ПРОБЛЕМИ ПРАВООХОРОННОЇ ТА ПРАВОЗАХИСНОЇ ДІЯЛЬНОСТІ

УДК 343.222.4(477)
DOI https://doi.org/10.32782/2521-6473.2024-3.12

Ш. Б. Давлатов, кандидат юридичних наук, доцент,
доцент кафедри правоохоронної діяльності
Університету митної справи та фінансів

А. В. Подгорна, здобувачка вищої освіти ІІ рівня
Університету митної справи та фінансів

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА НЕЗАКОННЕ ПРИВЛАСНЕННЯ ВІРТУАЛЬНИХ АКТИВІВ

У статті здійснено комплексний аналіз правового статусу віртуальних активів, зокрема, розглянуто необхідність та стратегії кримінально-правового захисту таких об'єктів. Оскільки такі об'єкти права власності з'явились ще нещодавно і не кожен готовий сприймати віртуальну власність серйозно, ми маємо намір спробувати пояснити всю важливість захисту віртуальної власності від незаконних посягань, акцентуючи увагу на її економічному значенні. Розглянуто властивості, класифікацію та потенційні ризики для віртуальних активів. Особливу увагу приділено ризикам, які можуть бути пов'язані з неправомірним посяганням на віртуальні активи як об'єкту цивільного права. Оскільки віртуальні активи активно інтегруються в бізнес – процеси, важливо виявити їх роль як інструментів інвестування та механізму обміну, висвітлено проблематику кримінально правової охорони віртуальних активів, зокрема їх значення для розвитку економіки.

У статті зазначається що право власності на віртуальний актив є зовсім новим явищем, яке потребує чіткого особливого юридичного регулювання. Звертається увага на проблему юридичної невизначеності змісту право власності на віртуальний актив в науковій спільноті. Обґрунтовується необхідність законодавчого регулювання віртуальних активів та постійного вдосконалення роботи з ними для забезпечення правової визначеності, та за допомогою проведення спеціальних курсів підвищення кваліфікації для правоохоронних органів.

Зроблено висновок, що теперішній стан захисту віртуальних активів від кіберзлочинності не відповідає вимогам сьогодення. Доведено, що міжнародна співпраця та впровадження новітніх технологій є ефективним засобом боротьби з кіберзлочинністю. Зазначається, що без належного комплексного та системного регулювання віртуальної власності неможливо ефективно захистити права та інтереси громадян в умовах стрімкого розвитку технологій.

Ключові слова: *віртуальні активи, правове регулювання, віртуальна власність, кримінальна відповідальність, кіберзлочин, міжнародне співробітництво, віртуальна ігрова власність, судова практика, кримінальне правопорушення, кібербезпека, віртуальні ігрові активи, віртуальна ігрова власність.*

Sh. B. Davlatov, A. V. Podhorna. Criminal liability for the illegal appropriation of virtual gaming assets

In the article was made a complex analysis of the legal status of virtual gaming assets and examined in details the necessity of criminal legal protection. The article highlights and provides an detailed overview of features of virtual assets, ways of their classification and potential threats to their preservation. Particular attention was paid to risks related to unlawful infringement of ownership of virtual assets. In the article was examined in detail the issues faced by law enforcement agencies and owners of virtual assets during the collection of evidence and prosecution for cybercrimes, connected to virtual assets. Also was considered the potential ways of further use of illegally gained virtual assets by offenders. Due to this information, were made evaluation of national and international politics in combating crimes such as cybercrimes, money laundering, terrorism financing, and the proliferation of weapons of mass destruction. Another important point in the article is the attention to the shortcomings and problems of this combating, and different proposals and motivation for their elimination. In the article was mentioned that virtual property is a completely new phenomenon for legal authorities that requires clear special legal regulation. The article draws attention to the problem of legal uncertainty of the content of virtual property among scientists. The author substantiated the need for legislative regulation of virtual assets and continuous improvement of work with them through special courses for law enforcement agencies. Also, in the article was made the conclusion that the current state of protection of virtual assets from cybercrime does not meet the requirements of today and in connection to this it was proved that international

cooperation and the introduction of new technologies are effective methods of combating cybercrime. Finally, in the article was noted that without proper comprehensive and systematic regulation the issues of virtual property, it would be impossible to protect the rights and interests of citizens and government.

