Forensic Characteristics of Criminal Offenses Related to Illegal Circulation of Virtual Assets

Dmytro Nesterov*

* Crypto Analytics Consultant (NDA), Kharkiv, Ukraine,
ORCID: https://orcid.org/0009-0008-3252-4649, e-mail: nesterov.dmitriy85@ukr.net

DOI: 10.32353/khrife.2.2026.12 UDC 343.985(477)
Received:14.05.2026 / Reviewed: 26.05.2026 / Accepted for printing: 25.06.2026 /
Available online: 30.06.2026

This article purpose is to reveal peculiarities of forensic characteristics of crimes related to illegal circulation of virtual assets, as well as to determine the main elements of their commission mechanism. For achieving this goal, complex of general scientific and special legal methods of cognition was applied, in particular dialectical, system-structural, formal-legal, comparative-legal, logical-semantic one, analysis and synthesis, modeling and generalization. The article is devoted to research on forensic characteristics of criminal offenses related to illegal circulation of virtual assets, which in conditions of global digitalization and rapid information development of technologies are becoming increasingly dangerous to society. Topic relevance is due to active use of cryptocurrencies, decentralized financial services, anonymous payment instruments and artificial intelligence technologies in mechanisms of committing fraud, cybercrime and legalization of proceeds from crime. Growth of transnational cybercrime, spread of phishing schemes, use of mixers, toggle switches, offshore jurisdictions and platforms with end-to-end encryption create significant difficulties for law enforcement agencies in detecting, documenting and investigating such offenses. Particular attention is paid to the problems of forming an evidentiary base associated with virtual nature of digital traces and difficulty of identifying persons involved in illegal transactions with virtual assets. The research results determined that virtual assets as a subject of criminal encroachment form specific mechanism of criminal

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translated by Andriy Bublikov). The author acknowledges translation as corresponding to the original.

activity that is characterized by a high level of latency, cross-border nature, use of modern information technologies and complexity of localizing the place of commission of a criminal offense. It was substantiated that digital traces contained in blockchain, electronic wallets, user accounts, PC memory, messengers, social networks, databases of communication operators and Internet providers are of crucial importance for the investigation. The most common methods of committing crimes related to the illegal circulation of virtual assets are analyzed, including phishing attacks, hacking of cryptocurrency exchanges and electronic wallets, use of fake platforms, manipulation of tokens, fraudulent investment projects, DeFi-exploits, NFT fraud and legalization of income using cryptocurrency services and online casinos. It is proven that significant part of such offenses is committed by transnational organized criminal groups with a clear division of roles between participants. It is argued that offender in this category of crimes is characterized by a high level of digital competence, specific expertise in the field of information technology, programming or finance and an orientation towards obtaining material benefits. It is proposed to classify the subjects of such criminal offenses as technically trained specialists, professional cybercriminals and persons with legal professional status who apply their knowledge to implement criminal schemes. It is concluded that criminal offenses related to illegal circulation of virtual assets are a complex multi-level phenomenon that combines cybercrime peculiarities, economic crime and transnational organized activity. The need for further development of forensic investigation methods, improvement of legislative regulation of circulation of virtual assets and increasing level of technical training of law enforcement agencies in the field of work with digital evidence and blockchain technologies is emphasized.

Keywords: *virtual asset; blockchain; cross-border crimes; legalization (laundering) of money obtained by criminal means; fraud; theft; forensic characteristics; illicit trafficking.*

Research Problem Formulation

Technological innovation has driven economic and social progress, but the same innovation has brought to market the factors that facilitate cyberfraud, lowering barriers, expanding reach and enabling fraudsters to scale operations. Many financial and non-financial services have rapidly proliferated online during the *COVID-19* pandemic. As highlighted in joint publication of the *FATF* (International Group on Combating Money Laundering, *Financial Action Task Force*), Egmont Group of Financial Intelligence Units and Interpol on Illicit Financial Flows from cyberfraud and related crimes are experiencing explosive growth driven by emerging technologies,

artificial intelligence (AI) and deepfakes based on [1].

State Financial Monitoring Service emphasizes that development of financial infrastructure increases difficulties in combating fraud. Growing use of virtual assets (hereinafter referred to as VA), as well as instant and cross-border payment channels with insufficient targeted mitigation measures, allow the transfer of proceeds before their detection or intervention. Often, large-scale cyberfraud schemes are carried out or facilitated by transnational organized criminal groups: such schemes are managed with the help of specialized fraud centers [2]. A similar situation with the masking of illegal transactions through their implementation using VA has developed in most black markets (sale of weapons, drugs, provision of illegal services, etc.) and in the sphere of legalization (laundering) of criminal proceeds.

State Financial Monitoring Service of Ukraine records following cases of laundering proceeds from fraudulent actions and cybercrimes: use of AI technologies for the purpose of illegally passing remote identification and gaining access to a client's account; intentional forgery of deposit documents for fraudulent appropriation of funds of banking institution; fraudulent sale by an individual of commercial real estate objects, which construction had no legal relationship, for cash; fraudulent appropriation of cash and non-cash funds of citizens under the guise of raising funds for the needs of the Armed Forces of Ukraine; appropriation of funds of individuals by deception or abuse of trust (selling non-existent goods through social networks) with subsequent withdrawal of funds to a cryptocurrency exchange; use of fake website of a State body to access personal data and bank accounts for the purpose of illegally debiting funds; use of phishing emails to gain access to the victim's bank account and make illegal transfers [3].

There are frequent cases of laundering criminal proceeds using VA: conducting transactions with crypto assets; using a third-party exchange service using regular current accounts not intended for such activities, involving minors and foreign citizens; using VA as ransom to unlock the work of non-resident companies that have suffered from cyberattacks; using fake crypto trading projects that are actually an element of a financial pyramid, with the aim of fraudulently seizing the funds of citizens of Ukraine and foreigners [4].

Interpol has observed similar trends in its jurisdictions. According to Interpol, widespread use of end-to-end encryption (*E2EE*) platforms, combined with complex jurisdictional and technical barriers, leaves investigators with "blind spots". In addition, work is often hampered by restrictive or inadequate data retention policies (for example, on crypto exchanges). By the time investigators request access

1 Cyber-Enabled Fraud. Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks. February 2026 / FATF : web. 9 p. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cyber-Enabled-Fraud%E2%80%93Digitalisation-and-ML-TF-PF-Risks.pdf.coredownload.inline.pdf (date accessed: 11.04.2026).

