УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2025-1/184

КІБЕРЗЛОЧИННІСТЬ У ФІНАНСОВІЙ СФЕРІ: ПРЕДИКАТНА РОЛЬ, ІНСТРУМЕНТИ ЛЕГАЛІЗАЦІЇ ТА ПРОБЛЕМАТИКА ДОКАЗУВАННЯ

CYBERCRIME IN THE FINANCIAL SECTOR: PREDICATE ROLE, LEGALIZATION TOOLS AND ISSUES OF PROOF

Кутепов І.О., аспірант заочної форми навчання докторантури та аспірантури
Одеський державний університет внутрішніх справ

Цифровізація економіки, глобалізація фінансових інструментів і стрімкий розвиток криптотехнологій докорінно трансформували не лише законну господарську діяльність, але й механізми вчинення злочинів у сфері легалізації доходів та ухилення від сплати податків.

У поданому дослідженні здійснено комплексний аналіз трансформації кіберзлочинності у сфері легалізації доходів, отриманих злочинним шляхом, та ухилення від сплати податків в умовах цифрової економіки.

Особливу увагу приділено подвійному характеру кібердіянь, які можуть виступати як предикатними злочинами, так і інструментами подальшої легалізації.

Розкрито механізми використання криптоактивів, децентралізованих фінансових платформ, фіктивних онлайн-суб'єктів та анонімізованих сервісів для обходу регуляторних обмежень.

Зроблено акцент на кримінологічному портреті сучасного кіберзлочинця, складнощах його ідентифікації, а також структурній латентності цифрових злочинів.

У межах роботи окреслено соціально-економічні, нормативно-правові, психологічні та технічні причини вчинення кіберзлочинів у податковій та фінансовій сферах.

Окрема увага присвячена проблемам збору, верифікації та процесуального долучення цифрових доказів у кримінальному провадженні, що ускладнюється як міжнародними бар'єрами, так і відсутністю технічної компетентності в органів досудового розслідування.

Матеріали дослідження мають значення для формування національної політики цифрової безпеки, удосконалення кримінального процесуального законодавства, розробки механізмів міжнародного правового співробітництва та підготовки кадрів для спеціалізованих підрозділів із розслідування кіберекономічних правопорушень.

Метою статті є комплексне дослідження кіберзлочинності як феномену, що виконує подвійну функцію у механізмах легалізації доходів, отриманих злочинним шляхом, та ухилення від сплати податків, з урахуванням сучасних цифрових інструментів і глобального технологічного середовища. У межах цього дослідження передбачається проаналізувати типові способи використання криптоактивів та децентралізованих фінансових платформ у злочинній діяльності, визначити основні кримінологічні характеристики сучасного кіберзлочинця, розкрити причини та умови вчинення таких правопорушень, а також виявити прогалини національного кримінального й процесуального законодавства, що перешкоджають ефективному розслідуванню зазначених злочинів.

Ключові слова: кіберзлочинність, фінансова злочинність, легалізація доходів, ухилення від сплати податків, криптоактиви, цифрові докази, міжнародне правове співробітництво, предикатні злочини.

The digitalization of the economy, the globalization of financial instruments and the rapid development of crypto technologies have radically transformed not only legitimate business activities, but also the mechanisms for committing money laundering and tax evasion crimes.

The present study provides a comprehensive analysis of the transformation of cybercrime in the field of money laundering and tax evasion in the digital economy.

Particular attention is paid to the dual nature of cyber activities, which can act as both predicate crimes and tools for further legalization.

The mechanisms of using cryptoassets, decentralized financial platforms, fictitious online entities and anonymized services to circumvent regulatory restrictions are revealed.

Emphasis is placed on the criminological portrait of a modern cybercriminal, the difficulties of his identification, and the structural latency of digital crimes.

The author outlines the socio-economic, regulatory, psychological and technical reasons for committing cybercrime in the tax and financial spheres.

Particular attention is paid to the problems of collection, verification and procedural admission of digital evidence in criminal proceedings, which is complicated by both international barriers and the lack of technical competence of pre-trial investigation bodies.

The research findings are important for shaping the national digital security policy, improving criminal procedure legislation, developing mechanisms for international legal cooperation and training of personnel for specialized units for investigating cybereconomic offenses.