Key words: *virtual assets, legal regulations, virtual property, criminal liability, cybercrime, international cooperation, virtual gaming property, judicial practice, criminal offence.*

Постановка проблеми. Людина за своєю природою прагне продемонструвати свою індивідуальність і відокремитись від маси. Для цього вона вдається внесення коректівів у своє життя. Наприклад, граючи в відео-гру, людина створює собі унікального персонажа, купує різні предмети, зброю, інші елементи. Вона прагне до соціальної взаємодії, ділитися своїми ігровими досягненнями та активами з іншими людьми, отримуючи визнання серед інших гравців, проявляючи свою творчість, і в результаті отримує емоційне задоволення. Це детальніше описують у своїй науковій праці Дж. Клеггорн та М. Д. Гріффітс. [13].

Акаунт, фінанси, облікові записи, ігрові предмети, ігрова валюта та інші цифрові об'єкти стають віртуальним активом, який потребує захисту та регулювання. Адже коли речі набувають мати такі риси, як унікальність, рідкість, попит, культурне значення, історичність, естетичність, інвестиційний потенціал, впливовість, прибутковість, з'являються охочі володіти та розпоряджатися таким майном. Але не всі люди є доброчесними, високоморальними, і тому, з різних причин, вдаються до неправомірного привласнення віртуальних активів чи інших кримінальних правопорушень, пов'язаних з шахрайством та кіберзлочинністю. З розвитком ігрової індустрії цінність віртуальних активів зросла, зокрема й через значні фінансові витрати на придбання гри та її доповнень. Постає питання: як захистити право власності на віртуальні активи та як ефективно вести боротьбу з кіберзлочинністю, фінансуванням тероризму та поширенням зброї масового знищення.

Новизна теми наукової статті полягає у висвітленні правової природи віртуального ігрового активу, його особливий статус, зокрема, в складі кримінального правопорушення, складності доведення доказів, боротьби з такими правопорушеннями, а також механізмів вдосконалення системи захисту права власності на віртуальні активи та забезпечення правопорядку.

Аналіз останніх досліджень та публікацій. Питання віртуальної власності у своїй працях розглядали багато вчених, серед яких можна виділити таких, як Булеца С. Б., Еннан Р., Сліпченко С. О, Горобець Н. О., Співак О. М., Бутнік-Сіверський О., Некіт К. Г., Овсієнко О. В., Радутний О. Е., Шкалебей В. А., Добровольська В. В., Однак, питання захисту права власності на віртуальні активи та боротьби з кіберзлочинами на сьогодні залишається переважно не вивченим.

Метою статті є дослідження визначення статусу віртуальних активів, зокрема, у контексті кримінального правопорушення, оцінка ефективності боротьби з такими правопорушеннями, виявлення прогалин та формулювання пропозицій щодо вдосконалення механізму захисту права власності на віртуальні активи, а також боротьби з кіберзлочинністю, фінансуванням тероризму та поширенням зброї масового знищення.

Виклад основного матеріалу. Люди полюбляють відпочинок, чимало людей для цього обирають онлайн-ігри. Це чудова можливість відволіктись від буденного життя та зануритися у віртуальний світ, розвивати свого персонажа, здобувати ігрову валюту та предмети. Процес вирішення ігрових завдань та досягнення результату приносить людям задоволення. Деякі гравці готові витрачати чимало зусиль, часу та власних коштів для цього. Поряд з чесними гравцями існують і ті гравці, які хочуть нечесним шляхом досягти успіху в грі, а також ті, які готові порушувати правила заради власного збагачення, помсти, хуліганства, визнання, впливу, розваги та ідеологічних мотивів. Виникає потреба в захисті права власності на віртуальні ігрові активи та забезпеченні загального правопорядку. Слід проаналізувати юридичну природу такої власності та чи підлягає вона кримінально-правовому захисту.

