UDC 343.1:004.9(477)
Doi: 10.63341/naia-chasopis/1.2026.47

ISSN 2519-4216
E-ISSN 2519-4313

Digital evolution of forensic methods for investigating criminal offences in the field of official activity in Ukraine

Oleksandr Amelin*
PhD in Law, Associate Professor
Office of the Prosecutor General
01011, 13/15 Riznytska Str., Kyiv, Ukraine
State Tax University
08201, 31 Universytetska Str., Irpin, Ukraine
https://orcid.org/0000-0002-0933-2111

Abstract
The purpose of the study was to analyse the capabilities of digital forensics in investigating official offences by integrating international standards and forensic-by-design concepts with Ukrainian criminal procedural legislation. A comparative legal analysis of international and Ukrainian standards of digital forensics revealed a systemic gap between technical standards and procedural and judicial practice, where courts practically do not articulate the requirements for forensically correct handling of digital evidence. The systematic classification of digital traces by types of official offences in criminal legislation allowed systematising specific sources of origin, types of digital traces, and typical threats to the integrity of evidence for each element of official offence in the context of large-scale digitalisation of the public sector. The case study method was used to examine the judicial practice of Ukraine, the United States of America, and Germany regarding the use of digital evidence in cases of official offences, which made it possible to establish the absence of references to international standards of digital forensics in the motivational parts of Ukrainian court decisions and to identify gaps in the procedural design of electronic evidence that make it impossible to verify the authenticity and integrity in accordance with the requirements of ISO/IEC 27037:2012. A four-block algorithm for the digital forensics methodology for investigating official offences related to official forgery (Article 366 of the Criminal Code of Ukraine) was developed, which includes forensically oriented initial recording of the digital situation, identification of relevant sources of digital evidence, forensically correct acquisition and analysis, and presentation of evidence in court with compliance with the procedures of the chain of custody. The practical significance of the research results lies in the possibility of the use by the legislator to amend criminal procedural legislation, by law enforcement agencies to create specialised units in the field of investigating official offences using digital forensics, as well as by higher education institutions to introduce relevant educational components into legal education

Keywords:
electronic evidence; digital traces; forensic-by-design; international standards; state information systems; evidence; forensic copy

Article's History:
Received: 28.10.2025
Revised: 30.01.2026
Accepted: 31.03.2026
Published: 03.04.2026

Suggest Citation:
Amelin, O. (2026). Digital evolution of forensic methods for investigating criminal offences in the field of official activity in Ukraine. *Law Journal of the National Academy of Internal Affairs*, 16(1), 47-64. doi: 10.63341/naia-chasopis/1.2026.47.

*Corresponding author

Introduction

The digital transformation of the public sector changed the ways in which official offences are committed and the logic of the investigation: electronic document management, qualified electronic signatures, departmental registers and logs of access to information systems formed a qualitatively new array of digital traces of official abuses. The growing role of electronic evidence in cases of official forgery, illegal changes in registers and unauthorised use of official access to state databases is accompanied by a lack of methodological support in Ukraine, where investigators mostly do not have clear algorithms for working with digital traces. At the same time, the concepts of forensic-by-design and digital forensic readiness are being formed in the member states of the European Union and the United States of America, when requirements for the preservation of access logs and traceability of actions of officials are built into state information systems at the design stage. In the member states of the European Union (EU), the analysis of access logs and the history of changes in registers allowed to identify a specific employee and reconstruct the full mechanism of the service scheme (European Union Agency for Cybersecurity, 2025), while in Ukraine similar opportunities remained unrealised due to insufficient formalisation of procedural approaches. Under such conditions, the digital evolution of the forensic methodology of investigating official offences became important for improving the quality of evidence and adapting national practice to international standards of work with electronic evidence.

In modern Ukrainian procedural doctrine, the study of V.M. Fihurskyi (2023) was of fundamental importance for understanding the nature of electronic evidence, who showed that evidence in electronic form constituted a new socio-legal phenomenon and, in its properties, was not reduced to traditional documents or physical evidence. The scientist proved that the intangible nature of digital data, the dependence of the perception on a special software and technical environment, and the vulnerability to manipulation necessitated the separation as an independent procedural source, which required a rethinking of the usual rules for collecting, verifying, and evaluating evidence in criminal proceedings. In developing this position, L.V. Milimko & Y.V. Zhydovtsev (2025), analysing the practice of Ukrainian courts, established that electronic evidence has actually become a central element of evidence in cybercrime cases, but the procedural status remained unclear, which gave rise to contradictory approaches to the authenticity and admissibility of digital files, logs, screenshots, and data from cloud services.

O.D. Kvashuk (2025) also contributed to the understanding of the practical consequences of digitalisation for evidence, showing that based on case law the key problems remained non-compliance with the procedures for the extraction and fixation of electronic evidence, the vulnerability of the chain of custody, as well as the lack of unified approaches to expert verification of the authenticity of electronic documents and log files, on this basis justifying the need to develop standardised protocols for investigators' work with digital media. O.G. Predmestnikov & A.R. Bekhter (2024) demonstrated that the introduction of automated document management systems and video recording of procedural actions significantly changed the very structure of evidentiary material, shifting the emphasis from traditional paper documentation to digital traces of the activities of the participants in the proceedings, however, without proper forensic adaptation, these technologies could remain neutral from the point of view of the investigation.

Directly related to official offences was the cycle of works by T. Chepurna (2025), who, analysing the investigation of crimes committed by law enforcement officers, showed that the typical mechanism of such acts was almost always accompanied by digital traces from official electronic correspondence and changes in departmental registers to the use of departmental information systems to mask illegal actions. The author proved that during the inspection of the scene of the incident in cases of official offences, not only traditional material objects were of central importance, but also the digital environment of workstations, servers, and employee profiles in internal systems, and therefore the inspection took on the features of a complex digital-physical investigative inspection.

International studies focused on digital evidence and forensic-by-design demonstrated the regulatory and organisational horizon to which developed law enforcement agencies aspired. A. Akilal & M. Kechadi (2021), developing the idea of forensic-by-design in cloud systems, proposed an engineering framework within which the requirements for preserving digital traces, logging operations, and traceability of user actions were built into the system at the design stage, which allowed significantly increasing the evidentiary value of electronic traces. V. Kebande *et al*. (2021), substantiating the concept of digital forensic readiness, demonstrated that organisations that created intelligent repositories of potential digital evidence in advance were able to meet the needs of the investigation in complex cyber incidents much faster and more fully. F.I. Fagbola & H.S. Venter (2022), modelling intelligent digital forensic readiness for IoT infrastructure in smart cities, showed that proactive logging and automated anomaly detection not only facilitated further evidence collection, but also actually built a preventive component into the systems. T. Loskutov *et al*. (2023), considering the information and analytical support of the investigation of corruption offences, demonstrated that modern anti-corruption investigations are already unthinkable without the use of hybrid cybernetic

methods, where electronic evidence became the basis for building cross-border evidentiary chains. However, even in these studies, attention was focused primarily on the organisational, legal and technical aspects of digital evidence, while the algorithm of the investigator's actions in cases of official offences committed in the conditions of total digitalisation of public authorities remained insufficiently formalised.

The purpose of the study was to form a conceptually and algorithmically justified approach to the use of digital forensics in the investigation of criminal offences in the field of official activity in Ukraine, in particular, to develop an algorithm for investigating official forgery, taking into account international standards and the possibilities of the adaptation to the Ukrainian criminal procedural context.

Materials and Methods

The study was conducted within the conceptual framework of international standards for digital forensics, in particular ISO/IEC 27037:2012 (2012), which defined four key phases of the digital evidence lifecycle. The theoretical framework was developed by authors such as L. Pasquale *et al*. (2013), G. Grispos *et al*. (2017), and L. Daubner & R. Matulevičius (2021). The concepts involved designing information systems in such a way that the systems created and stored evidentiary information by default. An additional methodological basis was the recommendations of the European Network of Forensic Science Institutes (2015), which were updated to define reference procedures for forensic investigation and evidence evaluation.

The research was carried out in three consecutive stages, each of which applied specific methods of scientific knowledge and used relevant empirical materials. The first stage was devoted to establishing the legal basis for the digitalisation of public service and the forensic characteristics of official offences in the context of digital transformation. Systemic-logical interpretation was used to interpret the provisions of the Criminal Code of Ukraine[1] on the elements of official offences under Articles 364, 365, 366 and 366-2, as well as the Criminal Procedural Code of Ukraine[2] on the procedural regime of electronic evidence. The historical-legal method was used for a retrospective analysis of the transformation of the methods of committing official forgery, in particular, a comparison of Article 172 "Official Forgery" of the Criminal Code of the Ukrainian SSR of 1960[3], which provided for traditional paper forms of document forgery, with the current version of Article 366 of the Criminal Code of Ukraine[4], which covered digital methods of committing a crime through electronic documents, state information systems and electronic identification mechanisms[5]. This analysis allowed establishing a qualitative transformation of the forensic characteristics of official forgery from material traces in paper documents to digital traces in distributed information systems. The system-structural method was used to construct a classification of digital traces of official offences, which allowed systematising the types of digital traces, the sources of origin and typical threats to integrity.