The purpose of the article is to provide a comprehensive study of cybercrime as a phenomenon which performs a dual function in the mechanisms of money laundering and tax evasion, taking into account modern digital tools and the global technological environment. This study aims to analyze the typical ways in which cryptoassets and decentralized financial platforms are used in criminal activities, identify the main criminological characteristics of a modern cybercriminal, reveal the causes and conditions of such offenses, and identify gaps in national criminal and procedural legislation that impede the effective investigation of these crimes.

Key words: cybercrime, financial crime, money laundering, tax evasion, crypto assets, digital evidence, decentralized financial platforms, fictitious transactions, international legal cooperation, predicate offenses, digital identification, investigative intervention in the virtual environment.

Виклад основного матеріалу. У сучасних умовах цифрової трансформації національних економік, фінансових ринків і соціальних комунікацій відбувається глибока еволюція способів учинення кримінально караних діянь, що мають економічний характер.

Одним з ключових векторів цієї трансформації є впровадження технологічних інструментів, які з одного боку сприяють прозорості та ефективності управління, а з іншого – створюють безпрецедентні можливості для обходу законодавчих обмежень та розгортання високотехнологічних форм злочинності.

На Конгресі ООН 2000 року по попередженню злочинності і поводженню з правопорушниками сформульовано два види кіберзлочинів:

– у вузькому розумінні (комп'ютерні злочини): будь-яке протиправне діяння, що здійснюється шляхом електронних операцій з метою подолання захисту комп'ютерних систем і обчислюваних ними даних;

– у широкому розумінні (злочини з використанням комп'ютерів) прийнято розуміти як протиправне діяння, яке вчиняється шляхом, або у зв'язку з комп'ютерною системою, або у зв'язку з комп'ютерною системою або мере-

жею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [1, с.152].

Особливо це стосується сфер легалізації доходів, отриманих злочинним шляхом, та ухилення від сплати податків, де кіберзлочинність виконує не допоміжну, а дедалі частіше – системоутворюючу функцію.

Кіберзлочинність у цьому контексті не обмежується традиційним розумінням як посягання на інформаційні ресурси, системи чи персональні дані. Натомість вона охоплює комплекс цифрово-опосередкованих дій, які забезпечують приховування злочинних доходів, створення фіктивних транзакцій, маскування бенефіціарних власників і транснаціональну циркуляцію капіталу поза межами законного регулювання. За оцінками експертів, латентність «комп'ютерних злочинів» у США сягає 80%, у Великобританії – 85%, у Німеччині – 75%, в Україні – понад 90%. За даними Symantec Security, міжнародної служби захисту від кіберзагроз, щосекунди 12 людей у всьому світі стають жертвами кібератак, і щороку в усьому світі реєструється близько 556 мільйонів кіберзлочинів, збитки від яких становлять більше 100 мільярдів доларів США [2, с. 46].

Використання шифрування, криптографічних протоколів, анонімних браузерів, віртуальних приватних мереж (VPN), а також криптовалютних гаманців із прихованою структурою власності дозволяє організованим злочинним угрупуванням ефективно інтегрувати легалізаційні механізми у цифрову інфраструктуру.

Особливої складності набуває аналіз подвійної правової природи кіберзлочину в контексті фінансових правопорушень, де він виступає одночасно як предикатний злочин, тобто первинне джерело незаконного доходу, так і як інструмент подальшої легалізації цих доходів.

У таких випадках саме кібердіяння створює первинне майнове благо злочинного походження, а подальше його включення у законний обіг відбувається через інші кібермеханізми – від створення фіктивного онлайн-бізнесу до підробки цифрових рахунків-фактур. Таким чином, кіберзлочинність виступає як джерелом коштів, так і середовищем для їх легалізації, порушуючи класичну модель розмежування між предикатним та похідним етапом злочинної діяльності.

Це ускладнює як побудову обвинувального акта, так і визначення моменту закінчення злочину в розумінні статті 209 Кримінального кодексу України, адже часто технічний інструмент, за допомогою якого відбувається легалізація, є ідентичним тому, за допомогою якого було вчинено первинне правопорушення.