В Україні законодавчо було запропоновано визначення поняття «віртуальні активи» у Законі України «Про віртуальні активи» від 01.01.2024, який наразі не набрав чинності, де віртуальний актив визначено як нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів. Віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав [7]. Також інше визначення віртуальних активів подано в Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення» від 23.09.2024, де віртуальний актив визначено як цифрове вираження вартості, який можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних чи інвестиційних цілей [8].

Віртуальний актив, відповідно рекомендацій FATF, – це цифрове відображення вартості, яке може бути використане в торгівлі або передачі у електронному форматі і може використовуватися для здійснення платежів та інвестицій. До Віртуальних активів не належать цифрові представлення фіатних валют, цінних паперів, та інших фінансових активів [14, с. 137]. Таким чином FATF підкреслю, що віртуальні активи є новою, унікальною категорією зі своїми унікальними властивостями.

Тема віртуальних активів є відносно новою і науковці ще не сформулювали єдиного підходу до визначення термінології. Наслідком цього є юридична невизначеність, ускладнення процесів притягнення

до відповідальності, нестабільність рівня захисту, зловживання ситуацією з боку правопорушників, нестабільність ринку, неефективність регулювання процесів, ускладнення міжнародного співробітництва.

Віртуальні активи класифікуються за критерієм забезпеченості реальними активами на: забезпеченні (цифрові облігації, токенізовані активи, стейблкоїни, забезпечені криптовалюти, токени, забезпечені активами), та незабезпечені (ігрові предмети, криптовалюта, токени, криптотовари, криптовалюти з фіксованою ціною, які не підкріплені реальними активами) [7]. Співак О. М. у своїй роботі довів, що «віртуальними предметами, які можуть бути віртуальним майном у грі є артефакти (екіпірування віртуальних персонажів), віртуальні простори (наприклад, острови) та віртуальні персонажі (аватари) [10, с. 419].

Питання юридичної природи віртуальних ігрових активів є доволі спірним для вчених завдяки свої властивостям. Адже віртуальна ігрова власність й досі сприймається лише як засіб для покращення ігрового процесу. Наразі, з розвитком технологій, людство почало сприймати віртуальне ігрове майно як продукт їхньої праці. Ці речі почали мати реальну грошову цінність, яка формується з витраченого часу, зусиль, фінансових вкладень, а також через їх унікальність та рідкість в деяких випадках. Оскільки з'явились особи, зацікавлені у придбанні продуктів ігрової діяльності, з'явились і ті, хто готовий це запропонувати. Так зародились ринкові відносини у сфері віртуальних активів, але постає проблема з ідентифікацією суб'єктів таких правовідносин, їх статусу а також визначенням їх прав та обов'язків. Науковці закликають до створення актуального дієвого та перспективного законодавства, яке б врегулювало такі відносини повноцінно. Українська правова система також працює над врегулюванням цих питань, адже суди розглядаючи справи, визнають право власності на віртуальні ігрові активи.

Оскільки не всі користувачі відео-ігор є доброчесними, то багато з них вдаються до вчинення шахрайських схем, таких як: викрадення акаунтів, ігрових предметів, ігрової та реальної валюти, даних користувачів, введення в оману інших користувачів для подальших шахрайських схем, деякі вдаються до кіберзлочинів таких як: поширення та використання шкідливого програмного забезпечення для отримання несправедливої переваги у грі або з метою зробити гру непридатною для гри, атаки на сервери розробників, підробка сайтів, посилань. А деякі вдаються навіть до відмивання незаконно отриманих коштів та уникнення оподаткування. [1, с. 4]. Тому питання захисту віртуальної ігрової власності стає ключовою складовою забезпечення правопорядку в Україні та по всьому світі.

