УДК 343.98
DOI https://doi.org/10.24144/2307-3322.2026.93.5.30

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ЯК ІННОВАЦІЙНА СКЛАДОВА КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОЗАСТОСТОСОВНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВІЙНИ

Шевчук В.М.,
доктор юридичних наук, професор,
головний науковий співробітник
НДІ вивчення проблем злочинності
імені академіка В.В. Сташиса НАПрН України,
заслужений юрист України
ORCID: 0000-0001-8058-3071
e-mail: Shevchuk_viktor@ukr.net

Шевчук В.М. Використання технологій блокчейн як інноваційна складова криміналістичного забезпечення правозастостосовної діяльності в умовах війни.

Досліджуються актуальні проблеми використання технологій блокчейн у протидії злочинності та їх роль у системі криміналістичного забезпечення такої діяльності у сучасних умовах. Розкрито поняття і криміналістичну сутність віртуальних активів, виокремлено їх види, надано характеристику. Розглянуто сучасне розуміння технології блокчейн, яку визначено як своєрідний «ланцюжок блоків», що являє собою інноваційну технологію, що розглядається як децентралізований цифровий реєстр, який функціонує як розподілена база даних. Виокремлено види злочинної діяльності у цій сфері й запропоновано іноваційні підходи до криміналістичного забезпечення розслідування і судового розгляду кримінальних правопорушень, пов'язаних із використанням віртуальних активів та блокчейн технологій. Обгрунтовано, що криміналістика, інтегруючи сучасні досягнення науки й техніки, у реаліях сьогодення спрямовує свій науковий потенціал на створення ефективної системи криміналістичних засобів, прийомів і технологій у протидії злочинності у сфері незаконного обігу віртуальних активів, а вирішення цих завдань передбачає створення відповідного механізму та запровадження ефективної системи протидії злочинності у цій сфері. Використання таких технологій в умовах війни є фундаментом для створення нової моделі криміналістичного забезпечення органів правопорядку, що проявляється у зміні парадигми фомуванні доказової інформації при розслідуванні таких злочинів. Криміналістичне забезпечення розглядається як процес створення та надання науково обґрунтованих і перевірених на практиці техніко-, тактико-, методико-криміналістичних засобів й технологій, що використовуються практичними працівниками на основі отриманих ними знань та вмінь, відповідно до загальних засад і завдань кримінального провадження. Сучасна парадигма криміналістичного забезпечення еволюціонує від суто юридичної категорії до комплексного організаційно-технологічного механізму, функціональна спроможність якого безпосередньо залежить від рівня інтеграції інноваційних цифрових технологій у практику розслідування та судового розгляду кримінальних проваджень. Запропоновано перспективні напрями дослідження проблематики технологій блокчейн у криміналістиці і судовій експертизі.

Ключові слова: спеціальні знання, криміналістична методика, збирання доказів, кримінальне провадження, злочинна діяльність, віртуальні активи, цифрові активи, криптовалюта, фінансування тероризму, цифрова валюта, криміналістичні інновації, судова експертиза, криміналістичне забезпечення.

Shevchuk V.M. The use of blockchain technology as an innovative component of criminalistic support for law enforcement activities in war conditions.

Current problems of using blockchain technologies in the fight against crime and their role in the system of criminalistic support of such activities in modern conditions are studied. The concept and

criminalistic essence of virtual assets are revealed, their types are distinguished, and their characteristics are given. The current understanding of blockchain technology is considered, which is defined as a kind of «chain of blocks», which is an innovative technology that is considered as a decentralized digital ledger that functions as a distributed database. The types of criminal activity in this area are singled out and innovative approaches to criminalistic investigation and trial of criminal offenses related to the use of virtual assets and blockchain technologies are proposed. It is justified that criminalistics, integrating modern achievements of science and technology, in today's realities directs its scientific potential to create an effective system of criminalistic means, methods and technologies in combating crime in the field of illegal circulation of virtual assets, and the solution of these tasks involves the creation of an appropriate mechanism and the introduction of an effective system of combating crime in this area. The use of such technologies in conditions of war is the foundation for the creation of a new model of forensic support for law enforcement agencies, which is manifested in a paradigm shift in the formation of evidentiary information in the investigation of such crimes. Criminalistic support is considered as the process of creating and providing scientifically based and proven in practice technical, tactical, methodical and criminalistic tools, technologies used by practical workers based on the knowledge and skills they have acquired, in accordance with the general principles and tasks of criminal proceedings. The modern paradigm of criminalistic support is evolving from a purely legal category to a complex organizational and technological mechanism, the functional capacity of which directly depends on the level of integration of innovative digital technologies into the practice of investigation and trial of criminal proceedings.

Key words: special knowledge, criminalistic methodics, evidence collection, criminal proceedings, criminal activity, virtual assets, digital assets, cryptocurrency, terrorist financing, digital currency, criminalistic innovations, forensic examination, criminalistic support.

Постановка проблеми. В реаліях сьогодення розвиток суспільних відносин поява та активне застосування технологій блокчейн, заснованих на таких технологіях і криптовалютних платіжних системах, істотно змінили сам процес, а також можливості використання криміналістичних засобів, методів та технологій протидії сучасній злочинності, яка постійно трансформується, видозмінюється та модернізується під впливом різних чинників [1, с. 119-136]. Особливої актуальності і значимості у контексті технологізації злочинної діяльності і засобів та методів органів правопорядку щодо її протидії набувають кримінальні правопорушення, що пов'язані із незаконним обігом віртуальних активів і використання блокчейн-технологій [2, с. 170-178]. У цьому сенсі з початку повномасштабного вторгнення росії в Україну, віртуальні активи стали інструментом, який активно використовується у злочинній діяльності ворога (воєнні злочини, тероризм, екоцид, геноцид та ін.) [3]. Такі злочини вчиняються у різних сферах: безпековій, оборонній, енергетичній, національній, а також й в інших критично важливих і головних напрямах діяльності держави, посилюючи таку злочинну діяльність корупцією, легалізацією злочинних доходів тощо.