The second stage was aimed at analysing international standards of digital forensics, the implementation in Ukrainian legislation and judicial practice to identify gaps in legal regulation and forensic documentation. The comparative legal method was used to compare ISO/IEC 27037:2012 (2012) with the national analogue of DSTU ISO/IEC 27037:2017 (2017), as well as to identify the gap between technical standards and procedural and judicial practice in the context of European approaches (Committee of Ministers of the Council of Europe, 2019; Commonwealth Secretariat, 2025). National technical standards, in particular DSTU 7564:2014 (2014) were used to justify hash integrity verification, DSTU ISO/IEC 27040:2016 (2016) – organisation of evidence storage protection, backup copies and access control. The case-study method was used to analyse the judgments of Ukrainian courts[6,7,8,9,10] as well as two decisions of international case law, which represented the legal systems of common law and continental law, respectively: the decision of the Supreme Court of the United States of America in the case Van Buren v. United States[11] and the judgment of

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[2] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[3] Criminal Code of Ukraine RSR. (1960, December). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.
[4] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[5] Law of Ukraine No. 2155-VIII "On Electronic Identification and Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#Text.
[6] Judgment of Supreme Court in Case No. 715/758/20. (2022, November). Retrieved from https://iplex.com.ua/doc.php?regnum=107251729&red=1000034f2647aef95df9d6e093c285548f1c73&d=5.
[7] Judgment of Supreme Court in Case No. No. 450/168/18. (2022, February). Retrieved from https://iplex.com.ua/doc.php?regnum=103963360.
[8] Judgment of the High Court of Anti-Corruption in Case No. 991/185/23. (2023, March). Retrieved from https://iplex.com.ua/doc.php?regnum=109915446&red=1000035a4b7b910d8438484cac84f946a85d4f&d=5.
[9] Judgment of the Onufriivka District Court of Kirovohrad Region in Case No. 399/368/24. (2024, July). Retrieved from https://zakononline.ua/court-decisions/show/120611524.
[10] Judgment of the Chornomorsk City Court of Odesa Region in Case No. 123247255. (2024, November). Retrieved from https://youcontrol.com.ua/catalog/court-document/123247255/.
[11] Syllabus of the Supreme Court of the United States in Case "Van Buren v. United States". (2020, November). Retrieved from https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf.

the Tiergarten District Court (Germany) (Datenshutz Praxis, 2017), in order to establish the features of the judicial assessment of digital evidence, identify gaps in forensic documentation and establish the absence of references to international standards ISO/IEC 27037 in the motivational parts of Ukrainian court decisions. The third stage involved the development of a four-block algorithm of a digital forensic methodology for investigating official forgery with targeted recommendations. A synthetic method was used to integrate the results into a single methodological system. Modelling was used to develop sequential procedures in each of the four blocks of the algorithm. The system-structural method was used to formulate a set of targeted recommendations.

Results

Digitalisation of public service and transformation of the forensic characteristics of official offences. The official activities of state authorities and local self-government bodies in Ukraine take place in conditions of large-scale digital transformation, which radically changes both the methods of performing official functions and the forensic characteristics of crimes in the field of official activities. The legal basis for digitalisation is a set of regulatory acts, among which the central place is occupied by Law of Ukraine No. 851-IV[1], which recognises an electronic document as a full-fledged analogue of a paper one, provided that there is an electronic signature and the possibility of its visual reproduction, and also establishes the obligation to ensure the integrity and preservation of electronic documents within the established time limits. Further detailing of the legal regime of electronic identification was provided by Law of Ukraine No. 2155-VIII[2], which since 2018 has replaced the previous regime of electronic digital signature with a system of qualified electronic signatures and seals, harmonised with the European regulation eIDAS (European Union Agency for Cybersecurity, 2025). The infrastructural embodiment of digitalisation was the creation of the Unified State Web Portal of Electronic Services "Diya", the legal regime of which is enshrined in the Resolution of the Cabinet of Ministers of Ukraine No. 1137-2019-p[3], which determines the functionality of the portal and the obligation to keep records of requests and transactions in the relevant information systems. Such large-scale digitalisation means that most decisions of officials are mediated by electronic registers, departmental electronic document management systems, official e-mail, remote access to databases, which is accompanied by the emergence of specific digital traces – access logs to information systems, history of changes in registers, metadata of electronic documents, records of authorisation and transactions, time stamps and electronic signatures – which become a key element of evidence in criminal proceedings for official offences.

In this digital infrastructure, the classic elements of official offences, provided for in Articles 364 (abuse of power or official position), 365 (exceedance of power or official authority by an employee of a law enforcement agency), 366 (official forgery) and 366-2 (declaration of false information) of the Criminal Code of Ukraine[4], acquire a qualitatively new forensic characteristic. If under the Criminal Code of the Ukrainian SSR of 1960 (Article 172 "Official Forgery")[5] official forgery was associated primarily with entering false information into paper documents, forging signatures or seals, then in the current version of Article 366 of the Criminal Code of Ukraine, typical methods of committing this crime include the formation and signing by an official of electronic documents with knowingly false data using electronic identification mechanisms and trust services, entering false information into state information systems through an authorised web interface, unauthorised changes to records in databases using official accounts, blocking access to electronic documents or the deletion in order to hide illegal decisions, as well as intentional failure to submit or submission of knowingly false data in electronic declarations by persons authorised to perform state or local government functions.

Statistical indicators on official offences under Articles 364, 365 and 366 of the Criminal Code of Ukraine[6] are summarised based on official data of the Office of the Attorney General (n.d.), published in the form of a unified report on registered criminal offences and the results of the pre-trial investigation for the period 2020-2025. Under Article 364 of the Criminal Code of Ukraine (abuse of power or official position), 17,985 criminal offences were recorded in the period 2020-2025, however, 1,467 proceedings were sent to court with an indictment, which is 8.16% of the total number recorded. Under Article 365 of the Criminal Code of Ukraine (abuse of power or official authority by a law enforcement officer), out of 8,964 registered criminal offences in the period 2020-2025, 197 proceedings were sent to court with an indictment, which is 2.20%. For comparison, under Article 366 of the Criminal Code of Ukraine (official forgery), out of 30,899 registered offences in the period 2020-2025, 15,281 proceedings were sent to court with an indictment, which is 49.45%. The dynamics of the effectiveness of the investigation under each Article is presented in Figure 1.

[1] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, May). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15#Text.
[2] Law of Ukraine No. 2155-VIII "On Electronic Identification and Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#Text.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 1137-2019-p "On Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text.
[4] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[5] Criminal Code of Ukraine SSR. (1960, December). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.
[6] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.

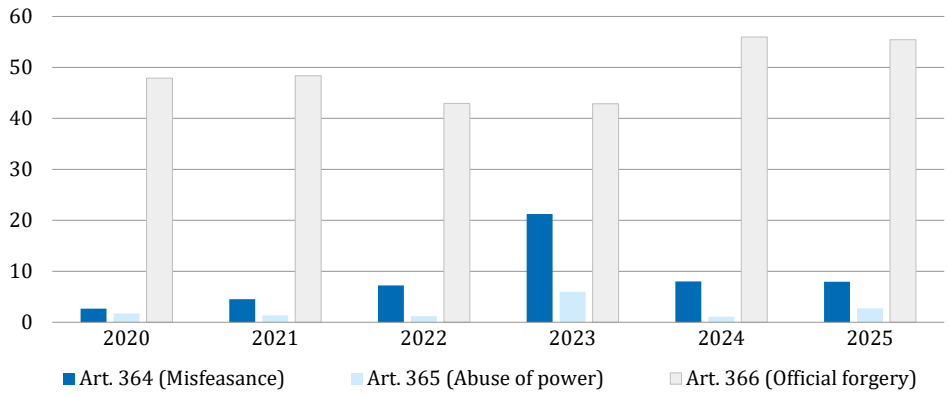

Figure 1. Efficiency of investigation of official offences under Articles 364, 365, 366 of Criminal Code of Ukraine (2020-2025)
Source: compiled by the author based on Office of the Attorney General (n.d.)

The data presented in the histogram demonstrate a significant disparity in the effectiveness of investigating various official offences. The indicators for Article 366 (official forgery) consistently exceed 40% throughout the entire period under study, reaching a maximum of 55.97% in 2024 and maintaining a consistently high level of 55.45% in 2025, which indicates a relatively high effectiveness of proving this category of offences. At the same time, Articles 364 and 365 demonstrate critically low indicators, which fluctuate within 1-21% and 1-6%, respectively, with a noticeable peak in 2023, which may be due to the intensification of anti-corruption efforts during this period. This disparity confirms the difficulty of proving crimes related to abuse or excess of power or official authority, compared to official forgery, where digital traces and documentary evidence are more accessible for recording and procedural processing, which is due to the insufficient use of digital forensics capabilities to document official manipulations in registers, electronic document management systems, and other digital environments.