Така правова невизначеність створює серйозні виклики для правоохоронної практики, оскільки потребує глибокого техніко-криміналістичного аналізу подій, які розгортаються у віртуальному просторі. У випадках податкових злочинів цифрові технології відкривають нові горизонти для агресивного податкового планування та технічного ухилення від сплати податків, зокрема через використання хмарних бухгалтерських платформ, електронного документообігу з модифікованими метаданими, фіктивних онлайн-продавців, бот-акаунтів, які генерують обіг для «скручування» ПДВ, а також через створення іноземних суб'єктів господарювання, що існують лише в цифровому середовищі.

При цьому особливу складність становить виявлення фактичного контролю над активами, які перебувають у розпорядженні осіб, котрі фізично знаходяться поза межами української юрисдикції. Правовий аналіз дозволяє констатувати, що національне законодавство, зокрема Кримінальний кодекс України, не завжди відповідає складності та гнучкості новітніх цифрових схем. Хоча стаття 209 Кримінальний кодекс України передбачає кримінальну відповідальність за легалізацію доходів, отриманих злочинним шляхом, а стаття 212 Кримінального кодексу України – за ухилення від сплати податків, ці норми часто залишають поза увагою цифрову специфіку інструментарію, який використовується злочинцями.

Наприклад, чинне законодавство не містить чіткої дефініції щодо злочинів, вчинених із використанням віртуальних активів або блокчейн-технологій, що створює серйозні бар'єри для кваліфікації дій і доведення вини в судовому процесі.

Кримінологічний аналіз дає підстави стверджувати, що кіберзлочинність у сфері економічних правопорушень є не лише інструментом, а й окремим ризиковим середовищем, у межах якого створюється нова типологія правопорушника: висококваліфікований IT-фахівець, здатний анонімізувати цифрові сліди, трансформувати походження активів та використовувати транскордонні платформи без залучення традиційної банківської системи.

Цей тип правопорушника не завжди входить у класичну модель «кримінального елемента», що додатково ускладнює профілактику і розслідування таких правопорушень. Так, Кузьменко О. В. у своєму дослідженні зазначає, що у криміналістичному аспекті особа кіберзлочинця має низку специфічних індивідуальних ознак , що обумовлені наявністю у таких осіб спеціальних знань та навичок у галузі інформаційних технологій, які використовуються ними для досягнення злочинного наміру [3, с.164]

У зв'язку з цим особливої актуальності набуває розробка комплексної державної політики цифрової кримінології, що має включати адаптацію кримінального законодавства до нових викликів, створення спеціалізованих підрозділів кібереконomічної розвідки, використання цифрових слідчих інструментів (digital forensics), а також активізацію міжнародного співробітництва у межах платформи Європолу, Інтерполу та Egmont Group.

Аналіз причин та умов кіберзлочинності, що безпосередньо впливає на вчинення легалізаційних і податкових злочинів, передбачає необхідність розгляду комплексу чинників – соціально-економічних, техніко-інфраструктурних, організаційних, нормативно-правових та психологічно-мотиваційних.

У їхньому сукупному впливі формуються сприятливі передумови для цифрового правопорушення, яке, своєю чергою, дедалі частіше виступає не просто у формі окремого діяння, а як елемент системного кримінального механізму.

На мікрорівні першопричин найчастіше постає висока технічна обізнаність правопорушників у поєднанні з відносною низькою правосвідомістю.

Для значної частини осіб, які вчиняють кіберзлочини у сфері легалізації доходів, фінансове шахрайство або податкове маніпулювання, характерним є не девіантний життєвий шлях, а технократична раціональність мислення, що базується на вмінні виявляти та експлуатувати прогалини у цифрових системах, обходити контрольні механізми та створювати алгоритми з прихованими каналами обігу ресурсів.

Це дозволяє таким правопорушникам діяти в межах ретельно сконструйованого кримінального дизайну, маскувати свою діяльність під технічні операції або аутсорсингові сервіси.

До ключових соціальних причин кіберзлочинності варто віднести зростаючу цифровізацію суспільства на тлі нерівномірного розвитку систем кібербезпеки.