Вбачається, що використання новітніх технологій, засобів та методів, поширення криптовалюти та технологій Blockchain у розвитку суспільства та країн світу, як будь-який соціальний процес, у свою чергу й має свої діалектичні наслідки. З одного боку, віртуальні активи стали новим інструментом злочинців і значного поширення набули вчинення кримінальних правопорушень, пов'язаних із використанням віртуальних активів та блокчейн-технологій [4]. З іншого – наявність у відкритому доступі всієї бази даних транзакцій у системі криптовалюти дає можливості правоохоронцям застосовувати інноваційні методи та інструменти боротьби зі та таким видом злочинності [5, с. 13], у тому числі й протидіяти таким формам транснаціональної огранізованої злочинної діяльності і засобами й методами криміналістики та судових наук [6, с. 3].

За таких умов вкрай важливим є наукове-методичне забезпечення, формування системи вмінь та навичок слідчих, детективів, оперативних співробітників органів правопорядку, надання можливості їм чітко розуміти особливості функціонування таких активів, знати можливості їх виявлення, встановлення походження, відстеження руху віртуальних активів, їх місцезнаходження. Це дозволить вчасно виявляти такі кримінальні правопорушення, ефективно їх розслідувати, встановлювати осіб, причетних до їх вчинення, ідентифіковувати, фіксувати, арештовувати та конфісковувати віртуальні активи у межах кримінального провадження.

Враховуючи тенденції розвитку суспільства та формування сучасних криміналістичних знань, варто зауважити, що саме процеси інтеграції, цифровізації, діджиталізації, пріоритезації та тех-

нологізації криміналістики сьогодні визначають інноваційні напрями криміналістичного забезпечення правозастостосовної діяльності в сучасних умовах війни та цифрової трансформації суспільних відносин, а також окреслюють перспективні напрями майбутього розвитку криміналістики та судових наук в контексті процесів євроінтеграції. Отже, ці та інші проблеми застосування технологій Blockchain і оновлення моделі криміналістичного забезпечення протидії такій злочинності постають як вельми актуальні та значимі у сучасних умовах воєнного стану, євроінтеграції суспільства, технологізації науки та активного поширення цифрових технологій у різних сферах правовідносин, що потребують ефективного захисту засобами і методами криміналістики, і визначають необхідність проведення спеціальних наукових досліджень.

Метою дослідження є аналіз вітчизняного та міжнародного досвіду використання технологій blockchain як важливої інноваційної складової криміналістичного забезпечення правозастостосовної діяльності в сучасних умовах воєнних дій та цифрової транформації суспільства. Для досягнення поставленої мети передбачається вирішення завдань, які спрямовані на удосконалення діяльності органів кримінальної юстиції, що базуються на перегляді та пропонуванні новітньої моделі криміналістичного забезпечення протидії злочинності у цій сфері. Наукова публікація підготовлена на виконання фундаментальної теми «Пріоритезація та технологізація у кримінальному провадженні у воєнний та повоєнний час», що досліджується в НДІ вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України.

Ступінь наукової розробленності проблематики. Аналіз сучасних наукових досліджень свідчить про значну увагу до проблеми кримінальних правопорушень, пов'язаних із використанням віртуальних активів та блокчейн-технологій. Науковці звертались до розроблення та дослідження окремих проблем криміналістичного забезпечення діяльності органів кримінальної юстиції при розслідування цих кримінальних правопорушень та пов'язаними із ними видами злочинної діяльності, зокрема: Л. Аркуша, А. Волобуєв, В. Гусєва, В. Журавель, А. Іщенко, В. Коновалова, В. Лукашевич, Є. Лук'янчиков, Г. Матусовський, М. Салтевський, Р. Степанюк, В. Тіщенко, Ю. Чорноус, Д. Цехан, В. Шевчук, В. Шепітько, Б. Щур, В. Юсупов та ін. Значна увага у наукових дослідженнях присвячувалася й проблемам злочинної діяльності, пов'язаної із використанням блокчейн-технологій, та пропонуванню рекомендацій по їх виявленню, розслідуванню і профілактиці (Р. Баранов, К. Дмитрієва, Ю. Калайда, Ю. Когут, В. Саєнко, К. Сенгвік, В. Шарпацька, В. Шевчук та ін.). Вагомий внесок дослідників виступає методологічним підґрунтям для подальших наукових розвідок проблем криміналістичного забезпечення злочинності у сфері використання блокчейн-технологій. Водночас, вбачається, що недостатньо приділено уваги дослідженню проблемам формування та практичної реалізації використання технологій blockchain як однієї із найважливіших інноваційних інстументів криміналістичного забезпечення правозастостосовної діяльності в умовах війни.

Виклад основного матеріалу. В реаліях сьогодення збройна російська агресія проти України супроводжується скоєнням величезною кількістю воєнних злочинів, фіксація яких відбувається переважно цифровими засобами (фото-, відеозйомка, супутникові знімки). Проте в умовах інформаційної війни та розвитку технологій штучного інтелекту (AI, OSINT, DEEPFAKE та ін.) постає гостра проблема збирання, фіксації та верифікації цих доказів [7, с. 1-19]. Традиційні методи зберігання даних нацентралізованих серверах є вразливими до кібератак та фізичного знищення. Використання технологій блокчейну є важливим інстументом у формування доказової інформації при розслідуванні воєнних злочинів. Фактично ця технологія пропонує інноваційну модель «цифрової пам'яті», яку неможливо змінити або видалити, що є ключовим у роботі із цифровими доказами.

Сьогодні цифрова реальність тісно пов'язана із появою нових форм злочинності, зокрема, значного поширення набуває вчинення кіберзлочинів, інформаційного шахрайства, кримінальних правопорушень у сфері незаконного обігу віртуальних активів та використання технологій Blockchain. Трансформормація сучасної злочинності під впливом активних процесів цифровізації, діджиталізації та європеізації нашого суспільства зумовлює необхідність грунтовних наукових досліджень цих проблем, їх спеціального вивчення і наукового дослідження [8, с. 100-108].