The systemic nature of the problems is also confirmed by the significant volume of complaints about failure to enter information into the Unified Register of Pre-Trial Investigations: in 2024 alone, investigating judges received almost 80 thousand complaints about decisions, actions, or inaction of an investigator or prosecutor, of which more than 37 thousand were satisfied (Supreme Court of Ukraine, 2024), and in the High Anti-Corruption Court (2025) out of 1,618 complaints filed, 920 (57%) concerned precisely the failure to enter information into the Unified Register of Pre-Trial Investigations in criminal proceedings on corruption and official offences, while only 209 complaints out of 984 considered on the merits were satisfied, which is 21%. The low efficiency of investigating official offences is due not only to the complexity of proving, but also to the insufficient use of digital forensics capabilities to document official manipulations in registers, electronic document management systems and other digital environments.

From the perspective of forensics, the digital evolution of official offences means the emergence of an extensive system of digital traces that must be purposefully identified, recorded, and interpreted. These include electronic documents in departmental electronic document management systems in PDF, XML, DOCX formats, signed with a qualified electronic signature, records in transaction logs of state registers, including land, demographic, construction, property rights registers and the Unified State Register of Declarations of Persons Authorised to Perform State or Local Self-Government Functions, system logs of servers and workstations that record the facts of entering the system, changing access rights and performing official operations, network logs of application gateways and VPN servers, electronic correspondence of officials in departmental domains, backup copies of databases and file storages, as well as data from mobile devices that were used for two-factor authentication or decision approval (Kent & Grance, 2006; Kalancha, 2025).

Unlike traditional physical traces, digital traces are extremely sensitive to any interference, are easily copied and can exist simultaneously in several environments, in particular in local media, virtual systems and cloud services. This necessitates the need for a special methodology for the collection and storage, which combines the technical approaches of digital forensics with the procedural guarantees of the Criminal Procedural Code of Ukraine[1], in particular with the admissibility of evidence (obtaining in accordance with the established procedure), judicial control over access to electronic systems, documentation of the technical means used and preservation of data integrity throughout the entire chain of custody. To systematise digital traces in terms of individual elements of official offences, a generalised forensic characteristic was used, presented in Table 1.

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.

Table 1. Types of digital traces in official offences and the forensic significance

Type of official offence	Typical methods of commission in the digital environment	Types of digital traces	Sources of origin	Typical threats to the integrity of evidence
Abuse of power or official position (Article 364 of the Criminal Code)	Use of official access for unauthorised changes to records in state registers; granting of illegal preferences through electronic systems	Access logs (time, IP address, account); history of changes to records in the database; authorisation logs; electronic official correspondence	State information systems (cadastres, registers); departmental document management systems; authentication servers	Automatic deletion of logs; configuration change by the administrator; lack of chain of custody; lack of hashing when copying
Official offence (Article 366 of the Criminal Code)	Creation and signing of electronic documents with knowingly false information; substitution of attached files in the document management system; change of details after signing	Electronic documents with QES; document version history; file metadata; approval and routing logs; electronic signature logs	Departmental electronic document management system; qualified trust service providers; file servers	Editing without saving previous versions; use of drafts outside the official system; technical limitations of the depth of the version history
Declaring false information (Article 366-2 of the Criminal Code)	Entering knowingly false information about income, expenses, property, corporate rights and financial obligations into an electronic declaration through the NACP register	Entries in the Unified State Register of Declarations; personal account login logs; IP addresses and session times; NACP electronic messages; QES usage logs	NACP information systems; qualified electronic signature services; declarant's postal services	Incompleteness of logs in case of technical work; limited storage period; shared use of accounts; difficulty in proving knowledge

Note: DB – database; IP address – Internet Protocol address; QES – qualified electronic signature; NACP – National Agency for the Prevention of Corruption
Source: compiled by the author based on DSTU ISO/IEC 27040:2016 (2016), DSTU ISO/IEC 27037:2017 (2017), I. Kalancha (2025)

The systematisation given in Table 1 demonstrates that for each element of official offences there is a specific set of digital traces, which differ in the sources of origin, technical characteristics of fixation and typical threats of loss of evidentiary information. Forensic practice shows that the success of the investigation largely depends on the timely identification of relevant sources of digital traces and the use of adequate technical means of the fixation, taking into account the specific threats to the integrity of each type of data. The Judgment in the ase No. 991/1512/23[1] is indicative, where correspondence in the messenger, fixed during the examination of a mobile phone in compliance with the procedural requirements for the protocol, became key evidence in establishing the circumstances of the crime. Similarly, in the case of unauthorised change of information in an automated system, the court relied on digital records of data modifications made by a person with access rights, which confirms the importance of system logs and proper fixation of changes in the database environment[2]. International practice demonstrates similar approaches: in the case of Van Buren v. The United States[3] Supreme Court of the United States analysed the logs of a police officer's access to a law enforcement database, recognising authorisation logs as a key digital trace for establishing the fact and time of access to confidential information (Congressional Research Service, 2021). The lack of a unified approach to working with these traces among various pre-trial investigation bodies necessitates the development of a standardised algorithm that would integrate international standards of digital forensics with Ukrainian procedural legislation.

The scientific literature has already drawn attention to the fact that the dominance of electronic forms of document management is transforming the institutional dimension of law enforcement and prosecutorial activities. Thus, in the work of O.Y. Amelin (2024b), devoted to the information support of the prosecutor's office and the implementation of its functions as an element of the national security mechanism, the author emphasises that the effectiveness of prosecutorial supervision is inextricably linked to the quality of access to information resources, compliance with data protection standards and the ability of prosecutorial bodies to work with digital traces in public administration. This is directly projected onto the forensic methodology of investigating official offences: the prosecutor as a procedural manager must understand the architecture of state information systems and the minimum technical requirements for the admissibility of digital evidence, which requires specialised training and methodological support.

International standards of digital forensics, national legal regulation and judicial practice in cases of official offences. The international standard for working with digital evidence is ISO/IEC 27037:2012 (2012), which defines four key phases of

[1] Judgment of the High Court of Anti-Corruption in Case No. 991/1512/23. (2024, November). Retrieved from https://iplex.com.ua/doc.php?regnum=123349217&red=100003508b6a1068a6e52617075203562acc4f&d=5.
[2] Ibidem, 2024.
[3] Syllabus of the Supreme Court of the United States in Case "Van Buren v. United States". (2020, November). Retrieved from https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf.

the digital evidence life cycle: identification of potentially relevant digital sources, secure data collection, creation of a forensically correct copy and its verification, preservation, and documentation of all actions with the evidence. DSTU ISO/IEC 27037:2017 (2017) emphasises that a copy of digital data should be created by a competent person according to a clearly documented procedure, and its integrity is confirmed by calculating cryptographic hash values. In international and national practice, the MD5, SHA-1, SHA-256 hash functions, as well as national standards, in particular DSTU 7564:2014 (2014), are used for these purposes, and modern recommendations emphasise the use of more stable algorithms of the SHA-2 and SHA-3 family or combining several algorithms to reduce the risk of collisions. Ukraine has formally implemented ISO/IEC 27037 through the national standard DSTU ISO/IEC 27037:2017 (2017), which declares identity to the international text and operates in the system of technical regulation. However, these standards are not integrated into the criminal procedural law, and the application during pre-trial investigation is of a recommendatory nature, which is directly reflected in court decisions, where there are practically no references to the requirements of ISO/IEC 27037 when assessing the admissibility and relevance of digital evidence.

Ukraine has formally harmonised technical approaches to working with digital evidence through the adoption of the national standard DSTU ISO/IEC 27037:2017 (2017), however, its provisions are not enshrined in the Criminal Procedural Code of Ukraine[1] as procedurally binding admissibility criteria. This is evident in judicial practice regarding official offences: even in cases where digital evidence is the central object of investigation, courts argue conclusions regarding its admissibility and reliability mainly through the norms of the Criminal Procedural Code of Ukraine and the legislation on electronic documents, without appealing to international standards of digital forensics. For example, in Decree in the name of Ukraine No. 154/2277/17[2] (Articles 364, 366 of the Criminal Code), where the subject of evidence assessment was the reliability of information entered into the electronic log of the checkpoint of the Unified Analytical and Information System "Inspector", the court confirmed the officiality, relying solely on mutual consistency with witness statements and data from related databases in accordance with Article 94 of the Criminal Procedural Code of Ukraine, – without applying any procedures for technical verification of the integrity of digital records.

A more progressive level of international approaches is associated with the concepts of forensic readiness and forensic-by-design, developed by scientists L. Pasquale *et al*. (2013), G. Grispos *et al.* (2017), and L. Daubner & R. Matulevičius (2021). The concept of forensic readiness assumes the organisational and technical readiness of systems for a potential investigation even before the incident occurs, which allows maximising the use of evidence while minimising the costs of the investigation. L. Pasquale *et al.* (2013) proposed an approach in which forensic requirements are explicitly modelled and integrated into the software development process, allowing systems to automatically take proactive actions to preserve potentially important, but ephemeral evidence based on an assessment of the risk of a crime occurring. An alternative strategy is forensic-by-design, which involves embedding forensic requirements directly into the relevant phases of the system development lifecycle in order to create systems that are forensically ready from the design stage (Grispos *et al*., 2017). L. Daubner & R. Matulevičius (2021) developed this approach by proposing to consider forensic readiness through the lens of information security risk management, which allows re-evaluating security decisions to ensure reliable data in the event that security measures prove ineffective, and also to take into account the potential disputes that digital evidence can resolve.

