Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

METHODOLOGICAL PROVISION OF TECHNICAL AND FORENSIC DOCUMENTATION OF DIGITAL AND PHYSICAL EVIDENCE IN PRE-TRIAL CRIMINAL PROCEEDINGS

INHA KALANCHA[1*], VASYL SMIKH[2], NADIIA MORHUN[3], SERHII BARHAN[4], EDUARD USHKANENKO[5]

[1]Public Law Department, Faculty of Law and International Relations, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.
[2]Department of Investigation of Particularly Important Cases, Main Investigative Department of the National Police of Ukraine, Kyiv, Ukraine.
[3]Department of Operational and Investigative Activities and National Security, National Academy of Internal Affair, Kyiv, Ukraine.
[4]Department of Law, Faculty of Economics and Business Administration, Kryvyi Rih National University, Kryvyi Rih, Ukraine.
[5]Department of Law, Higher· Educational Institution "Academician Yuriy Bugay International Scientific and Technical University", Kyiv, Ukraine.

E-mail: [1]inhakalancha@gmail.com, [2]vsmich@gmail.com, [3]morgun_nadiia@gmail.com, [4]serg_bargan@gmail.com, [5]ushkanenko@istu.edu.ua

ABSTRACT

Ensuring proper documentation of digital and physical evidence today determines not only the quality of the pre-trial investigation, but also the real possibility of making a fair court decision, which necessitates the need for procedures capable of guaranteeing the authenticity, integrity and traceability of evidentiary information in accordance with international ISO and NIST standards. The aim of the study is the substantiation and testing of the author's three-level conceptual model of methodological provision of documenting evidence, which integrates the technical, organizational, and legal levels of evidentiary information management. The model is built on the basis of the Forensic Documentation Integrity Index (FDII), which includes technical reliability, procedural admissibility, integrity of the storage chain, and methodological standardization. The methodology is based on a combination of comparative legal, functional analytical, and expert modelling approaches using Delphi survey, analytical hierarchy process (AHP), and correlation analysis (n = 27 experts). The results confirmed that the implementation of the model provides increased consistency between technical, procedural, and methodological parameters. The highest FDII value was recorded in the United Kingdom (0.94) due to the full digitalization of the chain of custody in accordance with the Forensic Science Regulator's Code and the Digital Forensics Science Strategy. In Germany (0.90), the stability of the system is ensured by the codification of procedures in the Strafprozessordnung (StPO) and BKA standards. In Ukraine (0.81), the highest increase (ΔFDII = +0.15) was recorded after the model was tested. Correlation analysis (r = 0.79–0.95) demonstrated the effectiveness of the integration structure. The academic novelty is the creation and confirmation of the effectiveness of a three-level model of documenting evidence. The practical value is the formation of a toolkit for harmonizing the Ukrainian system with international standards ISO/IEC 27037, 27041 and NIST IR 8387.

Keywords: *Digital Evidence, Forensic Documentation, Methodological Model, Chain of Custody, Criminal Justice, Innovation, Legal Governance*

1. INTRODUCTION

In the 21st century, the rapid development of digital technologies has radically changed not only the social, but also the forensic sphere. Today, digital evidence – from electronic correspondence and metadata to video recordings, GPS tracks and data from cloud services – actually determines the outcome of pre-trial investigations. The risk of violating the integrity of the chain of custody, losing admissibility in court, and distorting evidentiary information increases in the absence of a unified model for their documentation, thereby necessitating a standardized approach critically urgent right now. However, the integration of such evidence into the evidentiary process requires not only technical competence, but also clearly developed methodological support that guarantees its authenticity, integrity, and procedural admissibility [1, 2]. As Ukrainian researchers [3, 4] noted, the national practice of recording and preserving electronic and physical evidence still remains fragmented: there is no unified system for recording actions, the continuity of the *chain of custody* is not always ensured, and the technical procedures of copying and hashing are not always correctly reflected in procedural documents. This creates risks for the reliability of evidence and complicates its assessment in court. Methodological support for technical and forensic documentation should be considered not as an auxiliary activity, but as a central element of the evidentiary process [4].

International experience demonstrates that effective documentation of digital evidence is possible only if methods are standardised and roles are clearly divided between investigators, experts, and technical specialists. In the UK, the implementation of the *Forensic Science Regulator Act 2021* and the *Digital Forensics Science Strategy* have provided uniform requirements for the processes of extracting, analysing, and storing digital data [5–7]. German researchers [8, 9] emphasize the importance of creating scenario databases and validation sets of digital traces to increase the reproducibility of examination results. Ukraine is only forming its own normative and methodological framework, combining classical forensics with modern digital technologies [10, 11].