2 Типологічне дослідження на тему: «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації — 2025» : затв. наказ. Держфінмоніторингу України від 22.12.2025 р. № 116. URL: https://surl.li/spkkxl (date accessed: 11.04.2026).

3 Там само.

4 Там само.

to relevant data, it is often no longer available.

Cybercrime is fueled by persistence of darknet marketplaces and forums. These platforms are increasingly intertwined with *E2EE* platforms in a hybrid anonymity ecosystem. Cryptocurrencies remain a preferred payment method for cybercriminals, especially during ransomware attacks.

Online fraud by criminal groups targets as individuals as organizations to profit from schemes such as investment fraud, Business Email Compromise (*BEC*) and online payment fraud. With introduction of generative AI, fraudsters can personalize social engineering techniques and make them more convincing.

Ransomware remains the main threat in the EU, with over 120 active brands (according to Europol 2025). Extortion model continues to shift from data encryption to pressure victims to pay for non-disclosure of their data.

New technologies and monetization. Criminals are rapidly adapting to new technologies, making more difficult for law enforcement to track. Trafficking of child sexual abuse material for financial gain is on the rise, as are multi-level extortion models. Rise in AI-generated *CSAM* (*Child Sexual Abuse Material*) poses additional challenges.

Use of cryptocurrencies in cybercrime is growing rapidly. Criminals often prefer to use exchanges located in jurisdictions with weak Anti-Money Laundering (*AML*) protocols or in offshore financial centers [5].

In current conditions, the issue of neutralizing offenses related to the illegal VA circulation that currently is the most progressive and architecturally complex layer of cybercrime, is becoming particularly acute. Evolution of this area of illegal activity is taking place synchronously with the expansion of the digital economy and the introduction of the latest blockchain solutions. Such instruments as Bitcoin, Ethereum, Stablecoin, as well as *DeFi* services and NFT (non-fungible token), are increasingly becoming not only objects of investment, but also the main elements in schemes for the legalization of shadow capital, circumvention of financial monitoring mechanisms and material support for crime [6] (in particular, from international sanctions [7]).

Article Purpose

Reveal peculiarities of forensic characteristics of crimes related to illegal VA trafficking, as well as to identify the main elements of the mechanism of their commission.

Research Methods

Achievement of article purpose is ensured by comprehensive application of general scientific and special legal cognition methods. Dialectical method was useful for clarifying patterns that are revealed in the elements of the forensic characteristics of crimes related to illegal VA circulation.

5 IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026 / EUROPOL : web. 28 Apr 2026. DOI: 10.2813/5737847 (date accessed: 11.04.2026).

6 Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік / Кіберполіція України : офіц. вебсайт. 16.02.2026. URL: https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/ (date accessed: 11.04.2026).

7 Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume / Chainalysis : web. March 5, 2026. URL: https://live-chainalysis.pantheonsite.io/blog/crypto-sanctions-2026/ (date accessed: 11.04.2026).

Method of analysis and synthesis helped in processing scientific sources and practice-oriented approaches to international and national experience in investigation of transnational economic and cybercrimes, in particular, those related to the illegal VA circulation, as well as in identification of the main elements of forensic characteristics of crimes related to illegal circulation of virtual assets (subject of the crime, circumstances, time, place, methods of preparation, commission and concealment of crimes, criminal identity, etc.).

System-structural method made possible to form integral elements of the forensic characterization of crimes related to illegal VA circulation from transnational economic crimes, cybercrimes and legalization (laundering) of proceeds of crime using virtual currencies.

Formal legal method contributed to the analysis of national and international regulations on VA circulation, legalization (laundering) of proceeds from crime and fight against cybercrime.

Logical-dogmatic (logical-semantic) method was used to clarify content of categories: *method of preparation for crime, method of committing crime, method of concealing crime, crime traces* in the context of the forensic characterization of crimes related to illegal VA circulation, as well as to formulate conclusions.

Comparative legal method was useful for comparing scientific approaches to tactically ensuring interaction with victims in proceedings concerning serious and international crimes, as well as for taking into account international standards in the field of treating victims and protecting their rights in the context of potential mechanisms of international criminal justice. Modeling method helped to outline typical methods of preparing, committing and concealing crimes related to illicit VA trafficking.

Modeling method helped to outline typical methods of preparing, committing and concealing crimes related to the illegal VA trafficking.

Generalization method contributed to the systematization of results of processing of doctrinal sources and practical data and formulation of the author's conclusions regarding elements of the forensic characteristics of crimes related to the illegal VA circulation.

Analysis of Essential Researches and Publications

Researches on theoretical aspects of committing crimes related to illegal VA circulation have recently become increasingly interesting to scientists, as their number is constantly growing, as is the number of people whose lives have been affected by digital assets. Elements of forensic characteristics of crimes related to illegal VA circulation are fragmentarily disclosed in research papers by V. Bozhyk[8], A. Dolhov[9],

8 Божик В. І. Криміналістична характеристика легалізації майна, одержаного внаслідок ухилення від сплати податків: елементи та механізм злочинної діяльності. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2026. Вип. 93. Ч. 5. С. 28—34. DOI: 10.24144/2307-3322.2026.93.5.3 (date accessed: 08.04.2026).

9 Долгов А. Відповідальність за злочини, пов'язані з незаконним обігом крипто валют. *Ольвійський форум — 2025: стратегії країн Причорноморського регіону в геополітичному просторі* : мат-ли XXII Міжнар. наук. конф. (Миколаїв, 16—22.06.2025) / *Матеріали науково-практичних конференцій Чорноморського національного університету імені Петра Могили. Серія: Право.* 2025. № 1 (1). С. 40—43. DOI: 10.34132/mspc2025.01.11.08 (date accessed: 08.04.2026).

B. Derevianko [10], I. Zavydniak [11], M. Karchevskyi and co-authors [12], E. Maliutin [13], Ya. Nedilko [14], O. Kreminskyi [15], A. Movchan and V. Kozii [16], V. Sysoliatin [17] et al. The issue of international legal regulation of information security and formation of national criminal law policy in this regard is disclosed in the research paper by M. Karchevskyi and co-authors. In particular, the issue of information security in the field of information technology application in the context of VA use was considered. The scientists proposed a scientific and theoretical definition of information security, outlined the types of social relations that ensure it, and highlighted the issue of implementing international standards for combating criminal offenses in the field of information technology application and VA circulation [18].

