].

Щодо законодавства України, то у ньому визначений правовий статус таких реальних (можливих) учасників аналізованих правовідносин:

операторів обміну, кастодіальних сервісів, провайдерів переказів як суб'єктів первинного фінансового моніторингу та їх обов'язки відповідно до статей 10-12 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06 грудня 2019 року № 361-ІХ щодо: ідентифікації та верифікації клієнтів; моніторингу операцій; зберігання інформації; застосування посиленого фінансового моніторингу у випадках підвищеного ризику [11];

– надавачів платіжних послуг, які відповідно до Закону України «Про платіжні послуги» від 30 червня 2021 року № 1591-ІХ зобов'язані: ініціювати платежі; зберігати кошти користувачів (статті 15-23); управляти ризиками; забезпечувати безпеку платіжних операцій, повернення коштів у випадку несанкціонованих транзакцій. Також у цьому Законі визначено вимоги до договорів, до переддоговірної інформації, до безпеки операцій і до процедур повернення коштів у разі несанкціонованих транзакцій, що безпосередньо стосується операторів фіатних шлюзів, пов'язаних із криптосервісами [12, ст. 29–37, 51–52]. Ці норми безпосередньо формують правові механізми захисту клієнтів у випадках технічних збоїв або недобросовісної поведінки провайдерів;

– надавачів та користувачів електронних послуг, які відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» від 05 жовтня 2017 року № 2155-VIII [13] з метою електронної ідентифікації мають мати кваліфікований електронний підпис та печатки, електронні позначки часу, що має особливе значення для фіксації волевиявлень користувачів при здійсненні транзакцій із віртуальними активами та веденні журналів подій і може використовуватися як доказ у спорах щодо моменту вчинення транзакції;

– власників криптоактивів – щодо їх права на приватність та захист персональних даних, що охоплює обробку даних і журналів доступу, а також кореспондуючі обов'язки провайдера щодо законності обробки й безпеки даних та повідомляти про порушення безпеки, належні технічні та організаційні заходи відповідно до Закону України «Про захист персональних даних» від 01 червня 2010 року № 2297-VI (статті 6–8, 24) [14], що є підставою для правового захисту клієнтів у випадках витоку (несанкціонованого) доступу до даних;

– приватні VASP, на яких поширюються вимоги щодо управління ризиками, впровадження стандартів безпеки та проходження аудиту на договірних засадах або унаслідок приєднання до галузевих стандартів відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII [15].

Щодо прав та обов'язків учасників аналізованих правовідносин як суб'єктів оподаткування операцій із віртуальними активами, то норми Податкового кодексу України про це досі не набрали чинності, а тому до них застосовується загальний податковий режим. За умови імплементації Стандарту звітності для криптоактивів (CARF) та внесення змін до Директиви DAC8 ЄС, яка почне застосовуватися з 1 січня 2026 року і передбачатиме розбудову процедур due diligence та обов'язки звітування й обміну податково значущими даними з іншими юрисдикціями [16],

важливо врахувати зазначене під час внесення змін до Податкового кодексу України та Закону № 2074-IX.

В Україні на сьогодні законодавчо визначеного механізму захисту прав учасників правовідносин саме у сфері обігу віртуальних активів немає через те, що Закон № 2074-IX не набрав чинності і ліцензійно-дозвільну модель діяльності постачальників послуг, пов'язаних із віртуальними активами (VASP), передбачену в ньому, не запроваджено. Тому нагальною є потреба у його запровадженні. Окрім того, доцільно у майбутній національний режим ліцензування постачальників послуг з віртуальними активами інтегрувати AML-процедури [17, с. 149–154], тобто правила запобігання використанню криптовалют для відмивання грошей.