Відповідно до визначення кримінального правопорушення у ст.. 11 Кримінального кодексу України, кіберзлочини, пов'язані з віртуальними ігровими активами, є такими, оскільки ці правопорушення становлять суспільну загрозу, оскільки вони можуть завдати шкоду не лише окремим гравцям, а й компаніям, державам та суспільству вцілому [6]. Це може викликати великі збитки для індустрії, сприяти розповсюдженню шкідливого програмного забезпечення, витоку даних, відмивання грошей, фінансуванню тероризму та розповсюдженню зброї масового знищення, погіршення стану економіки. Через відсутність відповідного рівня регулювання відбувається ескалація злочинності та часто вимагається міжнародне тісне співробітництво правоохоронних органів. Хоча на думку Думчикова М. О та Репіна Д. А., прогнози високого ризику використання криптоактивів для фінансування тероризму та поширення зброї масового знищення є дещо перебільшеними, оскільки такий вид злочинності є досить традиційним і вони віддають перевагу фізичному пересуванню готівки, але ризик все ще залишається [4, с. 35–36].

В Українському кримінальному законодавстві кіберзлочини, пов'язані з віртуальними активами часто кваліфікують як шахрайство (заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою), а також застосовуються норми розділу XVI Кримінального кодексу України, що передбачає кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, де передбачені такі кіберзлочини, як незаконне втручання або злам комп'ютерів, створення, розповсюдження або збут шкідливого програмного забезпечення з метою протиправного використання, продаж та поширення конфіденційних даних, порушення правил експлуатації комп'ютерних пристроїв, що заподіяло шкоду, перешкоджання роботі комп'ютерних пристроїв шляхом здійснення DDos атак (масового надсилання великої кількості запитів) [5]. Тобто загалом кримінальне законодавство передбачає санкціонування основних видів кіберзлочинів, але ,все ж таки, потребує доопрацювання, уточнення та конкретики.

Але у п. 8 ст 1 Закону України «Про основні засади забезпечення кібербезпеки України» передбачено міжнародне співробітництво у сфері кібербезпеки, відповідно до укладених нею міжнародних договорів, що свідчить про прагнення України підвищити рівня кібербезпеки як на національному, так і на глобальному рівні і робить все можливе для цього [9]. Адже правопорушники можуть користуватись вразливістю системи, зокрема як це сталося у 2017 році, коли кібератака паралізувала тисячі комп'ютерних систем, допоки жертви не заплатили хакерам викуп у біткоїнах. Загальні збитки від цього нападу для лікарень, банків, підприємств оцінюються приблизно у 8 мільярдів доларів США по всьому світу. Подібних атак трапляється все частіше їх кількість та креативність тільки зростає [15, с. 3]. У світлі цього питання регулювання віртуальних активів стає особливо актуальним.

Булеца С. Б. та Тегза А. В. зазначають, що «віртуальна власність не кваліфікується як «майно» відповідно до права власності, але можуть бути захищені законодавством про інтелектуальну власність.

Пропонують розробити закон про постачальників послуг віртуальних об'єктів, яким би врегулювали відносини щодо реєстрації постачальників послуг віртуальних об'єктів, моніторингу їх діяльності, визначення прав та обов'язків осіб, які користуються такими об'єктами, ризики, пов'язані з використанням послуг віртуальних активів та вирішенням спорів, що виникають із контрактів та угод між постачальником послуг віртуальних активів та його клієнтами» [2, с. 92–93].

У притягненні до кримінальної відповідальності за кіберзлочини, пов'язані з віртуальними активами, перешкодою є складність визначення розміру нанесеної шкоди, доведення доказів і проблема ідентифікації осіб. Причинами на це є властивості віртуальних активів: правопорушники користуються повною анонімністю, VPN, чужими акаунтами та даними, соціальною інженерією для введення в оману гравців для досягнення своїх цілей, недостатнім рівнем обізнаності правоохоронних органів, складністю збору доказів або легкістю підробки чи видалення, недостатнім правовим регулюванням, недовірою жертв до правоохоронних органів, не синхронізованою правовою системою між різними країнами, застарілістю технологій правоохоронних органів. До такого висновку дійшли Яцик Т. П. і Шкалебей В. А. у своїй праці, та підкреслили, що моніторинг фінансових операцій, аналіз даних, виявлення тенденцій і ризиків, використання штучного інтелекту та аналітики, спрощення процесу розслідування сприяють забезпеченню ефективності виявлення, розслідування та попередження правоохоронними органами кримінальних правопорушень у сфері обігу віртуальних активів [12, с. 222–223].