These concepts suggest building in mechanisms from the design stage for complete and immutable logging of user actions, time synchronisation, cryptographic protection of logs, delimitation of access to audit records and the possibility of automated reconstruction of events from logs. In practical terms, these approaches have been implemented, for example, in the Estonian data exchange infrastructure X-Road, where a distributed architecture is combined with the use of the KSI blockchain for cryptographic signing of access logs, which provides long-term evidentiary confirmation of the immutability of records of access to state registers (e-Estonia, n.d.). Similar principles directly apply to official offences: in the case of proper implementation of forensic-by-design, each access by an official to a sensitive register leaves a trace in the action log that can be protected from modification, which can be used as highly reliable digital evidence. The European Network of Forensic Science Institutes (2015) developed the Best Practice Manual for the Forensic Examination of Digital Technology, which details the sequence of actions when working with digital media, focuses on the risks of data modification during the study, formulates requirements for the laboratory environment and the qualifications of experts. The degree of implementation of these international approaches in the Ukrainian practice of investigating official offences is reflected in the comparative analysis (Table 2).

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[2] Judgment of the Supreme Court in Case No. 154/2277/17. (2023, May). Retrieved from https://iplex.com.ua/doc.php?regnum=111192893.

Table 2. International standards of digital forensics and the status of the implementation in Ukraine

Standard/concept	Basic principles	Status of implementation in Ukraine	Identified gaps	Recommendations for implementation
ISO/IEC 27037:2012 (2012), DSTU ISO/IEC 27037:2017 (2017)	Four phases of working with digital evidence (identification, collection, retrieval, preservation); minimal intervention in the original data; application of hash functions; documentation of all actions	National analogue in force since 2019; used in individual expert institutions, but not integrated into the Criminal Procedural Court of Ukraine as a mandatory guideline	No mention of the standard in the Criminal Procedural Court of Ukraine; no legal definition of digital evidence; no mandatory requirements for hashing and chain of custody	Enshrine in the Criminal Procedural Court of Ukraine a definition of electronic evidence harmonised with ISO/IEC 27037; provide for the obligation to record the method of obtaining and ensuring integrity; introduce a training system for investigators and prosecutors
European Network of Forensic Science Institutes (2015)	Practical recommendations for forensic laboratories; requirements for planning expertise, documentation, validation of instruments, quality assurance	Used as a guideline by individual laboratories; not directly implemented by regulation, but taken into account in the methods of NDEKC and KNDISE	Lack of formal consolidation of ENFSI BPM in the accreditation system; lack of unified requirements for software validation; different levels of documentation quality	Provide for orientation on ENFSI-BPM in subordinate legislation; require documented procedures in accordance with BPM when accrediting laboratories; develop national methodological recommendations based on ENFSI-BPM
Forensic-by-design (Pasquale, 2013; Grispos, 2017; Daubner & Matulevičius *et al*., 2021; Commonwealth Secretariat, 2025)	Designing IT systems so that these systems create and store evidentiary information by default: full logging; log protection; time synchronisation; role-based access separation	Individual elements have been implemented in some state systems, but there is no single regulatory act on the minimum level of forensic readiness of state IT systems	There are no requirements for mandatory access logs in all SIS; no minimum log retention periods have been established; there are no criteria for assessing IT solutions for forensic-ready	Introduce forensic-ready requirements into the legislation on public electronic registers; include a forensic requirements section in the technical specifications for the creation of SIS; develop pilot implementation projects in critical systems

Note: SIS – state information systems; software – software; NDEKC – Scientific Research Forensic Centre of the Ministry of Internal Affairs of Ukraine; KNDISE – Kyiv Scientific Research Institute of Forensic Expertise; ENFSI – European Network of Forensic Science Institutes; BPM – Best Practice Manual
Source: compiled by the author

The comparative analysis presented in Table 2 demonstrates a systemic gap between international standards of digital forensics and the practical implementation in the Ukrainian system of investigation of official offences. The presence of national analogues of international standards, in particular DSTU ISO/IEC 27037:2017 (2017), in itself does not ensure the effective application without the integration of relevant requirements into criminal procedural legislation and mandatory departmental instructions. The concept of forensic-by-design deserves attention, the implementation of which at the level of designing state information systems could radically improve the quality of the evidence base in criminal proceedings on official offences by ensuring the automatic creation and reliable preservation of relevant digital traces of official activities.

Against this background, Ukrainian criminal procedural legislation demonstrates limited adaptation to digital reality. The Criminal Procedural Code of Ukraine[1] in Articles 98-99 operates with categories of material evidence and documents, without distinguishing electronic evidence as an independent procedural form, while the current version of Article 99 only covers information on material media in general terms and does not establish a special regime for digital objects. Law of Ukraine No. 851-IV[2] fixes the equality of legal force of electronic and paper documents, but does not contain mandatory requirements regarding the retention periods of access logs, backup copies, previous versions of documents or methods of recording the integrity of an electronic document for the purposes of future criminal proceedings. Law of Ukraine No. 2155-VIII[3] creates a qualified electronic signature regime and imposes certain obligations on qualified providers to maintain certificate registers, but does not establish a direct obligation to keep detailed logs of key usage, which significantly complicates the investigation of abuses of qualified electronic signatures in the field of official activities.

Judicial practice acts as a regulator of digital evidence in criminal proceedings on official offences. An analysis of court decisions reveals six cases that illustrate the approaches of Ukrainian courts to the assessment of digital evidence in cases on official offences.

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[2] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, May). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15#Text.
[3] Law of Ukraine No. 2155-VIII "On Electronic Identification and Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#Text.

In criminal proceedings against a customs inspector in Decree No. 715/758/20[1], the electronic journal of the automated system "Inspector" was examined, which recorded the actions of the official during customs clearance of goods. The court recognised that the electronic journal is an official document within the meaning of Article 99 of the Criminal Procedural Code of Ukraine[2], since it contains legally significant information, and the official's entry into the system using the official's login and password, which is unique and not subject to disclosure, is equated with an electronic digital signature as a mandatory requisite of an electronic document. Accordingly, entering knowingly false information into such a journal constitutes an objective aspect of official forgery, as provided for in Article 366 of the Criminal Code of Ukraine[3]. The motivational part of the resolution does not contain any mention of the use of hash functions or the chain of custody procedure, and the assessment of the admissibility of evidence is limited to an analysis of the system user's powers and the procedural aspects of the inspection and seizure of equipment.

Decree in the name of Ukraine No. 592/6618/16-k[4] considered the accusation of a customs official under Part 2 of Article 364 and Part 1 of Article 366 of the Criminal Code of Ukraine[5], which was based, in particular, on the incrimination of entering knowingly false information into the information bases of the Unified Automated Information System of the State Fiscal Service and the software and information complex "Inspector-2006", as well as drawing up and storing in the EAIS-ASMO subsystem a knowingly false act on the inspection of a vehicle. The central object of the evidentiary controversy was the photographs stored in the "Inspector 2006" database: the court decided the issue of the availability, date of entry and reliability solely through the mutual consistency of witness testimonies in accordance with Article 94 of the Criminal Procedural Code of Ukraine[6], without applying any procedures for technical verification of the integrity of digital data.

The practice of the High Anti-Corruption Court in cases under Article 366-2 of the Criminal Code of Ukraine[7] demonstrates the use of various forms of digital evidence. Judgment in the case No. 991/185/23[8] examined data from the Unified State Register of Declarations of the NACP, the log of user actions in the NACP information system and bank statements provided on an optical medium, recognising this information as appropriate and admissible evidence of property declaration of false information. Decree No. 629/5254/21[9] analysed criminal proceedings under Article 366-3 of the Criminal Code of Ukraine[10] regarding the intentional failure to submit an annual declaration by the declaring entity, emphasising that the obligation to submit is implemented by filling out the declaration on the official website of the NACP, and the disposition of Article 366-3 of the Criminal Code of Ukraine does not make criminal liability dependent on prior written notification to the NACP about the fact of failure to submit a declaration. It is noteworthy that the court focused exclusively on the substantive and legal issues of the offence, leaving out of consideration the issue of technical verification of digital traces in the NACP information system.