Упродовж останнього десятиліття цифровізація фінансових операцій та поява нових інструментів, зокрема віртуальних активів (криптовалют, NFT, токенів тощо), розвиток децентралізованих фінансових систем (DeFi) докорінно трансформували правове поле економічної взаємодії як на національному, так і на міжнародному рівні [9, с. 207-235]. За останні роки технологія

блокчейну в Україні стрімко набула популярності, особливо у сфері криптовалют. Зростання популярності віртуальних активів і їх значна поширеність, призвело до збільшення випадків їх використання для вчинення злочинної діяльності - шахрайства, відмивання грошей, фінансування тероризму і ядерного шантажу [10, с. 32-45]. Анонімність та децентралізація, які притаманні блокчейн-технологіям, створюють значні виклики для органів кримінальної юстиції і перешкоджають законній діяльності суб'єктів таких правовідносин [11].

Варто зауважити, що стримування злочинності в криптовалютній системі є можливим завдяки роботі органів криміньної юстиції із виявлення та протидії злочинності у сфері обігу віртуальних активів. При цьому, віртуальні активи (virtual assets) – це цифрове представлення вартості, яка може бути передана, збережена або обміняна в цифровому вигляді, і яку можуть використовувати для здійснення платежів або інвестиційної діяльності. Вони є різноманітними [12, с. 13-35], їх можна класифікувати за функціональністю та призначенням: 1. *Криптовалюти* – найпоширеніший вид віртуальних активів, що використовують криптографію для забезпечення безпеки транзакцій й контролю над створенням нових одиниць та працюють на децентралізованій технології блокчейн: а) монети (coins) – цифрові активи, що мають власний, незалежний блокчейн і функціонують як для забезпечення транзакцій у відповідній блокчейн-мережі, оплаті комісій (газу) за операції або як засіб обміну (Bitcoin (BTC), Ethereum (ETH), Solana (SOL), Cardano (ADA), Polkadot (DOT) тощо); б) стейблкоїни (стабільні коїни) – особливий вид криптовалют, розроблений для стабілізації курсу порівняно з традиційними криптовалютами, як Bitcoin, Ethereum та ін., їх вартість прив'язана до фіатних валют, реальних активів (долару США, цінних паперів), біржових товарів (золота, нафти) чи інших криптовалют зі створенням централізованого резерву для їх гарантованого обміну за курсом (USDT (Tether), USDC (USD Coin), TUSD (TrueUSD), BUSD (Binance USD), DAI, XAUT (Tether Gold), FRAX); 2. *Токени* (tokens) – віртуальні активи не мають власного незалежного блокчейну, вони створені та функціонують на базі існуючих (найчастіше Ethereum за стандартом ERC-20, Binance Smart Chain за BEP-20 тощо) за допомогою смарт-контактів. Сфера застосування токенів ширша, ніж у криптовалют: токени-утиліти використовуються для надання доступу до певних послуг або функцій у межах децентралізованої системи (право голосу, оплата послуг); токени безпеки – для надання власнику, володільцю або утримувачу права на частку в компанії, прибуток, дивіденди або інші фінансові активи подібно до акцій або облігацій, лише у цифровій формі; токени управління – для надання власникам, володільцям або утримувачам право голосу в управлінні децентралізованими автономними організаціями (DAO) або протоколами DeFi (UNI (Uniswap), AAVE, LINK (Chainlink) тощо); невзаємозамінні Токени (NFT) – особливий вид токенів (унікальний та неподільний). Кожен NFT має унікальний ідентифікатор, що зберігається в блокчейні і не може бути замінений іншим NFT на відміну від монет, коли одну монету завжди можна обміняти на іншу. Токени NFT використовуються для підтвердження прав власності на цифровий (цифрові картки, віртуальні ігрові предмети, унікальні цифрові аудіо/відео записи, право власності на віртуальні ділянки землі, нерухомість, аватарів, предмети з віртуальних світів) або матеріальний об'єкт (картини, скульптури, нерухомість) або може бути доказом справжності певного віртуального активу [13, с. 205-211].

Відмінність криптовалют та токенів полягає у наявності або відсутності власного незалежного блокчейну, що суттєво впливає на процеси їх обігу. Процес обігу криптовалют розпочинається з того, що продавець ініціює транзакцію, яка негайно транслюється до всієї мережі блокчейна, де кожен вузол (комп'ютер) отримує інформацію про транзакцію та здійснює перевірку її автентичності за допомогою алгоритму консенсусу. Після схвалення транзакції разом з іншими підтвердженими операціями додається до нового блоку. Цей завершений блок, що містить унікальний хеш попереднього блоку, хронологічно приєднується до існуючого ланцюжка, створюючи безперервний та незмінний реєстр. Після інтеграції нового блоку, усі копії блокчейна на вузлах мережі оновлюються, а транзакції в ньому стають підтвердженими та незворотними. Постійна верифікація всіх транзакцій відбувається з кожним циклом досягнення консенсусу мережі. Токени, не маючи власного блокчейну, функціонують на базі існуючих блокчейнів за допомогою смарт-контактів.

Варто зауважити, що блокчейн (англ. blockchain – «ланцюжок блоків») – це інноваційна технологія, що являє собою децентралізований цифровий реєстр, який функціонує як розподілена база даних. Цей реєстр підтримується мережею численних комп'ютерів, відомих як вузли, розташованих по всьому світу. Дані в блокчейні організовані у послідовні блоки, кожен з яких розташова-

ний у суворому хронологічному порядку та захищений за допомогою криптографії. Кожен такий блок містить часову позначку, криптографічний хеш (контрольну суму) попереднього блоку, а також дані про транзакції, представлені у вигляді хеш-дерева. Захист від підробки та видозміни інформації досягається завдяки тому, що хеш поточного блоку інтегрується до наступного. Це означає, що спроба змінити будь-який блок вимагатиме відповідних змін у всіх наступних блоках ланцюга, що робить таку маніпуляцію практично неможливою. Блокчейн забезпечує безпеку, децентралізацію та консенсус у мережі, дозволяючи учасникам взаємодіяти без посередників.