Судова практика по всьому світу повільно адаптується до нових умов сьогодення, цією прогалиною користуються кіберзлочинці. Але це не привід для стагнації, прагнення до розвитку завжди приносить позитивні результати. Втрачаючи можливості, державні органи втрачають довіру громадян, фінанси, правопорядок та інші фактори. Швидко адаптуючись до реалій, країни стають новими лідерами в певних процесах. Як влучно вказує у своїй праці Р. Еннан: «…що рано чи пізно суди, а й слідом за ними й законодавці будуть змушені визнати реальність «віртуальної» власності» [5, с. 129].

Ленінський районний суд м. Запоріжжя у справі № 334/3046/22 про проведення обшуку в рамках кримінального провадження, яке стосується несанкціонованого збуту інформації з обмеженим доступом (стаття 361-2 Кримінального кодексу України), 5 серпня 2022 року ухвалив рішення залишити клопотання без задоволення, зазначивши про відсутність доказів [11]. Це рішення підтвердило існуючі складнощі в роботі з віртуальними активами, особливо у зборі доказів. Докази про незаконну діяльність з віртуальними активами легко підробити, видалити і важко підтвердити. Цей фактор ускладнює розслідування, і правопорушники користуються цим.

Орджонікіджевський районний суд м. Запоріжжя у справі № 335/3376/24 про несанкціоноване розпорядження інформації з обмеженим доступом (стаття 361-2 Кримінального кодексу України) 24 квітня 2024 року ухвалив вирок, затвердивши угоду про про визнання винуватості між прокурором та обвинуваченим у вчиненні кримінального правопорушення, визнав винуватим обвинуваченого та призначив покарання у вигляді штрафу [3]. Це рішення продемонструвало тенденцію до підвищення рівня боротьби з кіберзлочинністю та прагнення правоохоронних органів забезпечити правопорядок в Україні. Але також це рішення продемонструвало необхідність проведення консультацій, психологічної реабілітації та тренінгів, проведення навчання для громадян, та, можливо, активно залучати до легальної роботи фахівців в сфері ІТ, які займались кіберзлочинністю.

Захист права власності на віртуальне ігрове майно здійснюється за допомогою чіткої політики захисту, користування (права та обов'язки користувачів) та створення політики безпеки. Рекомендується користуватись двохфакторною автентифікацією, автентифікацією за допомогою біометричних даних, регулярним оновленням паролів та слідкувати за IP-адресою. Постачальники послуг мають надати можливість зберігати дані користувачів за допомогою шифрування, використовувати спеціальні програми для автоматичного виявлення підозрілих користувачів та IP-адрес, та блокувати у разі необхідності. Також бажано, щоб постачальник послуг регулярно оновлював програмне забезпечення та усував вразливі місця гри. Бажано, якщо постачальник працює зі сторонніми постачальниками (платіжна система, хостинг, захист від кібератак), то йому варто укладати договір з чітким визначенням прав та обов'язків сторін, відповідальності за безпеку та конфіденційність.

Алгоритм реагування на порушення порядку гри має включати постійний моніторинг, виявлення підозрілих користувачів, оцінка потенційного розміру збитків, блокування користувачів у разі необхідності, компенсація збитків, аналіз інцидентів із зазначенням передумов, мотивів та наслідків, та сформувати відповідні рекомендації для запобігання подібним ситуаціям в майбутньому.

Користувачі мають звертатися до суду та правоохоронних органів за потреби, однак також способами вирішення таких спорів можуть стати арбітраж або медіація, якщо судовий розгляд виявиться неефективним, невигідним, але повноцінно кримінальне розслідування вони не можуть забезпечити.