Аналізуючи вітчизняну практику у сфері захисту прав учасників правовідносин з обігу криптовалют, звернемо увагу на її особливості, які містять окремі висновки судів. Насамперед, деякі рішення стосуються арешту криптовалют з метою збереження речових доказів відповідно до статей 98 та 170 Кримінально-процесуального кодексу України і недопущення їх зникнення (перетворення). Наприклад, ухвала Печерського районного суду м. Києва від 05 серпня 2021 року у справі № 757/41966/21-к про арешт криптовалют у великих розмірах на біржах KUNA та Binance (562 300 USDT і 603 400 USDT) [18]; рішення Печерського районного суду м. Києва від 22 лютого 2024 року у справі № 757/7985/24-к (ухвала № 117258877) про арешт віртуальних активів (USDT) на криптогаманцях і акаунтах Binance на суму 1 350 700 USDT [18]. Ці рішення підтверджують, що навіть за відсутності спеціального закону можуть застосовуватися класичні забезпечувальні інструменти до криптовалют та її визнання майном (речовим доказом) для цілей арешту.

Іншою особливістю є та, що якщо буде доведено зв'язок криптовалют з кримінальним правопорушенням і можливість її використання як речового доказу, то суд може відмовити у скасуванні арешту (прикладом є рішення Печерського районного суду м. Києва № 760/17139/23 від 10 серпня 2023 року [19]. Також окремими судовими рішеннями був скасований арешт USDT (зокрема, у справі Печерського районного суду м. Києва № 760/15406/23 від 31 серпня 2023 року через «відсутність правового статусу криптовалют в Україні [19]. Зазначене підкреслює потребу в підготовці Вищим антикорупційним судом (далі – ВАКС) Верховного Суду узагальнених та уніфікованих мотивувальних стандартів та методичних рекомендацій.

Накладення арешту на віртуальні активи (із прямим зазначенням адрес (ID акаунтів) і сум у резолютивній частині судової ухвали) свідчить про реалістичність такого арешту та суттєво підвищує ймовірність ефективного захисту. Однак зазначене вимагає підготовки доказової бази (фіксації хешів транзакцій, листування з біржами, використання журналів доступу й витягів із блокчейн-трасування тощо) для детальної технічної аргументації зв'язку криптовалют із правопорушенням та співпраці судових і правоохоронних органів з провайдерами на підставі ухвал про арешт.

Окрім того, має місце використання біткоїнів як предмета неправомірної вигоди у корупційних провадженнях (наприклад, рішення ВАКС від 30 листо-

пада 2023 року про накладення арешту на криптоактиви колишнього Голови Держспецзв'язку (~1,2 млн USDT, TRX, BTC [20], вирок ВАКС від 14 листопада 2024 року про використання біткоїнів як предмета неправомірної вигоди у справі народного депутата А. Одарченка)[21].

Отже, судова практика підтверджує сприйняття криптоактивів як «майна» і «речових доказів» для цілей арешту і подальшої реституції, що вимагає подальшої гармонізації з MiCA, TFR і податковими режимами прозорості (з урахуванням майбутніх правил обміну даними. Зазначене може значно підвищити передбачуваність для провайдерів і якості захисту прав користувачів.

**Висновки і перспективи подальших досліджень.** Таким чином, процедура захисту прав учасників правовідносин з обігу криптовалюти через не набрання чинності Законом № 2074-IX базується на відповідних нормах іншого законодавства (наприклад, Законів України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», «Про платіжні послуги», Кримінально-процесуального кодексу України тощо). Це дозволяє судам накладати арешт на криптоактиви як майно і речові докази, але залишає прогалини у превенції, розкриттях і поверненні активів у разі кастодіальних збоїв. Натомість ЄС у MiCA та TFR уже встановив для емітентів ART, EMT та CASP чіткі вимоги до авторизації, управління ризиками, IT-безпеки, сегрегації клієнтських активів, процедур розгляду скарг і повноважень нагляду; визнав криптоактиви об'єктом речово-правового захисту.

Тому доречною є гармонізація українського законодавства з MiCA та TFR і майбутніми податковими стандартами (CARF/DAC8) шляхом: запровадження ліцензування VASP/CASP з інтегрованими AML-процедурами; управління інцидентами та повідомлення про порушення безпеки; запровадження механізму нагляду шляхом приписів, штрафів і відкликання дозволів; ухваленням методичних рекомендацій для судів щодо арешту криптоактивів, фіксації доказів (хеші транзакцій, листування з біржами, журнали доступу, результати блокчейн-трасування) і взаємодії з провайдерами.