Усі віртуальні активи зберігаються за блокчейн-адресою – унікальним ідентифікатором у блокчейн-мережі, який генерується на основі двох ключів: публічного та приватного. Перший є «відкритою» інформацією (подібно до номеру банківського рахунку), другий – секретним паролем та цифровим підписом, що надає доступ до коштів на цій адресі та можливість здійснювати транзакції. Приватні ключі зберігаються у криптогаманцях – програмному забезпеченні (мобільному додатку, десктопній програмі, онлайн-сервісі), апаратному пристрої (USB-флешці) або паперовому носії (файл або роздрукований аркуш із seed-фразою), що дозволяють керувати віртуальними активами. Перша група криптогаманців, підключених до мережі Інтернет є «гарячими» гаманцями, друга група, не підключеними до мережі – «холодними».

На сьогодні, на жаль, чинне законодавство не має єдності у формуванні теоретико-правових засад функціонування ринку віртуальних активів, що обумовлює колізійність нормативно-правового регулювання їх правового статусу та правовідносин, пов'язаних із віртуальними активами. У умовах війни та глобальних загроз головним завданням криміналістики є розроблення та застосування інноваційних засобів, прийомів та методів, що дозволяють ефективно збирати, досліджувати, використовувати у досудовому розслідуванні та судовому розгляді різноманітну доказову інформацію, у тому числі й цифрову.

Очевидно, що поява технологій Blockchain суттєво змінило способи і механізми злочинної діяльності, а також вплинуло на формування і можливості методів та засобів протидії злочинності у цій сфері, особливо в умовах гібридної війни [14, с. 411]. Практика показує, що з початку збройної російської агресії ці процеси активізувалися, адже віртуальні активи стали інструментом, який активно почав використовуватися у розвідувально-підривній і диверсійно-терористичній діяльності ворога. Значного поширення також набула організована злочинна діяльність із використанням блокчейн-технологій у безпековій та оборонній сфері, при вчиненні злочинів проти національної безпеки України, фінансування тероризму, шахрайства, застосування ядерного шантажу тощо.

Так, наприклад, Служба безпеки Украі ни виявила та заблокувала діяльність злочинного угруповання, яке займалося відмиванням та незаконним переведенням коштів, зокрема й з використанням криптовалют. Організаторами було створено мережу онлаин-ресурсів (сайти, телеграм-канали), які дозволяли користувачам конвертувати криптовалюту у готівку в особливо великих розмірах (на понад 240 млн грн). У процесі проведення НСРД і СРД було встановлено, що даним сервісом користувались й також особи, які підтримують та фінансують сепаратизм та терористичну діяльність. Під час розслідування було зясовано, що транзакції здійснювалися через заборонені іноземні електронні платіжні системи з використанням технологій блокчейн. Далі для відмивання та легалізації злочинних доходів організатори таких махінацій інвестували у нерухомість, земельні ділянки, фінансові установи, дорогоцінні метали та ін. [15, с. 92].

Важливо зауважити, що поряд із масовими вчиненнями російським агресором на території воєнних злочинів, значного поширення набули й інші пов'язані із ними види злочинної діяльності у криптосфері. Згідно зі звітом Chainalysis 2025 Crypto Crime Report [16]. Україна посідає 8-ме місце у світі за впровадженням криптоактивів і, звичаєно, це створює, з одного боку, певні можливості для злочинної діяльності у цій сфері, фінансування тероризму, оборони, так і нові виклики, яким треба ефективно протидіяти, як кримінально-правовими, так і кримінально-процесуальнми й криміналістичними засобами.

За офіційними даними вищезгаданого Звіту, найпоширеніщими злочинами у цій сфері є: а) шахрайство, що вчиняються із використанням інвестиційних пірамід та фішингових схем; б) відмивання коштів, які скоюються за допомогою використання криптоактивів для легалізації доходів, отриманих злочинним шляхом, зокрема через неліцензовані біржі; в) викрадення коштів через хакерські атаки за допомогою вчиненя таргетованих атак на криптогаманці громадян та державні установи; г) фінансування агресії та обхід санкцій, що вчиняється із використанням криптова-

лют для закупівлі товарів подвійного призначення в обхід міжнародних обмежень; д) торгівля людьми, коли використовуються криптоплатежі у схемах та операціях, пов'язаних із торгівлею людьми [16].

Вбачається, що при розслідуванні такої злочиної діяльності традиційні криміналістичні методи фіксації цифрової доказової інформації часто виявляються недостатніми через ризики фізичного знищення серверів або дистанційного видалення даних. За таких обставин технології Blockchain постають як інноваційний інструмент, що забезпечує вирішення криміналістичних та кримінально процесуальних завдань і гарантує цілісність, автентичність та хронологічну послідовність доказової інформації при розслідуванні кримінальних правопорушень з використанням блокчейн-технологій і пов'язаних із ними воєнних злочинів в Україні.

Зростання ефективності стримування нелегальної активності у криптосфері досягається завдяки декільком чинникам, й серед іншого, завдяки удосконаленню підходів до законодавчого урегулювання обороту віртуальних активів, яке дає змогу ефективніше виконувати свої зобов'язання відповідним спеціалізованим органам регулювання і нагляду за діяльністю постачальників послуг, пов'язаних з оборотом віртуальних активів. До того ж, в цій сфері дуже важливим чинником є взаємодія органів влади різних країн, оскільки віртуальні активи характерні своєю транснаціональною природою [17].

У цьому контексті вкрай важливим постає необхідність розроблення і пропонування науково-методичного забезпечення їх розслідування і судового розгляду, формування нової системи криміналістичних знань, вмінь та навичок у слідчих (детективів), прокурорів, оперативних працівників й інших суб'єктів кримінального провадження у протидії злочинності у сфері незаконного обігу віртуальних активів в умовах гібридної війни [18, с. 898]. Насьогодні практичні працівники потребують дієвих рекомендацій щодо збирання та використання доказової інформації при розслідуванні такої злочиної діяльності з використанням технологій блокчейну та різними видами віртуальних активів під час воєнних дій.