The relevance of the study is determined by the need to develop an integrated model of methodological support for technical and forensic documentation, which would simultaneously cover digital and physical evidence, meet international standards of digital forensics, and ensure their procedural admissibility as part of pre-trial proceedings. A comparative analysis of the approaches of Ukraine, Germany, and the UK identifies optimal methodological solutions that can be adapted to national practice, ensuring its transparency, reliability, and technological compatibility.

The present study addresses not only the practical need for improving forensic documentation procedures, but also the broader issue of IT knowledge enhancement in digital forensics. Existing best practices based on ISO/IEC and NIST standards provide important technical guidance for identifying, collecting, acquiring, preserving, and verifying digital evidence. However, their use often remains fragmented when these standards are applied separately from procedural admissibility requirements and organizational chain of custody control. Therefore, the contribution of this study is not limited to an incremental restatement of existing best practices. The proposed FDII-based model provides a more integrated analytical framework by connecting technical dependability, procedural admissibility, chain of custody integrity, and methodological standardization into one measurable structure. This enables the transformation of separate technical recommendations into a systematic tool for evaluating and improving forensic documentation systems.

The aim of the article was to substantiate and test the author's three-level conceptual model of methodological provision of documentation of evidence, which integrates the technical, organizational, and legal levels of evidentiary information management.

To achieve this aim, the study pursued the following objective of the following research objectives:

1. Analyse international standards, recommendations, and national regulatory legal acts of Ukraine, Germany, and the UK that regulate the procedure for collecting, recording, and preserving digital and physical evidence in pre-trial proceedings, identifying the possibilities of their adaptation to Ukrainian practice.
2. Arrange academic and methodological approaches to technical and forensic documentation of evidence and identify key problems of their application in investigative activities, including risks to the integrity of the chain of custody and the admissibility of digital data in court.
3. Develop a conceptual model of methodological support for the documentation of digital and physical evidence, integrating technical, organizational, and legal components, as well as identifying

organizational and technological conditions for its effective implementation in the activities of law enforcement agencies of Ukraine.

The study addressed the following research questions: RQ1: How do Ukraine, Germany, and the UK differ in the methodological provision of technical and forensic documentation of digital and physical evidence? RQ2: Which parameters most strongly determine the integrity of forensic documentation systems? RQ3: Does the proposed three-level model improve documentation consistency as measured by FDII? RQ4: What methodological improvements are required to harmonize Ukrainian practice with ISO/IEC and NIST-oriented standards?

The hypothesis is that the implementation of an integrated methodological provision with unified procedures for recording, hashing, storing, and processing digital and physical evidence increases their reliability, reproducibility, and judicial admissibility in pre-trial proceedings.

2. LITERATURE REVIEW

The issue of technical and forensic documentation of digital and physical evidence in current academic literature is characterized by a significant diversity of approaches, which reflects the interdisciplinary nature of this field. Researchers do not agree on a single understanding of which elements – technical, regulatory or organizational – play a decisive role in ensuring the reliability of digital materials. Studying the European context, Marcinauskaitė [12] argues that the main problem is the lack of unified rules for authentication and procedural recording of electronic evidence, which causes significant differences in the judicial interpretation of their admissibility. Abdullah et al. [13] actually deny the priority of the normative dimension and emphasize that a violation of the chain of custody, insufficient control over hashing and the lack of independent logging remain the main source of evidentiary vulnerability even in the presence of clear procedures.

The difference in technical approaches is also noticeable. Göbel et al. [14] propose scenario modelling and the creation of supervised training sets as a basis for testing forensic techniques. Abdul-Samad et al. [15] approach the issue differently, believing that scenario modelling does not eliminate the fundamental problem of the lack of unified technical standardization. In their opinion, only strict adherence to ISO/IEC 27037 and 27041 ensures true reproducibility of digital artifacts. Some authors offer another perspective: Guttman et al. [16] criticize technological practices of short-term testing and insist on the introduction of state repositories for long-term storage of electronic evidence with unified metadata formats capable of withstanding multi-stage authentication.