In current conditions of global digitalization, cryptocurrencies are turning into a significant financial instrument, which, due to anonymity and cross-border nature, poses new challenges to economic security, including money laundering, terrorist financing and specific cybercrimes. Despite existence of international countermeasures and the adoption in Ukraine of

10 Деревянко Б. В. Ризики здійснення операцій з криптовалютою (біткойнами) громадян і суб'єктів господарювання України. *Форум права*. 2017. № 3. С. 33—39. URL: https://repository.ndippp.gov.ua/bitstream/handle/765432198/269/Derevyanko__FP_2017_3_8.pdf?sequence=1&isAllowed=y (date accessed: 07.05.2026).

11 Завидняк І. О. Особливості криміналістичної характеристики економічних транснаціональних злочинів, вчинених із використанням сучасних комп'ютерних технологій. *Аналітичне-порівняльне правознавство*. 2021. № 3. С. 178—183. DOI: 10.24144/2788-6018.2021.03.33 (date accessed: 08.04.2026).

12 Карчевський М. В., Шульженко Н. В., Куковинець Д. О. та ін. 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. Харків, 2023. 152 с. DOI: 10.31359/9789669986818 (date accessed: 11.04.2026).

13 Малютін Е. В. Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу : автореф. дис. … канд. юрид. наук. Дніпро, 2024. 26 с. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (date accessed: 08.04.2026).

14 Неділько Я. В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій : дис. … д-ра філос. в галузі права. Київ, 2023. 257 с. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content (date accessed: 08.04.2026).

15 Кремінський О. В. Розслідування легалізації (відмивання) доходів, отриманих злочинним шляхом, в умовах використання віртуальних валют : дис. … д-ра філос. в галузі права. Ірпінь, 2022. 229 с. URL: https://drive.google.com/file/d/1hRfh1Vp-mnRti_ftfs5eSfOSvhTI9rln/view (date accessed: 08.04.2026).

16 Мовчан А. В., Козій В. В. Основи розслідування злочинів щодо незаконного заволодіння криптовалютою. *Наука і правоохорона*. 2022. № 4 (58). С. 178—189. DOI: 10.36486/np.2022.4(58).17 (date accessed: 08.05.2026).

17 Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук. Київ, 2024. 230 с. URL: https://uacademic.info/ua/document/0423U100236 (date accessed: 08.04.2026).

18 Карчевський М. В., Шульженко Н. В., Куковинець Д. О. та ін. Зазнач твір. DOI: 10.31359/9789669986818 (date accessed: 11.04.2026).

the Law: *On Virtual Assets* [19] (hereinafter referred to as Law on VA), legal regulation remains fragmented, and the procedure of bringing to justice is complicated by anonymity of transactions, the use of mixers, jurisdictional conflicts and the lack of technical expertise in law enforcement agencies. A. Dolhov determined that overcoming these obstacles requires adapting national legislation to international standards, systematically improving digital competence of investigators and judges, and introducing specialized blockchain monitoring tools, which will allow for effective VA integration into official financial system while minimizing criminal risks [20].

In recent years, Ukrainian forensic science has significantly intensified research into the problems of investigating crimes related to VA. An example is O. Kreminskyi, who formed elements of a forensic characteristic of the legalization (laundering) of proceeds from crime in the use context of virtual currencies. The researcher determined that forensic characteristic of legalization of criminal proceeds with VA use of is based on complex, pre-planned schemes that include the stages of preparation, commission and active concealment of traces of the crime using crypto casinos (where up to three quarters of the funds are laundered), anonymous prepaid cards, crypto ATMs and game currencies in MMORPG games. Characteristic features of such crimes are anonymity of transactions, lack of linking of accounts to specific individuals, and the use of mixer services to obfuscate blockchain chains that allows entities with a high level of knowledge in IT fields and finance to effectively mask the sources of origin of funds (drug trafficking, fraud, corruption). Investigation procedure is significantly complicated by cross-border nature of operations, where the crime scene is both the location of the computer and the territory of a country with computing power and evidence base is often formed not only from digital traces, but also from paper drafts. Typical portrait of law enforcement officer-criminal is a lone initiator who acts as part of organized groups, guided by selfish motives and using gaps in the legislation and the anonymity of the crypto field to avoid responsibility [21].

Separate category is made up of crimes committed using information and computer technologies [22] and criminal offenses related to the use of e-banking [23]. Scientists have identified the main elements of the forensic characteristics and mechanisms of committing these offenses that are derivatives of many crimes related to illegal VA circulation.

In a separate research paper, I. Zavydniak formulated peculiarities of forensic characteristics of economic transnational crimes committed with use of modern

19 Про віртуальні активи : Закон України від 17.02.2022 р. № 2074-IX (зі змін. та допов.; не набрав чин.). URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (date accessed: 08.04.2026).

20 Долгов А. Зазнач твір. DOI: 10.34132/mspc2025.01.11.08 (date accessed: 08.04.2026).

21 Кремінський О. В. Зазнач твір. URL: https://drive.google.com/file/d/1hRfh1Vp-mnRti_ftfs5eSfOSvhTI9rln/view (date accessed: 08.04.2026).

22 Неділько Я. В. Зазнач. твір. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content (date accessed: 08.04.2026).

23 Малютін Е. В. Зазнач твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (date accessed: 08.04.2026) ; Сисолятін В. В. Зазнач. твір. URL: https://uacademic.info/ua/document/0423U100236 (date accessed: 08.04.2026).

computer technologies that can be defined as a separate category of crimes related to illegal VA circulation. Most of these crimes are usually fraud and by VA nature they are precisely of a cross-border nature [24].

Important for formation of scientific opinion on formation of methods and techniques for combating crimes related to the illegal circulation of VA are reports, recommendations and other analytical information from Ukrainian and international bodies that combat cybercrime, organized crime and corruption, as well as those engaged in financial monitoring with the aim of identifying signs of legalization (laundering) of funds obtained through criminal means.

At the same time, national scientific community lacks fundamental and multidisciplinary researches to determine elements of the forensic characteristics of criminal offenses related to illegal VA circulation. This necessitates the research on this issue and elucidation of its individual components.

Main Content Presentation

The main goal of forensic characterization is to optimize the procedure of crime detection and investigation. It can be imagined as an ideal model of typical connections and sources of evidentiary information that allows predicting optimal path and the most effective means of investigating individual categories of crimes [25].