При цьому варто враховувати, що скоєння кримінальних правопорушень, пов'язаних з використанням віртуальних активів, мають високий ступінь латентності [19, с. 21-25], складну доказову базу та потребують спеціальних знань у сфері інформаційних технологій, економіки та фінансового моніторингу [20, с. 138-139]. У практиці досудового розслідування через відсутність усталених процесуальних механізмів і нормативно визначених процедур щодо виявлення, ідентифікації, фіксації, арешту та конфіскації віртуальних активів у межах кримінального провадження виникають труднощі з їх виявленням, встановленням походження віртуальних активів, отриманих або пов'язаних з протиправною діяльністю, а також із відстеженням руху віртуальних активів та їх місцезнаходження для подальшого блокування і конфіскації, встановленням осіб причетних до незаконного використання криптовалют через анонімність транзакцій та децентралізовану природу функціонування блокчейн-систем тощо. Очевидно, що ці й інші обставини потребують інноваційних підходів до криміналістичного забезпечення правозастостосовної діяльності та протидії злочинності у сфері незаконного обігу віртуальних активі в умовах війни.

Сучасне розуміння і використання новітніх (криміналістичних, кримінальних) технологій у контексті криміналістичного забезпечення протидії злочинності має подвійний характер. З одного боку, сучасні технології використовуються злочинцями для вчинення кримінальних правопорушень. У цьому сенсі новітні технології входять до механізму злочинної діяльності і стають кримінальними технологіями досягнення злочинних цілей (технології злочинної діяльності*)* [21, с. 281-287]. З іншого боку, технології є інструментом, що дозволяє не тільки успішно протидіяти кримінальним правопорушенням (злочинам), але і запобігати їм. Вони виступають, як криміналістичні технології, і пов'язані вони із діяльністю із розслідування та судового розгляду [22, с. 87].

Криміналістичне забезпечення являє собою своєрідний процес створення та надання науково обґрунтованих і перевірених у судово-слідчій практиці засобів (техніко-криміналістичних, тактико-криміналістичних, методико-криміналістичних, судово-експертних, інформаційних, попереджувально-профілактичних), які використовуються працівниками органів кримінальної юстиції на основі отриманих ними знань та вмінь, відповідно до загальних засад і завдань кримінального судочинства з метою протидії кримінальним правопорушенням і встановлення істини у кримінальному провадженні [23].

Сьогодні інструментарій криміналістичного забезпечення органів кримінальної юстиції охоплює не лише традиційні криміналістичні засоби та методи, а й технології нового покоління: за-

стосування ШІ для аналітики масивів даних та дослідження об'єктів судової експертизи, OSINT для встановлення обставин і осіб, причетних до вчинення злочинів, біометричні технології – для ідентифікації та верифікації, інструменти блокчейн, сучасні методи ідентифікації загиблих у збройних конфліктах [24]. Водночас, застосування новітніх технологій, засобів та методів у криміналістичному забезпеченні супроводжується низкою проблем (етичних, правових, процесуальних та ін.) [25, с. 12-46]. Отже, вбачається, що сучасна парадигма криміналістичного забезпечення еволюціонує від суто юридичної категорії до комплексного організаційно-технологічного механізму, функціональна спроможність якого безпосередньо залежить від рівня інтеграції інноваційних цифрових технологій у практику розслідування та судового розгляду кримінальних проваджень.

Застосування інновацій у криміналістиці та судовій екпертизі тісно пов'язані із активізацією використання новітніх засобів, методів та технологій. Серед них особливе місце займають цифрові технології, штучний інтелект, у тому числі й технології Blockchain. Водночас, в реаліях сьогодення існує низка проблем і викликів із якими стикаються органи кримінальної юстиції у протидії кримінальних правопорушень, пов'язаних із використанням віртуальних активів. Передусім, це зумовлено прогалинами у законодавчому регулюванні обігу віртуальних активів; відсутністю науково-методичних розробок ефективного розслідування кримінальних правопорушень, пов'язаних із використанням віртуальних активів; складнощами у збирані цифрових доказів та проведенні судових експертиз щодо незаконного обігу віртуальних активів; відсутнісю апробованих криміналістичних методик розслідування цих кримінальних проявів із врахуванням міжнародних і європейських стандартів тощо.

Безумовно, що такі загрози і виклики потребують розроблення та пропонування інноваційних підходів і модернізації криміналістичного забезпечення протидії сучасній злочинності у цій сфері, оновлення та удосконалення системи органів кримінальної юстиції до сучасних умов, спрямованих на забезпечення безпеки та обороноздатності України. Реалії сьогодення визначають сучасні тенденції розвитку юридичної науки, у тому числі й криміналістики щодо формування інноваційних напрямків застосування криміналістичних знань, новітніх інструментів криміналістичного забезпечення злочинів, пов'язаних із віртуальними активами та блокчейн-технологіями.

Кримінальні правопорушення, пов'язані з використанням віртуальних активів, маючи високий ступінь латентності, складність формування доказової бази, потребують шипрокого застосування спеціальних знань у сфері інформаційних технологій, економіки та фінансового моніторингу [26, с. 107]. У практиці досудового розслідування через відсутність усталених процесуальних механізмів і нормативно визначених процедур щодо виявлення, ідентифікації, фіксації, арешту та конфіскації віртуальних активів у межах кримінального провадження виникають труднощі з виявленням таких кримінальних правопорушень, встановленням походження віртуальних активів, отриманих або пов'язаних з протиправною діяльністю, відстеженням руху віртуальних активів та їх місцезнаходження для подальшого блокування та конфіскації, встановленням осіб причетних до незаконного використання криптовалют через анонімність транзакцій та децентралізовану природу функціонування блокчейн-систем тощо.