Із урахуванням зазначеного та шляхом внесення змін до Закону № 2074-IX, Податкового кодексу України, іншого законодавства в Україні можна запровадити сучасну модель захисту прав учасників правовідносин з обігу криптовалюти, аналіз якої є перспективним напрямом досліджень.

### *Література*

1. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. URL : <https://zakon.rada.gov.ua/laws/show/2074-20#Text>
2. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets (MiCA). EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>
3. EBA. Guidelines on customer due diligence and ML/TF risk factors for crypto-asset service providers (EBA/GL/2023/15), (January 2024). URL: <https://www.eba.europa.eu>
4. AA v Persons Unknown [2019] EWHC 3556 (Comm) – judgment (High Court). Judiciary UK. URL: <https://www.judiciary.uk>
5. FCA. PS23/6: Financial promotion rules for cryptoassets (08 червня 2023). URL: <https://www.fca.org.uk/publications/policy-statements/ps23-6-financial-promotion-rules-cryptoassets>

6. FCA. FG23/3 Finalised Guidance on cryptoasset financial promotions та супровідні матеріали (2023–2024). URL: <https://www.fca.org.uk/publications/fg23-3-finalised-non-handbook-guidance-cryptoasset-financial-promotions>
7. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
8. LMN v Bitflyer Holdings Inc & Ors [2022] EWHC 2954 (Comm) – Approved Judgment PDF. The National Archives. URL: <https://caselaw.nationalarchives.gov.uk>
9. Fetch.ai Ltd & Ors v Persons Unknown [2021] EWHC 2254 (Comm). Judiciary/BAILII. URL: <https://www.bailii.org>
10. D'Aloia v Persons Unknown & Ors [2022] EWHC 1723 (Ch). Judiciary UK. URL: <https://www.judiciary.uk>
11. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06 грудня 2019 року № 361-IX. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text>
12. Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text>
13. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05 жовтня 2017 року № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
14. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
15. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
16. Council Directive (EU) 2023/2226 of 17 October 2023 (DAC8) – Crypto-Asset Reporting. EUR-Lex. URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_2023\\_2226](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_2023_2226)
17. Ільченко М. Г. Суб'єкти фінансового моніторингу обігу криптовалют в Україні та їх повноваження: фінансово-правовий аспект. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. № 81(2). С. 149–154.
18. Ухвала Печерського районного суду м. Києва у справі № 757/41966/21-к від 05 серпня 2021 року. URL: <https://verdictum.ligazakon.net/document/98891298>.
19. Bargaen Law Firm. «Binance, USDT і кримінальний процес: судова практика щодо віртуальних активів» (21 червня 2025 року). URL: <https://bargaen.com.ua/2025/06/21/binance-usdt-i-kriminalnyj-protses-sudova-praktyka-shhodo-virtualnyh-aktyviv/> Юридична фірма BARGEN+1
20. Суд арештував криптовалюту ексголови Держспецзв'язку. URL: [https://lb.ua/society/2023/11/30/586863\\_sud\\_areshtuvav\\_kriptovalyutu.html](https://lb.ua/society/2023/11/30/586863_sud_areshtuvav_kriptovalyutu.html)
21. Хабарі в біткоїнах: справа нардепа Андрія Одарченка». URL: <https://hacc-decided.ti-ukraine.org/uk/cases/42023000000001295>

## Анотація

**Ільченко М. Г. Захист прав учасників правовідносин з обігу криптовалют крізь призму українських реалій та зарубіжного досвіду.** – Стаття.

У статті розглянуто механізм захисту прав учасників правовідносин з обігу криптовалют. Визначено особливості його правового регулювання, пов'язану із не набранням чинності Закону України «Про віртуальні активи» і який на сьогодні базується на положеннях іншого законодавства України та має враховувати законодавство ЄС і окремих зарубіжних країн із цього питання.