First important element of forensic characteristic, I. Zavydniak calls the topic of criminal acts, since it has a direct impact on other elements and is a condition for certain methods of committing and concealing a crime, signs of identity of criminal (crimes) [26]. In our opinion, this statement is quite correct, since in our case a special topic, namely: VA that creates unique correlations. It is worth agreeing with the fact that only cryptocurrency can leave such traces as public keys of wallets, number of transferred VA, unique transaction hash, exact time of the transfer and commission amount.

Since VA are inherently specific data sets, nature analysis of computer information as their substantive basis is of particular importance. Despite the fact that criminal procedural legislation of Ukraine currently does not single out digital data as an individual category of evidence base, during investigation of relevant crimes, the main role is played by information traces, that after proper legal registration are transformed into full-fledged evidence. It should be emphasized that virtual nature of computer information is devoid of traditional material embodiment and becomes available for analysis only through the use of software and hardware tools that convert digital codes into a form understandable to human perception. In a broad sense, such information can be defined as a set of information that exists on electronic storage devices or is transmitted via network channels is subject to processing, modification and reproduction using computer systems and telecommunication networks [27].

24 Завидняк І. О. Зазнач. твір. DOI: 10.24144/2788-6018.2021.03.33 (date accessed: 08.04.2026).

25 Батюк О. В., Благута Р. І., Гумін О. М. та ін. Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ : навч. посіб. / за заг. ред. Є. В. Пряхіна. Львів, 2011. 324 с.

26 Завидняк І. О. Зазнач твір. DOI: 10.24144/2788-6018.2021.03.33 (date accessed: 08.04.2026).

27 Мазуренко О., Розенфельд Н. Комп'ютерна інформація як предмет правопорушень, передбачених Розділом XVI КК України. *Право України.* 2004. Т. 6. С. 80—83.

Legal VA nature in Ukraine, even without entry into force of the Law on VA is in the realm of legal relations, since according to Article 177 of Civil Code of Ukraine:

"1. Objects of civil rights are things, money, securities, digital things, property rights, works and services, results of intellectual and creative activity, information, as well as other tangible and intangible benefits.

2. Objects of civil rights can exist in material world and/or digital environment determining the form of objects, acquisition peculiarities, exercise and termination of civil rights and obligations in relation to" [28].

In addition, according to Article 179-1 of Civil Code of Ukraine [29], VA is a digital thing and the courts do not have any issues with protecting the rights of victims in the event of seizure of their property in VA form.

If we consider the most common VAs as the topic of crime: cryptocurrencies then among them the most prominent place is occupied by convertible currencies that have an equivalent value in fiat currency and can be exchanged for regular money. In modern classification of digital assets, they include *Bitcoin and E-Gold*. Non-convertible currencies are usually limited to the ecosystem of specific software. By their nature, they are similar to virtual money in video games; in lack of objective market price, they rarely become an object of interest for offenders. However, there are mechanisms for converting such closed systems into open ones using unofficial exchange channels that de facto makes them convertible despite the developers' rules [30].

One of the objective conditions for committing criminal offenses related to illicit VA trafficking usually committed by transnational organized criminal groups is the clear determination of this type of crime by the objective situation in the world and in legislation of many countries [31].

As noted by Ya. Nedilko, in the situation structure of such criminal offenses, based on their peculiarities, one should distinguish: cyberspace, characterized by place, time, virtual interaction of participants in a criminal offense; material environment, namely: section of territory, set of various objects, behavior of event participants, psychological relationships [32].

Crime scene as a complex of material elements at the scene of the crime allows to reconstruct the criminal act algorithm and the specifics of the behavior of its subjects. Crimes in the area under research are characterized by an exceptional level of intellectual preparation and the use of multi-level methods of indirect influence on digital systems that significantly complicates recording of facts of unauthorized access. Characteristic sign of such acts is territorial disunity: location where the criminal plan (active actions) is directly implemented usually does not geographically coincide with the place of occurrence of socially dangerous consequences.

28 Цивільний кодекс України від 16.01.2003 р. № 435-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (date accessed: 08.04.2026).

29 Там само.

30 Громек М. Розшифровка криптозлочинів : посіб. для правоохорон. орган. / OSCE : web. 2024. 64 с. URL: https://oceea.osce.org/sites/default/files/f/documents/b/c/601719.pdf (date accessed: 08.04.2026).

31 Цивільний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (date accessed: 08.04.2026).

32 Неділько Я. В. Зазнач. твір. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content (date accessed: 08.04.2026).

Given cross-border nature of cybercrimes and difficulties (and sometimes impossibility) of identifying the physical point from which the intervention was carried out, in forensic and judicial practice it is advisable to consider commission place of the crime to be the territory where harmful results of the illegal activity actually occurred [33].

E. Maliutin identified and characterized the places where criminal acts related to the use of e-banking were committed, which are correlated with cybercrimes of illegal VA appropriation: places where devices were located that were used to commit illegal acts (smartphone, computer, laptop, tablet) – 74%; places where ATMs, banks and other financial institutions were located – 16%; place of residence of the victim, who was targeted by illegal acts, – 9% [34].

Temporal circumstances are certain peculiarities crime commission at a certain daytime, on certain days, months and years. Commission of crimes we are considering usually begins with illegal access to information. The latter is carried out while computer is working, it is not limited to a certain time period, since automated information systems can operate around the clock [35]. However, each method of committing such crimes, associated with the use of modern computer technologies has certain temporal features, since there is usually a difference in time and in the case of committing such criminal offenses at night, it can be assumed that the perpetrators are acting in a different time zone, where it is daytime at that time.

As for the methods of preparation for committing crimes of the type under research, the following can be distinguished: production of spy hardware or software for illegal use during operations to steal personal information; sale or distribution without necessary permission on Internet of information that is important during operations with VA creation of sites with appropriate topics for fraudulent schemes (pseudo-exchanges, pseudo-exchange services, dating sites, etc.) [36].

There are a large number of ways to commit crimes related to illegal VA trafficking, consequently within the framework of this research paper we will consider several positions of scientists on this topic and the most common methods used by criminals around the world.

According to A. Dolhov, the methods of committing fraud using VA include the following phenomena: *rug pull* (sudden disappearance of liquidity, i.e. artificially inflating the price of a crypto asset with its subsequent collapse due to the sale of its bulk), *NFT* fraud (forgery, plagiarism of unique VAs) and *DeFi* exploits (use of protocol vulnerabilities to hack digital services and VA steal) [37].