Швидке проникнення електронних фінансових послуг, дистанційної ідентифікації, платіжних інструментів нового покоління та криптоактивів створює інституційну асиметрію між новими можливостями та спроможністю держав контролювати їх використання. Це спричиняє ситуацію, за якої злочинна ініціатива нерідко випереджає правозастосовну відповідь, а механізми цифрової звітності стають об'єктом маніпуляцій, підробок та технічної інтервенції.

Серед економічних чинників на перший план виходить висока прибутковість кіберзлочинної діяльності за відносно низького рівня ризику бути викритим, що створює позитивну мотивацію до повторного вчинення правопорушень.

В умовах глобального доступу до цифрових платформ, ринків даркнету, анонімних криптоплатформ, послуг хакерських угруповань на замовлення тощо – кібердіяння перестає бути локальною загрозою й набуває рис інфраструктурного підприємництва зі злочинним наміром.

Не менш важливою є нормативно-правова причина, яка полягає у тому, що значна частина цифрових технологій та інструментів, що використовуються при вчиненні кіберзлочинів, формально не підпадають під конкретні склади злочину в чинному кримінальному законодавстві.

Наприклад, маніпуляція хеш-ідентифікаторами у блокчейн-системі або створення токенів із фіктивним ринковим обігом можуть бути визнані правопорушеннями лише за умови наявності матеріального наслідку, тоді як сам процес підготовки та маскування лишається у «сірій зоні» кримінального права.

Сприятливою організаційною умовою є також недостатній рівень технічної спроможності органів досудового розслідування, відсутність доступу до глобальних інструментів кіберрозвідки, нестача аналітичних ресурсів та обмеженість міжнародного співробітництва у сфері цифрових розслідувань.

Нерідко злочинці користуються різницею у правових режимах юрисдикцій, «паркують» свої криптоактиви в офшорних хостингах, розміщують сервери за межами дії європейських регламентів або створюють псевдо-DAO (децентралізовані автономні організації) як ширми для грошових потоків.

Не можна не враховувати й психологічно-мотиваційні фактори, які включають ідеалізацію образу «хакера-аноніма» у молодіжній субкультурі, підкріплену поп-культурною глорифікацією кіберповстанців або криптоентузіастів. У поєднанні з анонімністю, дистанційністю та «відсутністю жертви у прямому сенсі» це сприяє етичній десенсибілізації до наслідків скоєного, а також раціоналізації порушення закону як технічної гри або змагання з державою. Таким чином, здійснення кіберзлочинів у контексті легалізаційних і податкових злочинів є наслідком переплетення складних міждисциплінарних факторів, які включають не лише кримінальні мотиви, але й глибші суспільні та інфраструктурні розриви, зокрема – між технологічною динамікою й інституційною інерцією. Ефективна протидія такій злочинності потребує розуміння не лише її зовнішніх проявів, але й системних причин, що створюють підґрунтя для її відтворення у глобалізованому цифровому середовищі. Популярною є думка, що збільшення кількості кіберзлочинів зумовлено низкою наступних факторів:

1) висока завантаженість правоохоронних органів, результатом чого є обмеженість ресурсів правоохоронних органів;

2) анонімність та глобальний характер кіберзлочинів, що викликає виникнення юрисдикційних питань;.

3) стрімкий технологічний прогрес;

4) брак кібергігієни, яка спричинена недостатньою обізнаністю користувачів про безпечну поведінку в Інтернеті та відсутністю відповідальності за недотримання кібергігієни [4, с. 665].

Очевидно, що така кримінологічна специфіка кіберзлочинця потребує особливого підходу з боку органів досудового розслідування. Ідентифікація особи, яка вчинила кіберзлочин, зокрема у сферах легалізації доходів та ухилення від оподаткування, є однією з найскладніших проблем сучасного кримінального процесу та криміналістики.

Ця складність зумовлена структурною невидимістю кіберзлочинця, що є прямим наслідком трьох чинників: анонімності цифрового середовища, делокалізації дій у кіберпросторі та високої технічної адаптивності самого правопорушника.

Типовий кіберзлочинець у сфері фінансової злочинності суттєво відрізняється від класичного образу злочинця: він діє дистанційно, часто через автоматизовані системи, використовує проксі, VPN, Tor-мережі, криптографічне шифрування і мультифакторну аутентифікацію.