The empirical base is supplemented by two court decisions that demonstrate the complexity of assessing digital evidence in criminal proceedings for official offences. Judgment in the case No. 123247255[11] considered the accusation of a state inspector of a customs post under Part 1 of Article 366 of the Criminal Code of Ukraine[12] of entering knowingly false information into the "Passage Log" software module of the Unified Automated Information System (UAIS) of the State Customs Service. The court described in detail the system architecture and the mechanism for recording all user actions using personal logins and passwords, which creates an electronic trace of each operation in the system. The Judgment is acquittal: the court stated that the prosecution did not prove beyond reasonable doubt the illegality of the inspector's actions and could not recreate a lawful model of the official's behaviour in similar factual circumstances. Decree in the name of Ukraine No. 991/503/23[13] demonstrates another aspect of the same problem: the courts of previous instances based

[1] Judgment of the Supreme Court in Case No. 715/758/20. (2022, November). Retrieved from https://iplex.com.ua/doc.php?regnum=107251729&red=1000034f2647aef95df9d6e093c285548f1c73&d=5.
[2] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[4] Decree in the name of Ukraine No. 592/6618/16-k. (2023, January). Retrieved from https://iplex.com.ua/doc.php?regnum=108686222.
[5] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[6] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[7] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[8] Judgment of the High Court of Anti-Corruption in Case No. 991/185/23. (2023, March). Retrieved from https://iplex.com.ua/doc.php?regnum=109915446&red=1000035a4b7b910d8438484cac84f946a85d4f&d=5.
[9] Judgment of the Supreme Court in Case No. 629/5254/21. (2025, February). Retrieved from https://iplex.com.ua/doc.php?regnum=125297104.
[10] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[11] Judgment of the Chornomorsk City Court of Odesa Region in Case No. 123247255. (2024, November). Retrieved from https://youcontrol.com.ua/catalog/court-document/123247255/.
[12] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[13] Judgment of the Supreme Court in Case No. 991/503/23. (2025, August). Retrieved from https://iplex.com.ua/doc.php?regnum=129691175.

the conviction of the judge under Part 1 of Article 366-2 of the Criminal Code of Ukraine[1] (declaration of false information) on the tables of the sequence of actions of the user of the Unified State Register of NACP declarations with IP addresses, obtained by NABU detectives in accordance with Article 93 of the Criminal Procedural Code of Ukraine[2]. The Supreme Court confirmed the admissibility and reliability of these digital data, assessing these data exclusively through the criteria of Article 94 of the Criminal Procedural Code of Ukraine in conjunction with other evidence – without any reference to ISO/IEC 27037 (2012) standards or procedures for verifying the integrity of electronic records.

International case law in cases of official offences in the digital environment demonstrates more detailed attention to the technical aspects of digital evidence and forensic procedures for obtaining it. In the decision of the Supreme Court of the United States Van Buren v. United States[3] Georgia State Police Officer Nathan Van Buren, having legal access to a law enforcement database, used it to obtain vehicle licence plate information for personal gain, which was the subject of a Computer Fraud and Abuse Act[4] charge. The digital logs of access to the database became key evidence of the fact that protected information was accessed using valid credentials, while the legal debate revolved around the interpretation of the concept of exceeds authorised access in the context of using legitimate access for unauthorised purposes. A similar emphasis on the evidentiary value of access logs to government information systems is contained in the decision of the Tiergarten District Court in 2017, where an official of the Berlin Bürgeramt population registration office was found guilty of five hundred and sixty-one unauthorised accesses to the electronic Melderegister in violation of the Bundesdatenschutzgesetz (Datenshutz Praxis, 2017). The court relied on detailed access logs that recorded each request by the employee's personal login with a time stamp and the content of the request, and qualified the very fact of unauthorised digital access to a closed state personal database as a complete breach of official duties, imposing a fine of EUR 4,950. Ukrainian judicial practice in the above cases reveals a systemic limitation: courts focus on the formal and legal assessment of documents as evidence in accordance with Articles 84-99 of the Criminal Procedural Code of Ukraine[5] and do not articulate the requirements for forensically correct handling of digital evidence in accordance with international standards, in particular ISO/IEC 27037:2012 (2012), which necessitates the development of an integrated algorithm for digital forensic methods for investigating official offences.

Algorithm of digital forensic methodology for investigating official forgery and targeted recommendations. Based on the hypothesis that the quality of evidence of official forgery can be significantly improved by implementing a standardised algorithm of digital forensics, it is advisable to propose a four-block methodology that combines international standards ISO/IEC 27037:2012 (2012), forensic-by-design approaches and the requirements of Ukrainian criminal procedural legislation. The first block, forensically oriented primary fixation of the digital situation, should begin with the correct choice of procedural form: depending on the situation, a scene inspection under Article 237 of the Criminal Procedural Code of Ukraine[6], a search under Article 234 of the Criminal Procedural Code of Ukraine or temporary access to things and documents under Articles 159-166 of the Criminal Code is used. The investigator, in agreement with the prosecutor, must determine in advance which information systems, servers, workstations, mobile devices, removable media and network segments potentially contain traces of official offences. Before conducting a procedural action, it is necessary to involve a digital forensics specialist, who is tasked with identifying the sources of digital traces, proposing a safe procedure for the fixation and warning the investigator about the risks of losing volatile data, in particular RAM, temporary files, caches (Mastering digital forensics…, 2025). The state of the system at the time of the intervention is recorded by taking photos and videos of screens, saving current event logs, describing the equipment configuration and network connections in the protocol of the investigative action. Typical mistakes at this stage are turning off the server without first taking a RAM dump, working with the original data carrier instead of a forensic copy, and conducting live analysis on the suspect's workstation without using write-blockers and capturing hash values.

The second block of the algorithm, identification of relevant sources of digital evidence, requires an understanding of the architecture of state information systems. A typical state authority combines a departmental electronic document management system with the functions of registering incoming and outgoing documents, approving, applying a qualified electronic signature and storing versions, one or more industry registries, a local file server, a domain infrastructure with directory and authentication services, remote access tools via VPN or RDP gateways, integration gateways

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.
[2] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[3] Syllabus of the Supreme Court of the United States in Case "Van Buren v. United States". (2020, November). Retrieved from https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf.
[4] Computer Fraud and Abuse Act. (1986, January). Retrieved from https://www.justice.gov/jm/jm-9-48000-computer-fraud.
[5] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[6] Ibidem, 2012.

with interdepartmental systems of the Trembit level or X-Road analogues used within the framework of the "Diya" digital services. For each system, the investigator, together with a specialist, determines which database tables, audit logs, backup copies and configuration files may contain evidence of official forgery. At this stage, it is necessary to ensure interaction with administrators of information systems and centralised platforms, which is formalised by requests of the investigator in accordance with Article 93 of the Criminal Procedural Code of Ukraine[1] and by decisions of the investigating judge on temporary access to things and documents, which clearly indicate the types of data, the period for which the data are requested, and the requirements for the format of the provision. A significant gap in the current legislation is that neither the Criminal Procedural Code of Ukraine[2] nor special laws on electronic documents and trust services oblige subjects of government authority to store audit logs and backup copies for the minimum period sufficient for the investigation of potential official offences.

The third block, forensically correct acquisition and analysis of digital evidence, should be based on ISO/IEC 27037:2012 (2012) standards and NIST and ENFSI recommendations. The basic principle is to create a forensic copy of digital data using write-blockers and specialised software, in particular FTK Imager, X-Ways, dd in a Linux environment, while at least one modern SHA-256 hash algorithm is calculated and recorded in the protocol for each medium and, if necessary, compatibility with existing MD5 or SHA-1 tools, which forms a double level of integrity control (Kent & Grance, 2006; Scientific Working Group on Digital Evidence, 2019). Analysis methods depend on the type of evidence: for electronic documents in PDF, DOCX or XML format, the key is the study of metadata, including creation and modification dates, authorship, version history, comparison of checksums of different copies, detection of inconsistencies between text content and file structure; for databases, the analysis of transaction logs, triggers, backup copies is critical, which allows reconstructing the sequence of operations of an official; for operating system event logs, it is necessary to build a timeline of user actions, including logging in and out of the system, launching programs, installing updates, connecting external media; for network logs, it is important to correlate IP addresses, ports, VPN channels with specific workstations and accounts. The results of the analysis should be presented in the form of an expert opinion, the structure of which corresponds to the best European practices of the European Network of Forensic Science Institutes (2015): a clear separation of the descriptive part, technical observations, interpretation and the actual conclusion, where probabilistic judgments are carefully formulated.

The fourth block of the algorithm, the presentation of digital evidence in court, should take into account both the gaps in the Criminal Procedural Code of Ukraine[3] and the existing practice of the Supreme Court. The absence of special norms on electronic evidence in the code does not prevent the court from assessing such evidence as documents, but requires the prosecution to disclose as much information as possible about the origin, method of obtaining and ensuring the integrity of digital data. It is advisable in each proceeding on official offences to submit to the court protocols of investigative actions with a detailed description of the seized equipment and media, technical acts or reports of a digital forensics' specialist, an expert opinion indicating the used standards ISO/IEC 27037:2012 (2012) and national DSTU, chain of custody, which documents who, when and on what basis had access to forensic copies.