B. Derevianko considers the following two ways of committing VA fraud: stealing information about the *ID*-wallet and password from it; illegal transfer of information about the *ID*-wallet and password of the bitcoin owner to third parties by the

33 Завидняк І. О. Зазнач. твір. DOI: 10.24144/2788-6018.2021.03.33 (date accessed: 08.04.2026).
34 Малютін Е. В. Зазнач. твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (date accessed: 08.04.2026).
35 Панов М. І., Шепітько В. Ю., Коновалова В. О. та ін. Настільна книга слідчого : наук.-практ. вид. для слідч. і дізнавач. 2-ге вид., перероб. і допов. Київ, 2007. 728 с.
36 Малютін Е. В. Зазнач. твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (date accessed: 08.04.2026).
37 Долгов А. Зазнач твір. DOI: 10.34132/mspc2025.01.11.08 (date accessed: 08.04.2026).

wallet hosting service provider itself. Although such services state on their websites and in the contract that they are not interested in the password of the cryptocurrency owner, there are still serious doubts about this. And undeniable legal risk is the risk of unilaterally changing the terms of the contract and/or introducing paid services by the electronic wallet hosting service provider [38].

A. Movchan and V. Kozii distinguish the following ways of committing criminal offenses related to the illegal circulation of crypto assets:

1) hacking cryptocurrency exchanges and electronic wallets of individuals and withdrawing cryptocurrency from exchanges, exchange resources or other electronic wallets;
2) staging cryptocurrency theft by exchanges themselves;
3) fraudulent actions:
   - voluntary transfer of assets by victims to fictitious services controlled by attackers. The result is a complete loss of access to resources: either due to software manipulations that display a zero balance in the user's account, or due to the sudden termination of the service (exit scam), when operators disappear along with entrusted assets;
   - theft of confidential information through phishing attacks. This is an online fraud method aimed at gaining unauthorized access to cryptocurrency exchange accounts or private keys of electronic wallets by inducing victims to go to a fake page and enter their login and password that allows to instantly empty their balance;
   - manipulative schemes such as Scam (fraud). Essence is to release a new token to the market, the value of which the organizers artificially increase. By investing significant resources in marketing hype on social networks and simulating a rapid increase in price, swindlers attract a mass of small investors. When asset value reaches peak values, organizers massively sell off their own stocks, receiving excess profits. As a result, the price instantly collapses and investors are left with illiquid digital units that have no real value;
   - issuance of imitation tokens (clones). Offenders create digital coin whose name completely copies or is as similar as possible to the name of a promising project that has not yet been listed on major exchanges. Actively advertising such an "analogue" in messengers and social groups, fraudsters provide links to their own smart contracts: investors mistakenly buy a counterfeit that has no relation to the real project and cannot be implemented on the market [39].

According to *Chainalysis* (*2026 Crypto Crime Report*), the most popular methods of criminal offenses related to illegal VA circulation are fraud, such as:

1) Phishing clones of exchangers. Fraudsters create copies of websites of well-known exchangers. Exter-

38 Деревянко Б. В. Зазнач. твір. URL: https://repository.ndippp.gov.ua/bitstream/handle/765432198/269/Derevyanko__FP_2017_3_8.pdf?sequence=1&isAllowed=y (date accessed: 07.05.2026).

39 Мовчан А. В., Козій В. В. Зазнач. твір. DOI: 10.36486/np.2022.4(58).17 (date accessed: 08.05.2026).

nally, pages look almost identical due to the same design, application form and rate (the domain differs by one character; there are no official contacts or exchange rules; the offer "the best rate only today");

2) Changing details in correspondence. The exchange is agreed upon in a chat or messenger, after that other party suddenly informs that details have changed (details are changed at the last moment; the other party asks to switch to another chat or contact; the data is sent as an image, not as text). This may look mundane, for example, "sorry, the previous wallet is temporarily unavailable," "use another account," etc. If the user does not check the details, cryptocurrency is sent to the scammer's address;
3) Fake payment confirmation. After agreeing on the exchange, the swindler sends a screenshot of supposedly made payment. Then pressure begins, saying that money has already been sent, so you need to transfer the cryptocurrency immediately and not wait for it to arrive.
4) QR code or wallet address spoofing. QR code or address for transferring cryptocurrency is sent to the user. In fact, they lead to the scammer's wallet. This happens when addresses are copied through third-party services or received in chats without verification (they ask to install a "special" extension or software; they offer to connect via remote access; address looks unfamiliar or differs from the previously agreed upon);
5) Manipulation of the rate after application. Initially, a rate is offered that looks slightly more favorable than market rate. When the user has already sent cryptocurrency, additional conditions appear. Often this is an additional verification fee, acceleration fee, a new rate. In the end, amount received is much less than expected;
6) Fake support service. Fraudsters pretend to be service employees or platform moderators. They write to the user and report a supposed problem with the transaction. Then they try to gain access to the wallet, asking for a seed phrase, *2FA* codes, access to the device or wallet.
7) Fake guarantor. In *Telegram* or another messenger, they offer to perform an exchange with the help of a guarantor who will supposedly control the transaction and hold the funds until the transaction is completed. In fact, guarantor can be part of a fraudulent scheme. He insists on a quick transaction and has no proven reputation outside of this dialog;
8) Network or token swapping. The user is asked to send cryptocurrency via a different network or to a different token. For example, instead of *USDT TRC20*, *USDT ERC20* is offered or details for *USDT* are sent on a network that the user's wallet does not support. As a result, funds can "hang" or be difficult to return. Network changes simply during transaction and the explanation seems rushed or unclear;
9) risks of cash exchange. The exchange is carried out during a personal meeting. Problems arise at the moment of money transfer, where there are possible underpayments, substitution of banknotes, or other manipulations (meeting is arranged

in a random place; attempts are made to speed up the transfer of money; it is prevented from calmly counting and checking banknotes);

10) Fake *AML* verification. After receiving cryptocurrency, the user is informed that funds have allegedly been subject to *AML* verification and an additional payment is demanded, justified by a mandatory deposit, tax or verification fee and the promise that transaction will be unblocked after that. The main sign is the requirement for additional payment and the lack of a pre-known verification procedure [40].