Кіберзлочинність набуває транскордонного характеру, постає загроза не тільки для окремих країн, але й для всієї міжнародної спільноти. Контролювати ситуацію вдається завдяки тісній міжнародній співпраці. Міжнародні організації сприяють цьому, встановлюючи стандарти, проводячи навчання, координацію

та обмін інформацією. ООН активно бере участь у боротьбі з кіберзлочинністю на глобальному рівні, зокрема, Спеціальний комітет ООН з кіберзлочинності 8 серпня 2024 року схвалив проєкт глобальної Конвенції проти кіберзлочинності, який ще мають підтримати країни-члени під час голосування. Ця конвенція може стати першою в історії міжнародною конвенцією про кіберзлочинність. Європейська організація Markets in Crypto-Assets Regulation спрямовує свою діяльність на встановлення загальних правил ринку цифрових активів для фінансової стабільності та захисту інвесторів. Їх діяльність полягає у суворому нагляді за дотриманням постачальниками вимог захисту активів користувачів та несенням відповідальності у разі втрати криптоактивів інвесторів, відслідковуванням зловживань, пов'язаних з транзакціями і послугами. Центр скарг на злочини в інтернеті ФБР (IC3) працює на виявлення та запобігання злочинності в інтернеті, а також відновленням активів шляхом їх замороження. Інтерпол та Європол забезпечують обмін інформацією між національними правоохоронними органами, сприяють проведенню спільних операцій проти кіберзлочинності. Вони проводять тренінги, глобальні кампанії з підвищення обізнаності, надають технічні засоби, програмне забезпечення та інші системи, а також рекомендації щодо роботи з цифровими доказами. У 2005 році було засновано Будапештську конвенцію Ради Європи про кіберзлочинність для налагодження міжнародної співпраці, запобігання та боротьби з кіберзлочинами, а також гармонізації національного законодавства. Міжнародна група з протидії відмивання грошей (FATF) – глобальний орган з боротьби з відмиванням грошей та фінансування тероризму на глобальному рівні, але також він займається розробкою стандартів та рекомендацій щодо регулювання віртуальних активів, та схиляє країни до адаптації законодавства. Їх стандарти стали основою національного регулювання в багатьох країнах.

В перспективі вбачається, що боротьба з кіберзлочинністю набуває глобального уніфікованого регулювання на міжнародному рівні, активно розробляються стандарти регулювання віртуальних активів та гармонізується законодавство України відповідно до міжнародних стандартів. Така співпраця створить простіше для відслідковування спільне середовище для цифрових транзакцій та значно підвищить ефективність боротьби з кіберзлочинністю. Розробка ефективного сучасного законодавства, криміналізація нових форм кіберзлочинів, автоматизація контролю за транзакціями, а також тренування правоохоронних органів насамперед у віртуальних тренувальних середовищах для тестування тільки підкреслює згуртованість та серйозність такої боротьби.

Висновки і перспективи. Отже, віртуальні ігрові активи мають чітко регулюватися та захищатися від незаконних маніпуляцій кіберзлочинців. І дійсно, ігрові предмети мають цінність та їхня вартість тільки зростає. Варто пам'ятати про основні правила безпеки перебування в Інтернет-просторі, користуватись всіма рекомендаціями правоохоронних органів та спеціальних організацій. Держава також має сприяти захисту права власності на віртуальні активи та забезпечити правопорядок. Для цього вона має активно брати участь у міжнародному співробітництві, співпрацювати з міжнародним організаціями та виконувати необхідні вимоги та рекомендації для вдосконалення національної правової системи. Завдяки належному нормативно-правовому регулюванню суди зможуть ухвалювати більш ефективні рішення та сприяти розвитку кібербезпеки.

Можна зробити висновок, що у науковій статті було розглянуто статус віртуальних активів, їх характеристику, особливості їх юридичного захисту та використання. Розглянуто шляхи протидії кіберзлочинності та проаналізовано проблематику захисту прав і підтримки кібербезпеки. Також було підкреслено прагнення та перспективи розвитку української правової системи боротьби з кіберзлочинністю. Дана тема потребує більш детальної аналізу у новому науковому дослідженні.