Ключовими напрямами застосування технологій Blockchain в сучасних умовах воєнних дій є такі: 1. *Документування воєнних злочинів, адже блокчейн досить активно використовується для фіксації цифрових доказів (фото, відео, свідчень) руйнувань цивільної інфраструктури, що унеможливлює їх підробку або видалення. Так, наприклад, за ініціативи* Starling Lab вже подали до МКС досьє щодо руйнування шкіл у м. Харків, де автентичність кожного файлу підтверджена криптографічно; 2. *Захист культурної спадщини, оскільки створення децентралізованих реєстрів викрадених (знищених) культурних цінностей дозволяє забезпечити їх міжнародне визнання і процес майбутньої реституції; 3. Протидія фінансуванню агресії, коли органи правопорядку використовують блокчейн-аналітику для відстеження криптоактивів, що спрямовуються на фінансування збройної агресії, тероризму і для виявлення схем обходу санкцій; 4. Забезпечення законності і прозорості гуманітарної допомоги та закупівель, оскільки запровадження смарт-контрактів у сфері оборонних та відновлювальних закупівель дозволяє мінімізувати корупційні ризики та забезпечити підзвітність розподілу міжнародної допомоги.*

*Практика показує, що насьогодні досить надійним способом ф*іксації та збереження доказів вчинення воєнних злочинів є використання децентралізовані сховища. Наприклад, застосування платформи *Starling Lab,* коли цифрова інформація, фото-, відеозйомка, супутникові знімки руй-

нувань автоматично завантажуються в децентралізовані мережі (IPFS), а їх метадані (час, GPS, датчики пристрою) карбуються в блокчейні. Це створює «незнищенний архів», який неможливо видалити навіть при фізичному знищенні серверів у конкретній країні. При цьому процес роботи з доказовою інформацією при розслідуванні злочинів, пов'язаних із блокчейном, кардинально відрізняється від розслідувань традиційних кіберзлочинів чи економічних. Основна складність полягає в тому, що речовий доказ (актив) знаходиться в децентралізованій мережі, а знаряддя злочину (ключі) – у фізичному або цифровому просторі підозрюваного.

Особливості виявлення таких злочинів часто відбувається через моніторинг або за заявою потерпілого. Першочергове завдання – ідентифікація адреси гаманця. Необхідно провести аналіз трансакцій, проаналізувати використання блокчейн-експлорерів (Etherscan, Blockchain.com) для встановлення маршруту коштів. Також важливо виявити так звані лення «точки виходу», здійнити пошук трансакцій, що ведуть на централізовані біржі (Binance, WhiteBIT тощо). Це критично, оскільки лише там можна встановити реальну особу через процедуру KYC. Далі важливим є збір метаданих, провести фіксацію IP-адрес, з яких здійснювався доступ до гаманців (через запити до провайдерів або аналіз логів веб-сервісів).

Фіксація доказової інформації при дослідженні цифрових слідів має свою специфіку. Передусім, цифрові сліди у блокчейні є публічними, тому їх потрібно процесуально закріпити, щоб вони стали допустимими доказами. Це здійснюється за допомогою: а) *скриншот-фіксації*, проводиться протоколювання огляду веб-сторінок з блокчейн-трансакціями, де важливо фіксувати не лише суму, а й хеш трансакції (TXID), час та адреси відправника чи отримувача; б) *збереження логів*, а також вилучення даних про сесії зв'язку, використання VPN-сервісів або браузера Tor, що вказує на умисел приховування слідів; в) *використання хеш-сум*, будь-який вилучений цифровий файл (база даних гаманця, скриншот) має бути захешований (алгоритми MD5, SHA-256) безпосередньо в протоколі огляду, щоб виключити звинувачення його підробки.

Алгоритм роботи з віртуальними активами також має свою специфіку. Важливим у цій діяльності є виявлення блокчейн-адреси, за якою зберігаються віртуальні активи пов'язані з протиправною діяльністю. Вирішення цього завдання здійснюється шляхом кластерізації адрес (групування блокчейн-адрес в один «кластер», що вказує на їхню приналежність одному власнику. Далі проводиться трасування потоків коштів (відстеження руху криптовалюти від початкової адреси (адреси викрадених коштів або адреси-вимагача) через різні «шари» транзакцій до кінцевих адрес призначення) або за допомогою баз даних професійних блокчейн-аналітичних платформ (Chainalysis Reactor, CipherTrace, Crystal Blockchain, TRM Labs), що містять інформацію про блокчейн-адреси, пов'язані з викраденням, шахрайством, фінансуванням тероризму тощо.

При розслідуванні кримінальних правопорушень, пов'язаних із віртуальними активами, найбільш поширені такі види судових експертиз: 1) експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза; 2) експертиза телекомунікаційних систем і засобів (дослідження цифрових та аналогічних приладів); 3) психологічна експертиза для аналізу листування підозрюваного з потерпілим, форм і методів впливу, переконання або тиску, можливого введення в оману, психологічного примусу або маніпуляції; 4) судова економічна експертиза для встановлення ринкової вартості віртуальних активів на певний момент часу, розмір заподіяної шкоди, економічний механізм обігу віртуальних активів у межах злочинної схеми.

Звернення до судового експерта стосовно проведення судової експертизи операцій із цифровими активами під час розслідування таких кримінальних правопорушень може бути викликано різними обставинами (зокрема, в разі злому «гаманця» або онлайн-кабінету на криптовалютній біржі і викрадення певної кількості криптовалюти за допомогою їх перенесення на реквізити викрадача тощо [27, с. 156-160]. Наприклад, судовою експертизою можна вирішувати питання щодо обґрунтованості відображення криптовалюти у відповідних деклараціях, які заповнюються чиновниками і претендентами на відповідні публічні посади (як відомо, така практика вже має місце); обліку та відображення криптовалюти й операцій із ними у фінансовій та бухгалтерській звітності. Оскільки «блокчейн-експертизи» як окремого виду в законі ще немає, слідчі зазвичай ставлять питання в межах комплексної експертизи, де фахівець використовує софт (наприклад, *Crystal*), а його звіт долучається як «дослідження спеціаліста» або частина висновку комп'ютерно-технічної експертизи.