Крім того, він може розміщувати сервери в юрисдикціях із високим рівнем правового захисту конфіденційності або навіть змінювати цифрові сліди, застосовуючи антифорензічні інструменти (anti-forensics tools), такі як disk wiping, log cleaners чи fake meta generators. Це створює об'єктивні перепони для збору електронних доказів і процесуального ототожнення особи. Крім того, кіберзлочин не завжди скоюється одноособово.

У випадках легалізації доходів, отриманих злочинним шляхом, або податкових махінацій цифрового типу, йдеться про розгалужені мережеві структури: платформи-обмінники, криптовалютні мікшери, анонімізовані платформи NFT, хакерські форуми з розподілом ролей (кодери, оператори, «відмивачі», адміністратори). В результаті – криміногенна фігура розчиняється у колективному суб'єкті, що суттєво ускладнює персональне притягнення до відповідальності. Також значення має те, що багато кіберзлочинців використовують легальні сервіси як інструменти злочинної діяльності: наприклад, реєстрація компаній у закордонних юрисдикціях, користування біржами, які не проводять KYC/AML перевірку, створення цифрових платіжних шлюзів тощо.

У таких умовах суб'єкт злочину не лише ховається за технічним бар'єром, а й діє в сірій зоні правомірності, що унеможливлює швидку кваліфікацію його дій як злочинних без глибокого техніко-правового аналізу.

На додаток до цього, відсутність універсальних міжнародних стандартів цифрової ідентифікації або єдиної транскордонної системи слідчої взаємодії (на кшталт інтероперабельної цифрової кримінальної бази даних) часто робить запити про міжнародну правову допомогу малоефективними або надмірно тривалими. В умовах, коли цифрові докази можуть бути видалені за лічені хвилини, часовий аспект між запитом і діями приймаючої сторони стає критичним фактором невдачі слідства.

Таким чином, кримінологічний аспект кіберзлочинця у фінансових правопорушеннях характеризується глибокою латентністю, технічною мінливістю, розподіленістю відповідальності та формальною законністю інструментарію, який використовується. Подолання цих складностей вимагає не лише високого рівня технологічної компетентності слідчих та експертів, а й переосмислення підходів до ідентифікації суб'єкта в кіберпросторі, включаючи створення гібридної концепції ідентифікації, яка поєднує цифрові сліди, поведінковий аналіз та юридичну презумпцію контролю.

У системі кримінального провадження щодо легалізації доходів, отриманих злочинним шляхом, або ухилення від сплати податків, поява криптоактивів суттєво трансформувала як характер злочинної поведінки, так і механізми її процесуального виявлення та доведення. Криптовалюти і токенізовані активи, будучи відносно новими інструментами фінансового обігу, функціонують у режимі високої технічної складності та юрисдикційної розмитості, що в сукупності створює значні перешкоди для ефективного розслідування.

У сучасних умовах цифрової економіки криптоактиви дедалі частіше використовуються не лише як засіб інвестування чи технологічної інновації, а й як ефективний інструмент приховування походження доходів, здобутих злочинним шляхом.

Як зазначає Білан І.А., криптовалюта, завдяки своїм сприятливим характеристикам та привабливості, все

частіше використовується у злочинних цілях та з метою фінансування тероризму. У світових масштабах фінансування терористичної діяльності за допомогою криптовалюти за останній постійно збільшується. Згідно звіту Chainalysis, у 2022 році терористичні організації та хакерські угруповання отримали тіньових майже $10 млрд. США саме завдяки криптовалютам [5 , с. 156].

Криптовалюти створюють принципово нову екосистему фінансового обігу, в якій відсутність централізованого регулювання, транскордонний характер транзакцій та анонімізаційні механізми забезпечують легке й маскувальне переміщення злочинного капіталу без традиційного фінансового посередництва.

Використання блокчейн-технологій дозволяє зловмисникам уникати залучення банківської системи чи формальних суб'єктів фінансового моніторингу. Легалізація коштів через криптоактиви реалізується шляхом включення їх до ланцюга цифрових транзакцій, що візуально не має ознак злочинного походження. Типовою практикою є змішування потоків через мікшерні сервіси, де десятки користувачів об'єднують свої транзакції задля унеможливлення ідентифікації джерела кожної з них. Додаткову складність становить використання криптовалют із підвищеним рівнем приватності, таких як Monero або ZCash, що технічно унеможливлюють виявлення адрес відправника та отримувача на рівні блокчейну.