The practical applicability of the proposed algorithm should be demonstrated on a case study of a hypothetical case of official forgery in the field of public procurement. It is worth assuming that the head of the procurement department of a central executive body, having access to the electronic document management system and the public procurement web portal, entered into the electronic draft contract and approval letters knowingly false information about the actual volumes of supplies and the cost of services, and also made an unauthorised replacement of the attached commercial proposal files. At the first stage of the investigation, the investigator, with the participation of a specialist, conducts an inspection of the body's server room and the suspect's workplace, recording the system configuration, taking current event logs and a dump of the RAM of the electronic document management system server. Then, using temporary access, the investigator receives from the administrator of the central public procurement platform complete audit logs for the relevant tender, including the history of file downloads and replacements, IP addresses, time stamps and user IDs. At the third stage, the specialist creates forensic copies of the server disks and the official's workstation using SHA-256, analyses the metadata of electronic documents, correlates these metadata with the audit logs of the procurement platform, as well as with the data of the network logs of the VPN gateway. At the fourth stage, the expert reconstructs the chronology in the conclusion: the expert finds that on a certain day and time from the workstation of the head of the department, the system was logged in, commercial proposal files

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[2] Ibidem, 2012.
[3] Ibidem, 2012.

were replaced, and essential terms of the contract were edited. In court, the combination of electronic documents, audit logs, and network logs, the suitability of which is confirmed by the correct collection and hashing procedure, makes it possible to prove the fact of official forgery in a digital environment with a high level of evidentiary persuasiveness.

Based on the above algorithm, it is possible to formulate a set of targeted recommendations. It is advisable for the legislator to propose supplementing Article 99 of the Criminal Procedural Code of Ukraine[1] with a separate part that would legalise the concept of electronic evidence in the following wording: electronic evidence is digital data that is stored, processed or transmitted in electronic form and is important for establishing the circumstances of criminal proceedings, in particular electronic documents, files, databases, electronic messages, metadata, event logs of information systems, as well as other forms of digital information; electronic evidence is submitted in the form of forensic copies or in the form of duly certified electronic extracts indicating the method of the receipt and means of ensuring integrity. It is also worth considering the possibility of supplementing the provisions of Articles 364, 366 and 366-2 of the Criminal Code of Ukraine[2] with qualifying features reflecting the use of information and communication systems, for example, committed by unauthorised changes to information in state information systems or by entering knowingly false information into state electronic registers, which would allow for a more accurate reflection of the increased public danger of the digital aspects of such crimes.

For law enforcement agencies, in particular pre-trial investigation bodies and prosecutors, organisational, staffing and methodological recommendations are key. It is advisable to provide for the creation of specialised digital forensics units in the field of official offences investigation within the structure of the National Police, the State Bureau of Investigation and the National Anti-Corruption Bureau, which will be entrusted with supporting investigations, where work with state information systems is central. Such units should be provided with a minimum list of software and hardware, including modern forensic workstations, write-blockers, licensed software for creating forensic images and analysing event logs, and integrated into the budget planning system through public procurement mechanisms (Cyclopes, 2023). The Ministry of Internal Affairs, the State Bureau of Investigation and the Office of the Prosecutor General should approve by departmental orders methodological recommendations for working with digital evidence, including with reference to ISO/IEC 27037:2012 (2012) and DSTU ISO/IEC 27037:2017 (2017), with a clear description of the protocols of the investigator's and specialist's actions at each stage of the algorithm. In the study by O.Y. Amelin (2024a), devoted to the procedural aspects of the appointment and replacement of a prosecutor in criminal proceedings for offences in the field of official activity, attention is drawn to the need for prosecutors to specialise in cases of this category, which logically includes mastering the skills of working with digital evidence and understanding the principles of digital forensics.

For the scientific community, it is advisable to outline several priority areas of research. Firstly, the development of a classification of official offences in the digital environment, taking into account the specifics of various sectors of the public service, in particular fiscal, customs, land, urban planning, medical, and defence, which will allow identifying industry-specific features of digital traces and methods of the fixation. Secondly, empirical studies of the applicability of the proposed algorithm to real criminal proceedings in order to verify its effectiveness, for example, by analysing the dynamics of acquittals and convictions in cases where forensic actions were properly documented in accordance with international standards. Thirdly, an in-depth comparative legal analysis of the experience of countries that have already integrated the concept of electronic evidence and digital forensics standards into national legislation, in particular the states of the European Union, the United States of America, the United Kingdom, and the countries of Northern Europe, with an assessment of the possibilities of adapting the solutions in the Ukrainian context.

Finally, for higher education institutions that train lawyers and law enforcement officers, it is worth proposing the development of specialised educational components, in particular a separate course "Digital Forensics of Official Offences", within which students and trainees will master the basic principles of ISO/IEC 27037:2012 (2012), simulate the investigation of official forgery in electronic registers, and practice skills in working with event logs, electronic documents, and network logs in a training ground. Such a course can be integrated into master's programs in criminal law and procedure, cybersecurity, as well as into the system of advanced training for prosecutors and investigators, supporting the need to adapt legal education to the digital environment of the functioning of justice and public administration. Taken together, the proposed algorithm and set of recommendations form the basis for a conceptually and algorithmically sound digital forensic methodology for investigating official offences, which is based on international standards, real judicial practice, and the institutional needs of the Ukrainian law enforcement system.

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.

Discussion

The results obtained demonstrate a systemic problem of investigating official offences in the context of digitalisation of the public sector, which is manifested in the gap between the number of recorded criminal offences and proceedings that reach the judicial stage. The developed four-block algorithm eliminates the identified gaps in the chain of custody procedure by integrating the requirements of the Criminal Procedure Code of Ukraine and granting procedural status to intermediate copies, which is a fundamental difference from foreign models. Conceptually, this proposal echoes the Cloud Digital Forensic Readiness model presented by A. Akilal & M. Kechadi (2025), where automated management of law enforcement requests and control of checksums at all stages ensured data integrity in multi-jurisdictional calculations by creating secure channels for transmitting evidentiary information. E. Egho-Promise *et al*. (2024) emphasise the importance of adhering to standardised procedures for digital forensics in cloud computing, as the distributed nature of cloud infrastructure makes it more difficult to identify, collect, and preserve digital evidence compared to traditional local systems. The Ukrainian model additionally takes into account the procedural aspects of the national criminal process, as judicial practice assesses the admissibility of evidence primarily through the prism of the procedural form of its receipt, and not exclusively the technical correctness of forensic procedures, which was confirmed by the analysis of six court decisions of different instances. At the same time, the proposed approach maintains compatibility with the international standards ISO/IEC 27037:2012 (2012), which allows it to be integrated into cross-border investigations and ensure mutual recognition of evidence within the framework of international legal assistance, especially in cases of transnational corruption.

A detailed taxonomy of digital traces for each element of official offences demonstrates that the most vulnerable block is the log data block, in particular, change logs in databases, authorisation logs, and electronic correspondence of officials, which poses the main risk of losing evidentiary information at the initial stages of the investigation. The findings coincide with the work of S. Makura *et al.* (2021), where the limited retention period of operational logs in cloud systems is defined as the risk of losing evidence due to automatic overwriting, which varies from 7 to 30 days depending on the system configuration. The proposed typology develops this approach, outlining specific threats for each type of official offences: automatic deletion of logs after the expiration of the established retention period, lack of hashing when copying between different media, changing the system configuration by the administrator without saving previous settings, and editing documents without saving previous versions in electronic document management systems. These specifications provide a basis for developing forensic checklists that can be used by investigators to pre-assess the risks of losing digital traces and prioritise procedural actions during the investigation planning stage.

The proposed procedural safeguards are consistent with modern approaches to cloud forensics, which have systematised the challenges of preserving event logs of distributed systems as a major obstacle to reconstructing the sequence of events in criminal proceedings. However, unlike the general model of cloud forensics, which focuses on external cybersecurity threats from illegitimate users, the study takes into account the specifics of official offences, where the offender has internal authorised access to the infrastructure and can purposefully destroy digital traces of the offender's actions by using administrative privileges to modify event logs. S. Friedl & G. Pernul (2024), based on an empirical study of European organisations, found that funding and the presence of organisational policies are the main factors in the readiness of IoT environments for investigative intervention. In particular, the researchers found that most organisations do not have centralised procedures for backing up event logs of sensor devices, which significantly complicates further forensic investigation of such environments.

In terms of ensuring a continuous chain of custody, the proposed double control of hash values through the simultaneous use of SHA-256 and MD5 algorithms, as well as mandatory logging of all official operations with forensic copies, correspond to the approach of S. Nath *et al*. (2024), where the emphasis is on transparent reproducibility of the chronology of actions and the possibility of independent verification of integrity at any stage of the investigation by different subjects of criminal proceedings. Double hashing ensures compatibility with different expert tools that use different algorithms to verify data integrity, and reduces the risk of evidence rejection due to technical limitations of specific software or incompatibility of forensic utility versions between different expert institutions. At the same time, the solution of M. AlKhanafseh & O. Surakhi (2024), which proposes to combine blockchain and steganography technologies to record metadata of forensic copies in order to ensure the immutability and the possibility of verification in the long term for more than ten years, remains unattainable due to the lack of the necessary technical infrastructure in state bodies of Ukraine and the high cost of implementing distributed registries. The proposed measures are more feasible in the short term through the use of existing equipment and free open-source utilities, but retain compatibility with promising technologies for long-term fixation.