Отже, криміналістика, інтегруючи сучасні досягнення науки й техніки, у реаліях сьогодення спрямовує свій науковий потенціал на створення ефективної системи криміналістичних засобів,

прийомів і технологій у розслідуванні кримінальних правопорушень, пов'язаних із використанням віртуальних активів та блокчейн-технологій. Вирішення цих завдань та створення відповідного механізму передбачає запровадження ефективної системи протидії злочинності у цій сфері, реформування і удосконалення кримінального і кримінального процесуального законодавства, вжиття невідкладних заходів, спрямованих на удосконалення слідчої, експертної та судової практики.

Висновки. Таким чином, використання технологій Blockchain у сучасних умовах війни стали фундаментом для створення нової моделі криміналістичного забезпечення органів правопорядку. Це проявляється у зміні парадигми фомуванні доказової інформації при розслідуванні воєнних злочинів та процесу доказування. Зокрема, в умовах війни традиційні цифрові докази вразливі до знищення або маніпуляцій. Блокчейн трансформує концепцію «Chain of Custody» (ланцюжка зберігання доказів), створюючи математично підтверджений, незмінний реєстр подій, що є критичним для майбутніх міжнародних трибуналів та національних судів.

Дослідження проблем технологій блокчейн у криміналістиці і судовій експертизі передбачають необхідність проведення сучасних криміналістичних розробок у таких напрямах: 1) розроблення та удосконалення теоретико-методологічних засад використання блокчейн-технологій, криміналістичного дослідження цифрових слідів, цифрової криміналістики та теорії криміналістичних технологій – її концептуальних основ, загальних положень і практики застосування; 2) розробки окремих напрямків застосування блокчейн-технологій у кримінальному проваджені, у системі усіх розділів криміналістики, зокрема, у загальній теорії криміналістики, криміналістичній техніці, криміналістичній тактиці, криміналістичній методиці; 3) подальші дослідження окремих наукових теорій (теорія криміналістичних технологій, криміналістична теорія тактичних операцій, теорія криміналістичної алгоритмізації та програмування тощо); 4) формування та удосконалення форм і напрямів використання блокчейн-технологій і криміналістичних технологій, розширення меж їх застосування, адже у сучасних реаліях актуальним є комплексний підхід у дослідженні проблем застосування технологій та засобів криміналістичної техніки, тактики, методики у різних видах судочинства (кримінального, адміністративного, цивільного, господарського) та окремих напрямках діяльності, як злочинної, так і діяльності органів правопорядку у сфері протидії злочинності; 5) сучасний арсенал та інструментарій використання блокчейн-технологій і криміналістичних технологій, засобів і методів має відповідати європейським стандартам, оскільки такий арсенал має бути ефективним, надійним, етичним, валідним і адаптованим до сучасних вимог практики; 6) подальші розроблення і пропонування новітніх підходів у використанні блокчейн-технологій, їх ефективного застосування у кримінальному проваджені, охоплюючи технології застосування засобів криміналістичної техніки, тактики та методики розслідування тощо. Означена проблематика спрямована на удосконалення і подальший розвиток теоретико-методологічних засад теорії криміналістичних технологій, у тому числі й блокчейн-технологій, та належить до найбільш важливих напрямів криміналістичної доктрини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Orlovskyi R., Us O., Shevchuk V. Human Trafficking Committed by Transnational Organised Groups: Criminal Law and Criminalistic Means Combating. *Pakistan Journal of Criminology*, 2023, 15, 4, 119–136. URL: https://www.pjcriminology.com/wp-content/uploads/2023/11/8.-Human-Trafficking-Committed-by-Transnational.pdf.
2. Калайда Ю.П. Можливості блокчейн-технологій у розслідуванні кримінальних правопорушень, вчинених в кіберпросторі. *Інформація і право*. № 4 (39) 2021. С. 170–178. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).249299.
3. Баранов Р.О. Протидія легалізації злочинних доходів та фінансуванню тероризму з використанням віртуальних валют. *Державне управління: удосконалення та розвиток.* 2016. № 6. URL: http://www.dy.nayka.com.ua/?op=1&z=978 (дата звернення: 01.02.2026).
4. Sedgwick K. Bitcoin is Great for Criminals. It's Even Better for Law Enforcement. *Bitcoin.com*: website. 16.07.2018. URL: https://news.bitcoin.com/bitcoin-is-great-for-criminals-its-even-better-for-law-enforcement.
5. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки: монографія / за заг. ред. В.І. Борисова, М.В. Карчевського, М.В.

Шепітька; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса. Х.: Право, 2023. 152 с. https://ivpz.kh.ua/wp-content/uploads/2024/03/Моно_Інфобезпека_2023_НДІ-ВПЗ_авт_compressed.pdf.