Ще одним каналом є переміщення активів через децентралізовані фінансові платформи (DeFi), де користувачі можуть здійснювати обміни та кредитування без проходження жодної ідентифікації, а також створення візуально «ринкової» активності у вигляді торгівлі NFT або віртуальними токенами, які не мають реального економічного наповнення, але служать формальним засобом «відбілювання» активів.

При цьому легальне середовище використовується з метою формального обґрунтування вартості активів, що дозволяє конвертувати їх у фіатні гроші або інші законні форми власності. Складність боротьби з такими схемами полягає у тому, що навіть прозорість публічних блокчейнів, таких як Bitcoin, не гарантує юридичної ідентифікації особи. Без додаткових запитів до криптобірж або сервісів зберігання гаманців ідентифікувати бенефіціара транзакції практично неможливо.

При цьому значна частина інфраструктури обслуговується платформами, що не дотримуються процедур KYC або AML, а юрисдикційна фрагментованість регулювання дозволяє зловмисникам користуватись так званим нормативним арбітражем – переміщуючи активи між державами з м'яким або відсутнім регуляторним контролем. У цьому контексті особливу загрозу становить також поділ ринку на «чисті» та «брудні» криптоактиви, що формується внаслідок впровадження спеціалізованих систем перевірки походження токенів.

Головко К.В. зазначає, що дотримання правил AML у сфері віртуальних активів стикається з кількома проблемами. Однією з головних проблем є досягнення правильного балансу між конфіденційністю та дотриманням вимог. У той час як криптовалюти пропонують псевдонімність, правила AML вимагають ідентифікації користувачів, щоб запобігти зловживанням. Подолання цієї проблеми передбачає впровадження ефективних процедур «Знай свого клієнта» (KYC) та процесів перевірки особи. Ще однією проблемою є технічна складність блокчейн-мереж. Децентралізований характер цих мереж та використання цифрових гаманців представляють унікальні проблеми для моніторингу транзакцій та ведення обліку [6;с. 618].

Деякі криптобіржі використовують програмні інструменти для аналізу ланцюга транзакцій, тоді як інші декларують абсолютну конфіденційність та ідеологічний спротив будь-яким формам фінансового контролю, створюючи умови для безконтрольного обігу злочинного капіталу.

Правова проблема посилюється тим, що на міжнародному рівні відсутня уніфікована позиція щодо правового статусу криптовалют. Одні країни розглядають їх як активи, інші – як платіжні засоби, а ще деякі повністю ігнорують їх існування на законодавчому рівні. Це ускладнює ефективну протидію та унеможливлює створення сталого механізму запобігання легалізації через криптосередовище.

В зарубіжних країнах питання регулювання криптовалюти вирішується по різному. Так, у США криптовалюта визнається як майно, що є об'єктом оподаткування. Влада США регулює криптовалюти через законодавство про майнові права та протидію відмиванню грошей. В Китаї заборонено біржі криптовалют та ICO (ініціал-оферингів). Для Китаю є характерною певна обмеженість у використанні криптовалюти. Японія серед перших на законодавчому рівні визнала криптовалюту як законний засіб платежу. Також законодавство Японії досить детально регламентує криптовалюту та визначає її статус. Країни Європейського Союзу у більшості не визначають правовий статус криптовалют, а деякі країни-члени ЄС виробили власні підходи до закріплення статусу криптовалют. ЄС регулює використання криптовалютних активів за допомогою діяльності Європейського банку та Європейської комісії [7, с. 198].

Таким чином, криптоактиви у сучасному світі функціонують як високотехнологічна, анонімна і юридично пластична інфраструктура, що дозволяє не лише трансформувати злочинні доходи, але й інтегрувати їх у легальний обіг із мінімальним ризиком викриття. У зв'язку з цим ефективна протидія потребує не лише вдосконалення кримінального законодавства, але й налагодження міждержавного крипто-AML моніторингу, технологічної сумісності платформ контролю та транснаціонального обміну розвідувальною інформацією між підрозділами фінансових розвідок.