Список використаних джерел:

1. Арзянцева Д. А., Захаркевич Н. П. Проблеми використання цифрових активів у діяльності віртуальних організацій. *Management and entrepreneurship in Ukraine: the stages of formation and problems of development.* 2019. № 1. С. 1–7. URL: https://science.lpnu.ua/ sites/default/files/journal-paper/2019/dec/20445/ arzyanceva.pdf (дата звернення: 28.09.2024).

2. Булеца С. Б., Тегза А. В. Захист віртуальної ігрової власності: національний та зарубіжний досвід. *Науковий вісник Ужгородського національного університету.* 2022. № 69. С. 89–93. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/254419/251643 (дата звернення: 28.09.2024).

3. Вирок Орджонікідзевського районного суду м. Запоріжжя № 335/3376/24. 24 квітня 2024. *Єдиний реєстр досудових рішень.* URL: https:// reyestr.court.gov.ua/Review/118605909 (дата звернення: 29.09.2024).

4. Думчиков М. О., Репін Д. А. Легалізація доходів, отриманих злочинним шляхом за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект. *Журнал східноєвропейського права. 2020.* № 82. С. 32–37. URL: https://essuir.sumdu.edu.ua/bitstream-download/ 123456789/86278/1/Dumchykov_cryptocurrency.pdf;jsessionid=16FE658B3E908970558B05BA9E3C0B1E (дата звернення: 28.09.2024).

5. Еннан Р. Правовий режим «віртуальної власності»: поняття, ознаки, сутність і правова природа. *Погляд науковця. 2019.* № 3. С. 123–131. 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/Tpiv_2019_3_14.pdf (дата звернення: 28.09.2024).

6. Кримінальний кодекс України: Закон України від 07.09.2024 р. № 3902-IX. *Відомості Верховної Ради України.* 2001. 29 черв. (№ 25–26). Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#Text (дата звернення: 28.09.2024).

7. Про віртуальні активи : Закон України від 01.01.2024 р. № 2074-IX. *Відомості Верховної Ради України.* 2023. 17 лист. (№ 15) С. 47. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 28.09.2024).

8. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 23.09.2024 р. № 3894-IX. *Відомості Верховної Ради України.* 2020. 19 черв. (№ 25) С. 5. URL: https://zakon.rada.gov.ua/laws/show/361-20#top (дата звернення: 28.09.2024).

9. Про основні засади забезпечення кібербезпеки : Закон України від 28.06.2024 р. № 3783-IX. *Відомості Верховної Ради України*. 2017. 10 лист. (№ 45) С. 42. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ conv#top (дата звернення: 28.09.2024).

10. Співак О. М. Віртуальні активи та он-лайн ігри: правове регулювання та питання захисту. *Право і суспільство. 2024.* № 2. С. 416–419. URL: http:// pravoisuspilstvo.org.ua/archive/2024/2_2024/60.pdf (дата звернення: 28.09.2024).

11. Ухвала Ленінського районного суду м. Запоріжжя № 334/3046/22. 25 серпня 2022. *Єдиний реєстр судових рішень.* URL: https:// reyestr.court.gov.ua/ Review/105629728 (дата звернення: 28.09.2024).

12. Яцик Т. П., Шкалебей В. А. Розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів. *Науковий вісник Ужгородського національного університету*. 2023. № 80 (2). С. 219–223. URL: https:// visnyk-juris-uzhnu.com/wp-content/uploads/2024/01/36-1.pdf (дата звернення: 28.09.2024).

13. Cleghorn J., Griffiths M. D. Why do gamers buy "virtual assets" ? An insight in to the psychology behind purchase behaviour. *Digital education review. 2015.* № 27. P. 98–117. URL: https://www.researchgate.net/publication/276265219_Why_do_gamers_buy_virtual_assets_An_insight_in_to_the_psychology_behind_purchase_behavior (дата звернення: 28.09.2024).

14. Financial Action Task Force. International standards on combating money laundering and financing of terrorism and proliferation. *Paris*, 2023. P. 145. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/ FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (дата звернення: 28.09.2024).

15. Financial Action Task Force. Virtual Assets: What? When? How? *Easy guide to FATF standards and methodology.* P. 8. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/brochures/FATF-Booklet_VA.pdf (дата звернення: 27.09.2024).