We propose to combine the methods of committing such criminal offenses into groups: *"digitized" crimes* related to the illegal VA circulation (committed exclusively using cybernetic methods) and classic crimes (for example, kidnapping with subsequent ransom in VA form, intentional murder with the aim of taking possession of the victim's VA, etc.).

As for the methods of money laundering, almost all cross-border organized criminal groups launder money using VA and offshore jurisdictions that are the most common methods in the final phase related to tax evasion and concealment of traces. As V. Bozhyk notes, in 87% of criminal proceedings everything happens according to the following scheme: offshore, fictitious entrepreneurship ("conversion centers"), formation of scheme tax credit, violation of customs rules and smuggling, counterfeiting, withdrawal of profits through pseudo-entrepreneurship of individuals, an individual, understatement of turnover [41].

A new and popular way to legalize criminal proceeds is to launder them using gambling sites. It is through these services that almost three quarters of all dirty virtual money is laundered. According to *Trend Micro*, criminals are increasingly turning to game currency as a way to store the value of cryptocurrency. For this purpose, they buy currency of the most popular virtual games for cryptocurrency and then exchange it for fiat currency on special conversion services [42].

Another way to conceal criminal offenses related to the illegal VA circulation is the use of decentralized exchanges, over-the-counter (*OTC*) exchanges, mixers and tumblers. This technology was developed to hide traces of users' transactions. Many OSCE participating States are taking measures to restrict the use of such tools. Mixers and tumblers are services designed to increase the confidentiality and anonymity of cryptocurrency transactions. Their main function is to mix funds from different users, which masks the source of the funds [43].

Individuals of criminals in the type of crimes under research can be conditionally divided into three groups. The first group consists of individuals who combine

40 10 схем шахрайства при обміні криптовалюти у 2026 році: як розпізнати та захиститися / Finance.ua : вебсайт. 25.03.2026. URL: https://finance.ua/ua/goodtoknow/10-skhem-shakhraistva-pry-obmini-kryptovaliuty-u-2026-rotsi-yak-rozpiznaty-ta-zakhystytysia (date accessed: 08.04.2026).

41 Божик В. І. Зазнач твір. DOI: 10.24144/2307-3322.2026.93.5.3 (date accessed: 08.04.2026).

42 Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing : FATF Report / FATF : web. Sept. 2020. 24 p. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf (date accessed: 07.05.2026).

43 Громек М. Зазнач. твір. URL: https://oceea.osce.org/sites/default/files/f/documents/b/c/601719.pdf (date accessed: 08.04.2026).

a high level of professional training in the field of information technology and programming with unconventional thinking, technical ingenuity and a certain tendency to professional excitement. For them, computer systems are not only a tool for work, but environment for realization of their own intellectual capabilities. This group can include employees of cryptocurrency exchanges, VA issuing companies, as well as specialists from technical companies that provide relevant structures with cloud, artificial intelligence and other digital services.

The second group includes professional cybercriminals, whose activities are clearly of a self-interested nature. It is this category that poses one of the greatest threats both to individual business entities and to international economic security in general. Representatives of this group often form the core of transnational criminal groups that use modern information technologies to commit economic crimes on a significant scale.

The third group is the so-called respectable offenders: individuals who have legal professional status and specialized knowledge in the field of finance, accounting or programming. They can include accountants, economists and programmers who use their professional skills to prepare and implement criminal schemes aimed primarily at obtaining material benefit [44].

It should be emphasized that economic transnational crimes with use of modern computer technologies are usually committed by organized criminal groups. Thereby it is proposed to investigate the persons who committed them *"according to the scheme: 1) general offender peculiarities who committed an economic transnational crime, using computer technologies, and 2) peculiarities of persons who committed certain types of such crimes, taking into account the distribution of roles in an organized criminal group"* [45].

The most common motive for committing crimes in this category is selfish considerations, very rarely revenge. Persons capable of doing so pose a serious threat to the economy of any State and the international community as a whole [46].

The most important primary traces of crimes related to illegal VA circulation are contained in blockchain. Open information includes: sender and recipient addresses (public keys of wallets), transfer amount (number of tokens or cryptocurrency), transaction hash (unique identifier by which the record can be found), timestamp (exact time of transaction confirmation), commission. These traces will be present in case of using regular cryptocurrency, however, there are anonymous coins *(monero, zcash, dash, xeonbit)* that are difficult to track, since they use a specific modification of the blockchain aimed at ensuring anonymity and confidentiality of transactions.

Summarizing the above, it should be emphasized that for such criminal offenses, typical sign is availability of digital or electronic traces that arise while applying information technologies. Such information can include user accounts, memory of computer equipment and other electronic devices, profiles on social networks, resources for communicating or exchanging information on cryptocurrencies, databases of telecommunications operators

44 Завидняк І. О. Зазнач. твір. DOI: 10.24144/2788-6018.2021.03.33 (date accessed: 08.04.2026).
45 Там само.
46 Там само.

and Internet providers, as well as removable media, including *USB*-drives [47].

If the victim has had contact with the offender in person or via video link, he or she can be able to provide information about the offender's physical appearance and other characteristics [48]. Unfortunately, most often the victim does not have visual contact with the offender [49].

Conclusions

Performed research made possible to reveal the main elements of the forensic characteristics of criminal offenses related to illegal VA circulation and to determine their specific peculiarities in the conditions of modern digitalization of society. It was found that VA as a subject of criminal encroachment form a special mechanism of criminal activity, which is characterized by the use of information technologies, cross-border operations, a high level of latency and the complexity of identifying and documenting evidentiary information.

It has been determined that the main source of evidentiary information in such criminal offenses is digital traces that can be contained in blockchain, electronic wallets, user accounts, computer memory, messengers, social networks, databases of telecommunications operators and Internet providers. At the same time, peculiarities of functioning of anonymous cryptocurrencies, mixers, toggle switches and decentralized platforms significantly complicate establishing source of origin of assets and the route of their movement.

As an analysis result of the methods of committing criminal offenses under investigation, it was found that the most common are various forms of fraud, phishing attacks, hacking of cryptocurrency exchanges and electronic wallets, manipulation of tokens, use of fictitious platforms and services, as well as legalization of income through cryptocurrency services, online casinos and offshore jurisdictions. It was determined that criminal activity in this area is often carried out by organized transnational groups with a clear division of roles between participants.