Також проблемним питанням під час розслідування кіберзлочинів залишається збирання та використання в судовому процесі доказів, отриманих у цифровому середовищі.

У контексті цифровізації економіки та трансформації форм злочинної поведінки цифрові докази стають ключовими елементами у процесі доведення вини у справах щодо фінансових кіберзлочинів.

Проте їх збір, фіксація, обробка та долучення до матеріалів кримінального провадження супроводжуються низкою складних юридичних, процесуальних та технічних проблем, які суттєво ускладнюють ефективне здійснення досудового розслідування.

Насамперед, слід зазначити, що Кримінальний процесуальний кодекс України не містить чіткої процедури збору цифрових доказів, що створює правову невизначеність у питаннях дотримання процесуальної форми.

Варто зазначити, що складність вирішення проблеми допустимості цифрових (електронних) доказів пов'язана з характерною для них технічною природою походження. Цей різновид доказів містить абстрактні технічні і математичні моделі, які характеризується специфічними умовами виникнення, існування, копіювання та зберігання, що вочевидь відрізняє їх від інших видів доказової інформації [8, с.147].

Це стосується як способу отримання цифрової інформації (логів, метаданих, даних про IP-адреси, історії транзакцій тощо), так і способу її засвідчення, збереження, передачі та перевірки на цілісність.

Відсутність чіткого нормативного регулювання підвищує ризики визнання таких доказів недопустимими або неналежними під час судового розгляду, що ставить під загрозу результативність розслідування.

Крім того, у випадках фінансових злочинів, вчинених із використанням криптоактивів або цифрових платформ,

джерело цифрових доказів зазвичай знаходиться поза юрисдикцією України.

Козій В. В. підкреслює, що протягом останніх років у Кримінальному процесуальному законодавстві України відбулися певні зміни, які стосуються розслідування злочинів у сфері криптовалют. Зокрема, Законом України від 15.03.2022 «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» до ч. 10 ст. 170 КПК України внесено зміни та передбачено можливість накладення арешту на віртуальні активи, щодо яких ухвалою чи рішенням слідчого судді, суду визначено необхідність арешту майна. Окрему увагу варто звернути і на положення ч. 6 ст. 236 КПК України, якою в тому числі передбачено право слідчого, прокурора під час проведення обшуку долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх зняти (деактивувати) [9 ;с. 480].

Це означає, що органи досудового розслідування стикаються з потребою надсилання запитів про міжнародну правову допомогу, виконання яких може бути тривалим, неефективним або взагалі неможливим у разі відсутності відповідних двосторонніх чи багатосторонніх угод. У цих випадках слідчі нерідко змушені використовувати публічні онлайн-ресурси або дані з відкритих блокчейнів, які, однак, не мають правового статусу належного джерела доказів без належної процесуальної фіксації.

Важливою є також технічна складність забезпечення автентичності та незмінності цифрових даних, особливо якщо вони зберігаються у нестабільних, децентралізованих або тимчасових середовищах. Блокчейн, як децентралізована база даних, з одного боку, забезпечує незмінність транзакцій, а з іншого – вимагає спеціалізованих знань для правильної ідентифікації користувачів, структури записів, валідації даних, а також – для надання доказу зв'язку конкретної особи із записом у блокчейні. Для ефективного використання доказу на стадії судового розгляду кожен елемент має бути підтверджений належним джерелом, з чіткою верифікацією та технічною експертизою.

Особливий виклик становить перетин технічної та правової сфер, оскільки слідчі дії у цифровому середовищі часто не вкладаються у традиційні межі обшуку, виїмки чи тимчасового доступу до речей і документів.