An analysis of case law in six national cases showed that Ukrainian courts focus on the formal legal assessment of documents in accordance with Articles 84-99

of the Criminal Procedural Code of Ukraine[1], without articulating the requirements for forensically correct handling of digital evidence. Courts rarely refuse to accept evidence obtained using open-source tools if experts have confirmed the application of appropriate procedures when creating forensic copies, which indicates a pragmatic approach to assessing technical reliability regardless of the formal certification of the tools. This partly contradicts the findings of I. Ismail & K.A.Z. Ariffin (2025), who, based on Malaysian case law, found that the rejection rate of evidence obtained using uncertified tools was around 35% due to the lack of formal accreditation of forensic laboratory software. In the national context, the principle of procedural expediency is at work, as courts recognise the technical uniqueness of electronic traces even when using utilities without formal certification, given that alternative commercial solutions with licensed software are often unavailable due to budgetary constraints of expert units and lengthy public procurement procedures.

A systematic review by A.A. Ahmed *et al.* (2024) summarised global trends in Internet of Things forensics based on an analysis of over two hundred publications for the period 2019-2024 and highlighted the lack of interdisciplinary protocols for integrated ecosystems that combine cloud computing, mobile devices and sensor networks in a single data processing chain. The proposed algorithm addresses this shortcoming by combining technical and procedural phases in a single evidence route that covers all types of digital sources regardless of the architectural features and physical location in different segments of the state information infrastructure. The systematisation of digital traces is also consistent with the TAM-TOE entropy model proposed by S.I. Safie *et al*. (2025) to analyse the factors influencing the ability of government agencies to apply practices oriented to the ISO 27037:2012 (2012), where the technological, organisational and environmental levels are considered as equivalent determinants of the success of implementation. Unlike the Malaysian experience, where the main barrier was the distrust of staff in new protocols due to the habit of traditional working methods and fear of additional workload, the Ukrainian environment is faced primarily with underfunding of technical equipment of expert units and the lack of systematic training of investigators in the field of digital forensics, which prioritises budget-neutral changes to procedural rules and departmental instructions.

Thus, the results of the study confirm the need for a systemic transformation of approaches to the investigation of official offences through the introduction of the forensic-by-design concept, which implements the ISO/IEC 27037:2012 (2012) standards into state information systems and ensures evidentiary readiness at the design stage of e-government services. The proposed algorithm is consistent with leading international developments in the field of digital forensics, while adapting these developments to the Ukrainian procedural context, filling the gaps that were overlooked in previous studies due to the focus on general issues of electronic evidence without taking into account the specifics of official offences. The identified discrepancies with certain foreign approaches, in particular regarding the admissibility of open-source tools and the current unavailability of blockchain technologies, outline the directions of future empirical and normative research aimed at increasing the effectiveness of the investigation of official offences in the digital environment.

Conclusions

The study was devoted to the formation of a conceptually and algorithmically grounded approach to the use of digital forensics in the investigation of official offences in the context of a large-scale digital transformation of the public sector of Ukraine. The study found that the digitalisation of public service, which takes place on the basis of legislation on electronic documents, electronic identification and the functioning of the "Diya" portal, has radically transformed the forensic characteristics of official offences provided for by the current criminal legislation of Ukraine. The created extensive system of digital traces in state information systems requires specialised methods of detection and fixation, which are significantly different from traditional forensic approaches to material traces.

The systematisation of digital traces in the context of individual elements of official offences revealed specific sources of origin, technical characteristics of fixation and typical threats of loss of evidentiary information for each type of offence. A comparative analysis of international standards of digital forensics and the state of the implementation in Ukraine has shown a systemic gap between the presence of national analogues of international standards and the practical application due to the lack of integration into criminal procedural legislation. An analysis of six court decisions has demonstrated that Ukrainian courts focus on the formal and legal assessment of documents in accordance with the norms of criminal procedural legislation on evidence and substantiation, without articulating the requirements for forensically correct handling of digital evidence in accordance with international standards. Based on the identified gaps, a four-block algorithm of digital forensics methodology for investigating the most common type of official offences – official forgery, has been developed, which includes forensically oriented primary fixation of the digital situation, identification of relevant sources of digital evidence, forensically correct acquisition and analysis of data using hash functions and write-blockers, as well as presentation of evidence in

[1] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.

court in compliance with the requirements of the chain of custody. The practical applicability of the algorithm is confirmed through a detailed case study of a hypothetical case of official forgery in the field of public procurement, which demonstrates the sequence of forensic actions from the initial fixation of the server infrastructure to the presentation of an expert opinion in court.

The results obtained form a conceptual basis for overcoming the low efficiency of the investigation of official offences, which is manifested in the minimal share of criminal proceedings on official offences that reach the court stage with an indictment, as well as in significant volumes of complaints about the inaction of investigative bodies regarding the failure to enter information into the Unified Register of Pre-Trial Investigations in Corruption and Official Proceedings. The proposed approach allows transferring digital traces of official activity from the category of potential to the category of actually used evidence through standardisation of the procedures for the collection, recording, and presentation in court in accordance with international standards. The formulated targeted recommendations cover legislative amendments to criminal procedural legislation regarding the legalisation of the concept of electronic evidence and to criminal substantive legislation regarding the qualifying features of the use of information and communication systems, organisational and staffing measures for law enforcement agencies regarding the creation of specialised digital forensics units, priority areas of scientific research on the industry-specific nature of digital traces, as well as educational components for legal education in the form of a specialised course on digital forensics of official offences.

Promising areas of further research are the empirical verification of the proposed algorithm on an array of real criminal proceedings, the development of industry modifications of the methodology for specific sectors of the public service, in particular fiscal, customs, land and urban planning, as well as an in-depth analysis of the possibilities of implementing the forensic-by-design concept in the design of state information systems of Ukraine in order to ensure the readiness for a potential investigation from the stage of developing technical tasks.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Ahmed, A.A., Farhan, K., Jabbar, W.A., Al-Othmani, A., & Abdulrahman, A.G. (2024). IoT Forensics: Current perspectives and future directions. *Sensors*, 24(16), article number 5210. doi: 10.3390/s24165210.

[2] Akilal, A., & Kechadi, M. (2021). An improved forensic-by-design framework for cloud computing with systems engineering standard compliance. *Forensic Science International Digital Investigation*, 40, article number 301315. doi: 10.1016/j.fsidi.2021.301315.

[3] Akilal, A., & Kechadi, M. (2025). Cloud digital forensic readiness: An open source approach to law enforcement request management. *arXiv*. doi: 10.48550/arXiv.2507.04174.

[4] AlKhanafseh, M., & Surakhi, O. (2024). Evidence preservation in digital forensics: An approach using blockchain and LSTM-based steganography. *Electronics*, 13(18), article number 3729. doi: 10.3390/electronics13183729.

[5] Amelin, O.Y. (2024a). Certain aspects of the appointment and replacement of the prosecutor in criminal proceedings on offences in the sphere of official activity. *Constitutional State*, 56, 143-154. doi: 10.18524/2411-2054.2024.56.315691.

[6] Amelin, O.Y. (2024b). Realization of the functions of the prosecutor's office as an element of the mechanism of ensuring national security of Ukraine. *Constitutional State*, 55, 20-28. doi: 10.18524/2411-2054.2024.55.311949.

[7] Chepurna, T. (2025). Circumstances to be established during the investigation of official criminal offenses committed by law enforcement officers. *Scientific Perspectives. Series Law*, 6(60). doi: 10.52058/2708-7530-2025-6(60)-1020-1031.

[8] Committee of Ministers of the Council of Europe. (2019). *Electronic evidence in civil and administrative proceedings*. Retrieved from https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5.

[9] Commonwealth Secretariat. (2025). *Guidelines on the treatment of electronic evidence in criminal proceedings*. Retrieved from https://surl.li/wvxptj.

[10] Congressional Research Service. (2021). *Van Buren v. United States: Supreme Court holds accessing information on a computer for unauthorized purposes not federal crime*. Retrieved from https://www.congress.gov/crs-product/LSB10616.

[11] Cyclopes. (2023). *Cyclopes – fighting cybercrime – law enforcement practitioners' network: Deliverable D4.8.* Retrieved from https://surl.li/etafhm.