Відповідно до документів ЄС визначено права та обов'язки суб'єктів аналізованих правовідносин – споживачів, інвесторів, провайдерів послуг з віртуальними активами (криптоактивами) (VASP (CASP), органів нагляду. З'ясовано, що у Регламенті (ЄС) 2023/1114 (MiCA) визначено порядок розгляду скарг, повноваження органів нагляду тощо, а у Регламенті (ЄС) 2023/1113 (TFR) – обов'язок супроводжувати транзакції ідентифікаційними даними відправника й одержувача та порогів верифікації для операцій. Виокремлено коло прав та обов'язків інвесторів (споживачів), емітентів токенів, правовий статус провайдерів послуг із віртуальними криптоактивами (VASPs та CASPs). Проаналізовано механізми відновлення порушених прав за законодавством ЄС, Великої Британії, США.

Визначено правовий статус реальних (можливих) учасників аналізованих правовідносин за законодавством України: операторів обміну, кастодіальних сервісів, провайдерів переказів; надавачів та користувачів платіжних і електронних послуг; власників криптоактивів тощо. Зроблено висновок,

що наслідком порушення системи охоронюваних прав учасників правовідносин з обігу криптовалюти є настання майнових та процесуальних наслідків та потреба у застосуванні визначених механізмів відновлення.

Проаналізовано вітчизняну судову практику та проблеми захисту прав учасників правовідносин з обігу криптовалют. Запропоновано для запровадження сучасної моделі такого захисту внести зміни до Закону України «Про віртуальні активи», Податкового кодексу України, гармонізувавши їх норми з MiCA, TFR і майбутніми податковими стандартами (CARF/DAC8) шляхом запровадження (з-поміж іншого) ліцензування VASP та CASP, AML-процедур, механізму нагляду.

*Ключові слова:* криптовалюта, правове регулювання, фінансово-правове забезпечення, Закон України «Про віртуальні активи», правовідносини з обігу криптовалют, захист прав учасників правовідносин з обігу криптовалют.

## Summary

**Ilchenko M. H. Protection of the rights of participants in legal relations on the circulation of cryptocurrencies through the prism of Ukrainian realities and foreign experience. – Article.**

The article examines the mechanism for protecting the rights of participants in legal relations related to the circulation of cryptocurrencies. The peculiarity of its legal regulation is determined, which is associated with the non-entry into force of the Law of Ukraine "On Virtual Assets" and which is currently based on the provisions of other Ukrainian legislation and must take into account the legislation of the EU and certain foreign countries on this issue.

In accordance with EU documents, the rights and obligations of the subjects of the analyzed legal relations are determined – consumers, investors, virtual asset (cryptoasset) service providers (VASP (CASP), supervisory authorities. It was found that Regulation (EU) 2023/1114 (MiCA) defines the procedure for considering complaints, the powers of supervisory authorities, etc., and Regulation (EU) 2023/1113 (TFR) defines the obligation to accompany transactions with the identification data of the sender and recipient and verification thresholds for operations. The range of rights and obligations of investors (consumers), token issuers, and the legal status of virtual cryptoasset service providers (VASPs and CASPs) are identified. The mechanisms for restoring violated rights under the legislation of the EU, Great Britain, and the USA are analyzed.

The legal status of real (possible) participants in the analyzed legal relations under the legislation of Ukraine is determined: exchange operators, custodians services, transfer providers; providers and users of payment and electronic services; owners of crypto assets, etc. It is concluded that the consequence of a violation of the system of protected rights of participants in legal relations on the circulation of cryptocurrency is the occurrence of property and procedural consequences and the need to apply certain recovery mechanisms.

The domestic judicial practice and problems of protecting the rights of participants in legal relations on the circulation of cryptocurrency are analyzed. It is proposed to introduce a modern model of such protection by amending the Law of Ukraine "On Virtual Assets", the Tax Code of Ukraine, harmonizing their norms with MiCA, TFR and future tax standards (CARF / DAC8) by introducing (among other things) VASP and CASP licensing, AML procedures, and a supervision mechanism.

*Key words:* cryptocurrency, legal regulation, financial and legal support, Law of Ukraine "On Virtual Assets", legal relations on the circulation of cryptocurrencies, protection of the rights of participants in legal relations on the circulation of cryptocurrencies.

Дата надходження статті: 28.09.2025

Дата прийняття статті: 24.10.2025

Дата публікації: 27.11.2025