Наприклад, зняття інформації з онлайн-гаманця або смарт-контракту не завжди має фізичне відображення у вигляді матеріального носія, а отже потребує формування нових процесуальних інструментів, які б узаконювали дії слідчого у віртуальному середовищі. У цьому контексті залишається актуальною необхідність розробки окремого процесуального механізму цифрового слідчого втручання, із чітко визначеними правами, гарантіями та відповідальністю. Також слід звернути увагу на кадрову проблему, адже ефективний збір і аналіз цифрових доказів потребує не лише юридичної кваліфікації, але й високої технічної компетенції. У реальній практиці органи досудового розслідування часто не мають у своєму розпорядженні експертів з цифрової форензіки або криптоекономіки, що веде до поверхневого розуміння складних технічних процесів, неправильного трактування доказів або їх втрати на етапі збирання. На практиці існує ще одна суттєва проблема – відсутність уніфікованих стандартів зберігання та передачі цифрових доказів, що часто призводить до втрати доказової сили інформації внаслідок банальної зміни хеш-суми, помилок копіювання або некоректного оформлення технічних звітів. Збирання (отримання) цифрової інформації і цифрових носіїв інформації на поточному етапі розвитку кримінально-процесуальної науки недостатньо врегульоване. Окрім цього, треба наголосити, що законодавцем досі не розроблені ефективні необхідні процесуальні гарантії, які будуть ефективним інструментом захисту громадян від надмірної зацікавленості з боку правоохоронних органів під час проведення процесуальних дій [10, с. 451].

Таким чином, збір і долучення цифрових доказів у розслідуванні фінансових кіберзлочинів є багаторівневою проблемою, яка поєднує в собі правову прогалину, технічну складність, міжнародну недоступність і кадрову неспроможність. Подолання цієї проблематики потребує створення комплексної нормативної бази цифрової криміналістики, формування спеціалізованих груп цифрового розслідування, інтеграції в досудове розслідування експертів з ІТ та блокчейн-аналітики, а також налагодження тісної взаємодії з міжнародними платформами для правового обміну цифровими даними.

Підсумовуючи, кіберзлочинність перестає бути виключно сферою комп'ютерних атак чи шахрайств з персональними даними. Вона трансформується в інфраструктуру, що обслуговує економічну злочинність, легалізацію доходів та податкові правопорушення, забезпечуючи їм стійкість, гнучкість і майже повну анонімність. Протидія такій злочинності неможлива без докорінного оновлення правових підходів, оперативно-розшукових інструментів і міжвідомчої координації в умовах глобального цифрового ландшафту.

Висновки. Проведене дослідження підтверджує, що кіберзлочинність у сфері легалізації доходів та податкових правопорушень більше не є периферійним явищем, а формує структурне ядро сучасної економічної злочинності.

Її багатофункціональний характер – як джерела злочинного доходу, так і середовища для його подальшої легалізації – суттєво ускладнює кримінально-правову кваліфікацію, визначення моменту завершення злочину та формування доказової бази.

Криптоактиви, блокчейн-технології, DeFi-платформи та цифрові платіжні системи надають злочинцям інструменти для глобального переміщення капіталів з високим ступенем анонімності та низьким ризиком викриття. У свою чергу, національне законодавство України ще не адаптоване до цих технологічних умов, що створює «правовий вакуум» при кваліфікації діянь та ініціюванні розслідувань.

Складність ідентифікації кіберзлочинця, який часто діє анонімно, у складі розподілених мереж та з використанням технічних засобів маскування, вимагає переосмислення класичних криміналістичних моделей. Необхідною є побудова гібридної моделі ідентифікації, що включатиме цифрові сліди, поведінковий аналіз, аналіз транзакцій та презумпцію контролю над активами.

Окремий блок проблем становить збір і процесуальне оформлення цифрових доказів, які часто перебувають за межами юрисдикції України, не мають стабільної фізичної форми або зберігаються на децентралізованих платформах. Відсутність єдиної процедури цифрового слідчого втручання, низька кваліфікація працівників правоохоронних органів у сфері ІТ, а також неналагодженість міжнародної взаємодії ускладнюють формування належної доказової бази.

Ефективна протидія кіберлегалізаційним схемам потребує створення нормативної архітектури цифрової криміналістики, уніфікації підходів до обігу віртуальних активів, активізації співпраці з міжнародними організаціями (Європол, Інтерпол, Egmont Group), формування спеціалізованих аналітичних груп на стику ІТ, фінансового моніторингу та кримінального права. У цілому, лише інтеграція юридичних, технологічних і кримінологічних підходів може забезпечити системну протидію легалізації доходів у цифровому вимірі, адекватну до новітніх викликів цифрового транснаціонального кримінального середовища.