[12] Datenshutz Praxis. (2017). *Data breach at the registration office: A fine!* Retrieved from https://www.datenschutz-praxis.de/pleiten-pech-pannen/datenschutzverstoss-meldeamt-geldstrafe/.
[13] Daubner, L., & Matulevičius, R. (2021). Risk-oriented design approach for forensic-ready software systems. In *ARES '21: Proceedings of the 16th international conference on availability, reliability and security* (article number 48). New York: Association for Computing Machinery. doi: 10.1145/3465481.3470052.
[14] DSTU 7564:2014. (2014). *Information technologies. Cryptographic information protection. Hash function*. Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66229.
[15] DSTU ISO/IEC 27037:2017. (2017). *Information technology – protection techniques – guidelines for the identification, collection, retrieval and preservation of digital evidence*. Retrieved from https://online.budstandart.com/ua/catalog/doc-page?id_doc=74978.
[16] DSTU ISO/IEC 27040:2016. (2016). *Information technology – protection techniques – storage security*. Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=67146.
[17] e-Estonia. (n.d.) *KSI® blockchain in Estonia.* Retrieved from https://e-estonia.com/wp-content/uploads/faq_ksi_blockchain.pdf.
[18] Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital forensic investigation standards in cloud computing. *Universal Journal of Computer Sciences and Communications*, 3(1), 23-45. doi: 10.31586/ujcsc.2024.923.
[19] European Network of Forensic Science Institutes. (2015). *ENFSI guideline for evaluative reporting in forensic science: Strengthening the evaluation of forensic results across Europe (STEOFRAE)*. Retrieved https://enfsi.eu/wp-content/uploads/2016/09/m1_guideline.pdf.
[20] European Union Agency for Cybersecurity. (2025). *Technical implementation guidance*. Retrieved from https://surl.li/ofjdoq.
[21] Fagbola, F.I., & Venter, H.S. (2022). Smart digital forensic readiness model for shadow IoT devices. *Applied Sciences*, 12(2), article number 730. doi: 10.3390/app12020730.
[22] Fihurskyi, V.M. (2023). Evidence in electronic form in criminal proceedings. *Galician Studies: Law Sciences*, 3, 97-105. doi: 10.32782/galician_studies/law-2023-4-14.
[23] Fomina, T.H., & Rachynskyi, O.O. (2023). Electronic evidence in criminal proceedings: Problematic issues of theory and practice. *Bulletin of Kharkiv National University of Internal Affairs*, 102(3(Part 2)), 207-220. doi: 10.32631/v.2023.3.43.
[24] Friedl, S., & Pernul, G. (2024). IoT forensics readiness – influencing factors. *Forensic Science International Digital Investigation*, 49, article number 301768. doi: 10.1016/j.fsidi.2024.301768.
[25] Grispos, G., Garcia-Galan, J., Pasquale, L., & Nuseibeh, B. (2017). Are you ready? Towards the engineering of forensic-ready systems. *arXiv*. doi: 10.48550/arXiv.1705.03250.
[26] Ismail, I., & Ariffin, K.A.Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS ONE*, 20(9), article number e0331683. doi: 10.1371/journal.pone.0331683.
[27] ISO/IEC 27037:2012. (2012). *Information technology – security techniques – guidelines for identification, collection, acquisition and preservation of digital evidence*. Retrieved from https://www.iso.org/standard/44381.html.
[28] Kalancha, I. (2025). Evidence in electronic form in the criminal proceedings of Ukraine: Identification and integrity in the light of the chain of custody concept. *Science and Perspectives*, 8(51), 206-230. doi: 10.52058/2695-1592-2025-8(51)-206-230.
[29] Kebande, V.R., Karie, N.M., Choo, K.R., & Alawadi, S. (2021). Digital forensic readiness intelligence crime repository. *Security and Privacy*, 4(3), article number e151. doi: 10.1002/spy2.151.
[30] Kent, K., & Grance, T. (2006). *Guide to integrating forensic techniques into incident response*. Retrieved from https://csrc.nist.gov/pubs/sp/800/86/final.
[31] Kvashuk, O.D. (2025). The use of electronic evidence in criminal proceedings. *Central Ukrainian Journal of Law and Public Management*, 2, 50-56. doi: 10.32782/cuj-2025-2-5.
[32] Loskutov, T., Yunin, O., Verbytskyi, V., Momotenko, T., & Smirnov, A. (2023). Methods of information security in the investigation of corruption offences. *Lex Humana*, 16(1), 328-344.
[33] Makura, S., Venter, H.S., Kebande, V.R., Karie, N.M., Ikuesan, R.A., & Alawadi, S. (2021). Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring. *Security and Privacy*, 4(3), article number e149. doi: 10.1002/spy2.149.
[34] Mastering digital forensics: An ultra-extensive guide to investigations, tools, and techniques. (n.d.). Retrieved from https://securedebug.com/digital-forensics-investigations-tools-techniques/.
[35] Milimko, L.V., & Zhydovtsev, Y.V. (2025). Electronic evidence in criminal proceedings of Ukraine. *Uzhhorod National University Herald, Series Law*, 3(88), 302-308. doi: 10.24144/2307-3322.2025.88.3.45.

[36] Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In *2024 IEEE 8th international conference on trust, privacy and security in intelligent systems, and applications (TPS-ISA)* (pp. 11-20). Washington: Institute of Electrical and Electronics Engineers. doi: 10.1109/TPS-ISA62245.2024.00012.

[37] Office of the Attorney General. (n.d.). *Single criminal offense report*. Retrieved from https://data.gov.ua/dataset/8b9b1677-2407-454a-bfa7-76eb638c0ea1.

[38] Pasquale, L., Yu, Y., Cavallaro, L., Salehie, M., Tun, T.T., & Nuseibeh, B. (2013). *Engineering adaptive digital investigations using forensics requirements*. In *2013 21st IEEE international requirements engineering conference (RE)* (pp. 340-341). Rio de Janeiro: Institute of Electrical and Electronics Engineers. doi: 10.1109/RE.2013.6636745.

[39] Predmestnikov, O.G., & Bekhter, A.R. (2024). Use of innovative technologies in criminal procedure law: Challenges and opportunities. *Uzhhorod National University Herald. Series Law*, 3(82), 117-122. doi: 10.24144/2307-3322.2024.82.3.19.

[40] Safie, S.I., Zulkifli, M., Sapry, H.R., & Bashah, S.R.M. (2025). Integrating individual and organizational perspectives: A TAM-TOE framework for ISO 27037 adoption in Malaysian government digital forensics agencies. *Journal of Open Innovation Technology Market and Complexity*, 11(3), article number 100595. doi: 10.1016/j.joitmc.2025.100595.

[41] Scientific Working Group on Digital Evidence. (2019). *SWGDE position on the use of MD5 and SHA1 hash algorithms in digital and multimedia forensics*. Retrieved from https://www.swgde.org/wp-content/uploads/2023/11/2019-09-29-SWGDE-Position-on-the-Use-of-MD5-and.pdf.

[42] Supreme Anti-Corruption Court. (2025). *Analysis of the implementation of judicial proceedings by the Supreme Anti-Corruption Court in 2024 (as a court of first instance)*. Retrieved from https://court.gov.ua/storage/portal/hcac/statistics/analyses/justice_24.pdf.

[43] Supreme Court of Ukraine. (2024). *The state of the administration of justice in criminal proceedings and cases of administrative offenses by courts of general jurisdiction in 2024*. Retrieved from https://court.gov.ua/storage/portal/supreme/Analyz_zdijsnenna_pravosydda_2024.pdf.

Цифрова еволюція криміналістичної методики розслідування кримінальних правопорушень у сфері службової діяльності в Україні

Олександр Амелін
Кандидат юридичних наук, доцент
Офіс Генерального прокурора
01011, вул. Різницька, 13/15, м. Київ, Україна
Державний податковий університет
08201, вул. Університетська, 31, м. Ірпінь, Україна
https://orcid.org/0000-0002-0933-2111

Анотація
Метою дослідження був аналіз можливостей цифрової криміналістики в розслідуванні службових злочинів шляхом інтеграції міжнародних стандартів і концепцій forensic-by-design з українським кримінальним процесуальним законодавством. Порівняльно-правовий аналіз міжнародних та українських стандартів цифрової криміналістики виявив системний розрив між технічними стандартами та процесуальною і судовою практикою, де суди майже не артикулюють вимоги до форензично коректного поводження із цифровими доказами. Системна класифікація цифрових слідів за типами службових правопорушень у кримінальному законодавстві дала змогу систематизувати специфічні джерела походження, види цифрових слідів і типові загрози цілісності доказів для кожного складу службового злочину в умовах масштабної цифровізації публічного сектору. Методом кейс-стаді було досліджено судову практику України, Сполучених Штатів Америки та Німеччини щодо використання цифрових доказів у справах про службові злочини, що дало змогу встановити відсутність посилань на міжнародні стандарти цифрової криміналістики в мотивувальних частинах українських судових рішень і виявити прогалини в процесуальному оформленні електронних доказів, які унеможливлюють перевірку їх автентичності та цілісності відповідно до вимог ISO/IEC 27037:2012. Розроблено чотириблоковий алгоритм цифрової криміналістичної методики розслідування службових злочинів, пов'язаних зі службовим підробленням (ст. 366 КК України), що охоплює форензично орієнтовану первинну фіксацію цифрової обстановки, ідентифікацію релевантних джерел цифрових доказів, форензично коректне здобуття та аналіз, а також представлення доказів у суді з додержанням процедур ланцюга збереження доказів. Практичне значення результатів дослідження полягає в можливості їх використання законодавцем для внесення змін до кримінального процесуального законодавства, правоохоронними органами для створення спеціалізованих підрозділів у сфері розслідування службових злочинів із застосуванням цифрової криміналістики, а також закладами вищої освіти для впровадження відповідних освітніх компонентів у юридичну освіту

Ключові слова:
електронні докази; цифрові сліди; forensic-by-design; міжнародні стандарти; державні інформаційні системи; доказування; форензична копія