The research on offender's personality made possible to identify several typical categories of subjects of such crimes: technically trained specialists in the field of IT, professional cybercriminals and individuals with legal professional status who apply specific expertise in financial or technical fields to implement criminal schemes. Common sign of most offenders is a high level of digital competence and orientation towards obtaining tangible benefits.

Thus, criminal offenses related to the illegal VA circulation are a complex multi-level phenomenon that combines elements of cybercrime, economic crime and transnational organized activity. This necessitates further development of forensic methods for their detection and investigation, improvement of legislative regulation in the sphere of VA circulation and improvement of the level of technical training of law enforcement agencies in working with digital evidence and blockchain technologies.

47 Сисолятін В. В. Зазнач. твір. URL: https://uacademic.info/ua/document/0423U100236 (date accessed: 08.04.2026).

48 Малютін Е. В. Зазнач. твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (date accessed: 08.04.2026).

49 Сисолятін В. В. Зазнач. твір. URL: https://uacademic.info/ua/document/0423U100236 (date accessed: 08.04.2026).

Криміналістична характеристика кримінальних правопорушень, пов'язаних з незаконним обігом віртуальних активів

Дмитро Нестеров

Мета статті — розкрити особливості криміналістичної характеристики злочинів, пов'язаних з незаконним обігом віртуальних активів, а також визначити основні елементи механізму їх скоєння. Для досягнення поставленої мети застосовано комплекс загальнонаукових і спеціально-юридичних методів пізнання, зокрема діалектичний, системно-структурний, формально-юридичний, порівняльно-правовий, логіко-семантичний, аналізу й синтезу, моделювання й узагальнення. Статтю присвячено дослідженню криміналістичної характеристики кримінальних правопорушень, пов'язаних з незаконним обігом віртуальних активів, що в умовах глобальної цифровізації та стрімкого розвитку інформаційних технологій набувають дедалі більшої суспільної небезпеки. Актуальність теми обумовлена активним використанням криптовалют, децентралізованих фінансових сервісів, анонімних платіжних інструментів і технологій штучного інтелекту в механізмах учинення шахрайств, кіберзлочинів і легалізації доходів, одержаних злочинним шляхом. Зростання рівня транснаціональної кіберзлочинності, поширення фішингових схем, користування міксерами, тумблерами, офшорними юрисдикціями та платформами із наскрізним шифруванням створюють істотні труднощі для правоохоронних органів під час виявлення, документування й розслідування таких правопорушень. Особливу увагу приділено проблемам формування доказової бази, пов'язаним з віртуальною природою цифрових слідів і складністю ідентифікації осіб, причетних до незаконних операцій з віртуальними активами. У результаті проведеного дослідження визначено, що віртуальні активи як предмет злочинного посягання формують специфічний механізм злочинної діяльності, для якого характерними є високий рівень латентності, транскордонність, застосування сучасних інформаційних технологій і складність локалізації місця вчинення кримінального правопорушення. Обґрунтовано, що вирішальне значення для розслідування мають цифрові сліди, що їх містять блокчейн, електронні гаманці, акаунти користувачів, пам'ять комп'ютерної техніки, месенджери, соціальні мережі, бази даних операторів зв'язку й інтернет-провайдерів. Проаналізовано найбільш поширені способи скоєння злочинів, пов'язаних з незаконним обігом віртуальних активів, поміж яких фішингові атаки, злам криптовалютних бірж і електронних гаманців, користування фейковими платформами, маніпуляції з токенами, шахрайські інвестиційні проєкти, DeFi-експлойти, NFT-шахрайство й легалізація доходів за допомогою криптовалютних сервісів і онлайн-казино. Доведено, що значну частину таких правопорушень здійснюють транснаціональні організовані злочинні угруповання із чітким розподілом ролей між учасниками. Аргументовано, що особа правопорушника в цій категорії злочинів характеризується високим рівнем цифрової компетентності, спеціальними знаннями у сфері інформаційних технологій, програмування або фінансів і орієнтуванням на отримання матеріальної вигоди. Запропоновано класифікувати суб'єктів таких кримінальних правопорушень як технічно підготовлених спеціалістів, професійних кіберзлочинців і осіб з легальним професійним статусом, які застосовують свої знання для реалізації злочинних схем. Зроблено висновок, що кримінальні правопорушення, пов'язані з незаконним обігом віртуальних активів,

є складним багаторівневим явищем, яке поєднує ознаки кіберзлочинності, економічної злочинності та транснаціональної організованої діяльності. Наголошено на необхідності подальшого розвитку криміналістичних методик розслідування, удосконалення законодавчого регулювання обігу віртуальних активів і підвищення рівня технічної підготовки правоохоронних органів у сфері роботи із цифровими доказами й технологіями блокчейну.

Ключові слова: *віртуальний актив; блокчейн; транскордонні злочини; легалізація (відмивання) грошей, здобутих злочинним шляхом; шахрайство; крадіжка; криміналістична характеристика; незаконний обіг.*

Financing

This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer

Founders had no role in the research design, data collection and analysis, decision to publish or manuscript preparation.

Participants

Author contributed solely to the intellectual discussion underlying this document, case law research, writing and editing and assumes responsibility for its content and interpretation.

Declaration of Competing Interest

Author declares no conflict of interest.

References

10 skhem shakhraistva pry obmini kryptovaliuty u 2026 rotsi: yak rozpiznaty ta zakhystytysia [10 Cryptocurrency Exchange Scams in 2026: How to Recognize and Protect Yourself] (2026) / Finance.ua : vebsait. 25.03. URL: https://finance.ua/ua/goodtoknow/10-skhem-shakhraistva-pry-obmini-kryptovaliuty-u-2026-rotsi-yak-rozpiznaty-ta-zakhystytysia [in Ukrainian].

Batiuk, O. V., Blahuta, R. I., Humin, O. M. ta in. (2011). *Metodyka rozsliduvannia okremykh vydiv zlochyniv, pidslidnykh orhanam vnutrishnikh sprav* [Methods for investigating certain types of crimes under investigation by internal affairs bodies] : navch. posib. / za zah. red. Ye. V. Priakhina. Lviv [in Ukrainian].

Bozhyk, V. I. (2026). Kryminalistychna kharakterystyka lehalizatsii maina, oderzhanoho vnaslidok ukhylennia vid splaty podatkiv: elementy ta mekhanizm zlochynnoi diialnosti [Forensic characteristics of property laundering resulting from tax evasion: structural elements and mechanisms of criminal activity]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pavo*. Vyp. 93. Ch. 5. DOI: 10.24144/2307-3322.2026.93.5.3 [in Ukrainian].

Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume (2026) / Chainalysis : web. March 5. URL: https://live-chainalysis.pantheonsite.io/blog/crypto-sanctions-2026/.

Cyber-Enabled Fraud. Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks. February 2026 (2026) / FATF : web. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cyber-Enabled-Fraud%E2%80%93Digitalisation-and-ML-TF-PF-Risks.pdf.coredownload.inline.pdf.

Derevianko, B. V. (2017). Ryzyky zdiisnennia operatsii z kryptovaliutoiu (bitkoinamy) hromadian i sub'iektiv hospodariuvannia Ukrainy [Risks of Operations with Cryptocurrency (Bitcoins) for Citizens and Economic Entities of Ukraine]. *Forum prava.* № 3. URL: https://repository.ndipp.gov.ua/bitstream/handle/765432198/269/Derevyanko__FP_2017_3_8.pdf?sequence=1&isAllowed=y [in Ukrainian].

Dolhov, A. (2025). Vidpovidalnist za zlochyny, pov'iazani z nezakonnym obihom krypto valiut [Liability for crimes related to the illicit trafficking of cryptocurrencies].

Olviiskyi forum — 2025: stratehii krain Prychornomorskoho rehionu v heopolitychnomu prostori : mat-ly XXII Mizhnar. nauk. konf. (Mykolaiv, 16—22.06.2025) / *Materialy naukovo-praktychnykh konferentsii Chornomorskoho natsionalnoho universytetu imeni Petra Mohyly. Seriia: Pravo.* № 1 (1). DOI: 10.34132/mspc2025.01.11.08 [in Ukrainian].

Hromek, M. (2024). *Rozshyfrovka kryptozlochyniv* [Decrypting cryptocrimes] : posib. dlia pravookhoron. orhan. / OSCE : web. URL: https://oceea.osce.org/sites/default/files/f/documents/b/c/601719.pdf [in Ukrainian].

IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026 (2026) / EUROPOL : web. 28 Apr. DOI: 10.2813/5737847.

Karchevskyi, M. V., Shulzhenko, N. V., Kukovynets, D. O. ta in. (2023). *Mizhnarodni standarty ta natsionalna kryminalno-pravova polityka u sferi okhorony informatsiinoi bezpeky* [International standards and national criminal law policy in the field of information security protection] : monohrafiia / za zah. red. V. I. Borysova, M. V. Karchevskoho, M. V. Shepitka. Kharkiv. DOI: 10.31359/9789669986818 [in Ukrainian].

Kreminskyi, O. V. (2022). *Rozsliduvannia lehalizatsii (vidmyvannia) dokhodiv, otrymanykh zlochynnym shliakhom, v umovakh vykorystannia virtualnykh valiut* [Investigation of legalization (laundering) of criminal income by use virtual currencies] : dys. … d-ra filos. v haluzi prava. Irpin. URL: https://drive.google.com/file/d/1hRfh1Vp-mnRti_ftfs5eSfOSvhTI9rln/view [in Ukrainian].

Maliutin, E. V. (2024). *Osnovy metodyky rozsliduvannia kryminalnykh pravoporushen, pov'iazanykh iz vykorystanniam e-bankinhu* [Basics of the methodology of investigation of criminal offenses related to the use of e-banking] : avtoref. dys. … kand. yuryd. nauk. Dnipro. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-prozahist-disertatsij/malyutin/ [in Ukrainian].

Mazurenko, O., Rozenfeld, N. (2004). Komp'iuterna informatsiia yak predmet pravoporushen, peredbachenykh Rozdilom XVI KK Ukrainy [Computer information as the subject of offenses provided for in Chapter XVI of Criminal Code of Ukraine]. *Pravo Ukrainy*. T. 6 [in Ukrainian].

Movchan, A. V., Kozii, V. V. (2022). Osnovy rozsliduvannia zlochyniv shchodo nezakonnoho zavolodinnia kryptovaliutoiu [Fundamentals of investigation crimes regarding illegal possession of cryptocurrency]. *Nauka i pravookhorona.* № 4 (58). DOI: 10.36486/np.2022.4(58).17 [in Ukrainian].

Nedilko, Ya. V. (2023). *Rozsliduvannia kryminalnykh pravoporushen, shcho vchyniaiutsia z vykorystanniam informatsiinykh komp'iuternykh tekhnolohii* [Investigation of criminal offenses committed using information computer technologies] : dys. … d-ra filos. v haluzi prava. Kyiv. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content [in Ukrainian].

Panov, M. I., Shepitko, V. Yu., Konovalova, V. O. ta in. (2007). *Nastilna knyha slidchoho* [The Handbook for an Investigator] : nauk.-prakt. vyd. dlia slidch. i diznavach. 2-he vyd., pererob. i dopov. Kyiv [in Ukrainian].

Shchorichnyi zvit Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy za 2025 rik [Annual report of the Cyber Police Department of National Police of Ukraine for 2025] (2026) / Kiberpolitsiia Ukrainy : ofits. vebsait. 16.02. URL: https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/ [in Ukrainian].

Sysoliatin, V. V. (2024). *Rozsliduvannia kryminalnykh pravoporushen, pov'iazanykh iz vykorystanniam internet-bankinhu*

[Investigation of criminal offenses related with the using of Internet banking] : dys. ... kand. yuryd. nauk. Kyiv. URL: https://uacademic.info/ua/document/0423U100236 [in Ukrainian].

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020) : FATF Report / FATF : web. Sept. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf.

Zavydniak, I. O. (2021). Osoblyvosti kryminalistychnoi kharakterystyky ekonomichnykh transnatsionalnykh zlochyniv, vchynenykh iz vykorystanniam suchasnykh komp'iuternykh tekhnolohii [Features of the criminalistic characteristics of economic transnational crimes committed with the use of modern computer technologies]. *Analitychne-porivnialne pravoznavstvo*. № 3. DOI: 10.24144/2788-6018.2021.03.33 [in Ukrainian].

Nesterov, D. (2026). Forensic Characteristics of Criminal Offenses Related to Illegal Circulation of Virtual Assets. *Theory and Practice of Forensic Science and Criminalistics.* Issue 2 (43). Pp. 184—202. DOI: 10.32353/khrife.2.2026.12.