6. Shevchuk V., Vapniarchuk V., Borysenko I., Zatenatskyi D., Semenogov V. Criminalistic methodics of crime investigation: Current problems and promising research areas. *Revista Juridica Portucalense*, 2022, 32, 320–341.DOI: https://doi.org/10.34625/issn.2183-2705(32)2022.ic-14.
7. Shevchuk, V., Morozova T., Chornyi, H., Nehrebetskyi V., and Slobodeniuk, I. (2025). Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues. *International Annals of Criminology,* 2025. Pp. 1-19. DOI: https://doi.org/10.1017/cri.2025.10090.
8. Думчиков М.О. Процеси диджиталізації і криміналістика: ретроспективний аналіз. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 100-108. DOI: https://doi.org/10.33994/kndise.2020.65.11.
9. Shevchuk, V., Bululukov, O., Chornyi, H., Tyshchenko, O., & Baranchuk, V. Latest Criminalistic Tools and Technologies in the Investigation of Cybercrimes: International and Ukrainian Experience. *Law, State & Telecommunications Review/Revista de Direito, Estado e Telecomunicações*, 2025, *17*(2), 207-235. DOI: https://doi.org/10.26512/lstr.v17i2.55927.
10. Orlovskyi R., Us O., Shevchuk V. Committing a Criminal Offence by an Organized Criminal Group. *Pakistan Journal of Criminology,* 2022, 14, 2, 2022, 32-45. URL: http://www.pjcriminology.com/publications/committing-a-criminal-offence-by-an-organized-criminal-group.
11. What Are Blockchain Forensics? 2024. URL: https://miethereum.com/learn/what-are-blockchain-forensics.
12. Когут Ю.І. Технології блокчейн та криптовалюта: ризики та кібербезпека : практичний посібник. Київ : «СІДКОН»; ВД «Дакор», 2024. 316 с.
13. Шевчук В.М., Шарпацька В.М. Роль блокчейн-технологій у збиранні цифрових доказів та протидії злочинності у сфері незаконного обігу віртуальних активів. *Криміналістика та судова експертиза в дослідженнях молодих науковців*: зб. матеріалів наук.-практ. конф., м. Харків, 29 трав. 2025 р.; Нац. юрид. ун-т ім. Ярослава Мудрого; Нац. акад. прав. наук України. Харків : Право, 2025. С. 205-211. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20587.
14. Саєнко В.В. Виокремлення видів злочинної діяльності, у яких віртуальні активи є засобом вчинення кримінальних правопорушень, як підстава формування окремих криміналістичних методик розслідування. *Науковий вісник Ужгородського Національного Університету*, 2025. Право, 92: ч. 4. С. 409- 421. DOI: https://doi.org/10.24144/2307-3322.2025.92.4.57.
15. Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму) (20.12.2021 р. № 146). Київ: Державна служба фінансового моніторингу України. 2021. 117 с.
16. The chainalysis 2025 Crypto Crime Report https://go.chainalysis.com/2025-Crypto-Crime-Report.html.
17. Огляд законодавства щодо регулювання віртуальних активів у сфері боротьби з відмиванням коштів та фінансуванням тероризму. К., 2022. 587 с.
18. Konovalova V.O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: 5th International scientific conference (August 7-9, 2022). Lviv, Ukraine. 2022. Pp. 896–903. https://sci-conf.com.ua/wp-content/uploads/2022/08/MODERN-RESEARCH-IN-WORLD-SCIENCE-7-9.08.2022.pdf.
19. Бараннік Р.В. Кібербезпека і управління інформаційними ресурсами: навч. посіб. Київ: Юрінком Інтер, 2025. 236 с.
20. Никифорчук Д.Й., Чемерис Д.Д. Проблемні питання протидії криптовалютній злочинності в Україні. Шляхи реформування кримінальної поліції: вітчизняний та зарубіжний досвід: матеріали Міжнар. наук.-практ. круглого столу (м. Київ, 18 лют. 2022 р.). Київ: НАВСУ, 2022. С. 138-139. URL: https://elar.navs.edu.ua/server/api/core.
21. Шевчук В.М., Тищенко О.І. Технологізація криміналістики, судової експертизи і кримінального провадження в сучасних умовах цифровізації. *Юридичний науковий електронний журнал.* № 12. 2024. С. 375-380. DOI https://doi.org/10.32782/2524-0374/2024-12/86.

22. Панченко Є.В. Криптовалюти й електронні гроші як інструменти фінансової активності кіберзлочинців. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: міжвідомч. наук.-практ. конференція (м. Київ, 1 листоп. 2024 р.). Київ: НАВСУ, 2024. С. 85–89. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/82ef550b-2b39-4375-a5d1-.
23. Шевчук В.М. Інноваційні засади криміналістичного забезпечення правозастосовної діяльності: проблеми формування концепції. *Теорія та практика судової експертизи і криміналістики*: зб. наук. пр. Харків: Право, 2021. Вип. 23. С. 7-23. DOI: https://doi.org/10.32353/khrife.1.2021.01.
24. Динту В.А., Мітрофанов А.А. Bitcoin у системі легалізації доходів, одержаних злочинним шляхом. *Наукові праці Національного університету «Одеська юридична академія».* 2017. Т. 19. С. 122-129. URL: http://npnuola.onua.edu.ua/index.php/1234/article/view/524/495; DOI: https://doi.org/10.32837/npnuola.v19i0.524.
25. Matulienė, S., Shevchuk, V., & Baltrūnienė, J. (2022). Artificial intelligence in law enforcement and justice bodies: Domestic and European experience. *Theory and Practice of Forensic Science and Criminalistics*, *29*(4), 12-46. DOI: 10.32353/khrife.4.2022.02.
22. Дмитрєєва К.С., Іванова О.В. Криптовалюта як об'єкт дослідження судової економічної експертизи. *Нове українське право*. Вип. 6. 2021. С. 156-160. DOI: https://doi.org/10.51989/NUL.2021.6.23.
25. Бараннік Р.В. Кібербезпека і управління інформаційними ресурсами: навч. посіб. Київ: Юрінком Інтер, 2025. 236 с.
26. Федчишина В.В. Криптовалюта й блокчейни криптовалюти як інструменти корупції: реалії інституціалізації. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали VII Міжнар. наук.-практ. конф. (Київ, 8-9 груд. 2022). К.: НАВСУ, 2022. С. 101–111. https://www.navs.edu.ua/files/antykoruptsia/2022/materialy_konf_081222.pdf.
27. Дмитрєєва К.С., Іванова О.В. Криптовалюта як об'єкт дослідження судової економічної експертизи. *Нове українське право*. Вип. 6. 2021. С. 156-160. DOI: https://doi.org/10.51989/NUL.2021.6.23.

Дата першого надходження рукопису до видання: 3.02.2026
Дата прийняття до друку рукопису після рецензування: 20.02.2026
Дата публікації: 5.03.2026

© Шевчук В.М., 2026
Стаття поширюється на умовах ліцензії CC BY 4.0