The legal literature forms its own spectrum of contradictions. Brown [17] and Kasper and Laurits [18] warn that digital technologies create complex ethical dilemmas: the need to ensure the evidentiary value of electronic materials often conflicts with the right to privacy. Al-Billeh emphasizes something completely different: even minimal interference with digital data can lead to a loss of evidence in war crimes cases. So, he advocates for the most stringent, formalized procedures for recording each step of information processing. Illési [19] denies the universality of such an approach, noting that excessive formalization does not guarantee reliability without proper organizational infrastructure and internal auditing.

Comparative studies add even more analytical nuances. Gupta and Husain [20] concluded that the British model is the most standardized, but the American one — although more flexible — is more vulnerable to chain of custody violations. Ismail and Ariffin [21] argue that open-source forensic tools can be reliable if they are properly legally documented. Khan and Ahmed [22], Khan [23], emphasize that technological innovations will have no effect without changes in procedural norms and automated control mechanisms.

The reviewed literature can be synthesized into three main streams: technical preservation of digital artifacts, legal admissibility of evidence, and organizational compliance of forensic procedures. However, these streams remain fragmented, as technical studies often do not sufficiently address procedural admissibility, while legal studies rarely provide measurable criteria for assessing technical reliability. This gap justifies the proposed model, which integrates technical, legal, and organizational dimensions into one methodological framework.

So, current studies demonstrate not a consensus, but a wide spectrum – from technocentric models to exhaustive legal and organizational concepts. Two dominant trends – technological (standardization, automation, ISO/NIST) and legal (admissibility, transparency, control) – often develop in parallel, but are not integrated into a single system. The lack of a model capable of combining these approaches into a comprehensive framework for pre-trial proceedings constitutes a key research gap. The reviewed literature is based mainly on recent studies published in 2020–2025 and shows that digital evidence

research has developed in three directions: technical preservation, legal admissibility, and organizational compliance. However, these directions remain fragmented because technical studies rarely provide procedural criteria, while legal studies often do not offer measurable indicators of forensic reliability. This gap justifies the present study and the development of an integrated FDII-based model.

3. PROBLEM STATEMENT

The digitalization of criminal proceedings has become one of the key factors in the evolution of the modern justice system. The use of electronic media, cloud storage, biometric and video data, activity logs and other digital artifacts has significantly expanded the capabilities of forensics in identifying, recording, and verifying evidentiary information. At the same time, this has led to the emergence of new methodological and legal challenges related to the reliability, authenticity and procedural admissibility of digital and physical evidence [12, 13]. Different countries apply different standards of evidentiary support. For example, in the UK, clearly defined requirements of the Forensic Science Regulator's Code and the Digital Forensics Science Strategy are in force. In most European jurisdictions, the integration of international standards ISO/IEC 27037, 27041 and NIST IR 8387 recommendations is taking place gradually [15, 16]. Recent studies show that the main risks for the evidentiary process are not the loss of physical objects, but manipulation of digital data — their editing, distortion or unauthorized copying without proper recording in the chain of custody protocols [14, 24]. The lack of unified procedures for hashing and documenting electronic artifacts reduces the courts' confidence in digital evidence and creates grounds for their rejection during the consideration of cases [17, 19]. Comparative analysis shows that there is no complete consistency between the technical standards of digital forensics and procedural requirements for evidence even within the EU single legal space. In Germany, special attention is paid to scenario testing, validation of digital tools and data authenticity control [14], while the British model is focused on standardization and detailed documentation of each expert's action, which ensures high reproducibility of results [20]. The essence of the problem under study lies in the lack of a balanced methodological model of technical and forensic documentation of digital and physical evidence, which would simultaneously meet the requirements of technological reliability, procedural admissibility, and international standards of legal verification.

4. PROPOSED METHODOLOGY

4.1. Research Design

The methodological architecture of the study is based on a combination of comparative law, forensics, and digital analytics approaches aimed at identifying the level of methodological consistency of systems for technical and forensic documentation of digital and physical evidence in Ukraine, Germany, and the UK. The choice of these three countries is determined by their representativeness for different legal systems and models of forensic support. The UK embodies the Anglo-Saxon precedent system, which emphasizes standards for the admissibility of evidence and the independence of forensic expertise. Germany represents the continental Romano-Germanic tradition with clearly codified procedures and strict requirements for the documentation of investigative actions. Ukraine is at the stage of integrating international standards ISO/IEC and NIST into forensic practice, combining continental principles with elements of the Anglo-Saxon approach. Along with legal principles, countries were also selected based on technical criteria: the level of digital infrastructure in forensic departments, centralized chain of custody systems, the degree of integration of ISO/IEC 27037 and 27041 standards, the use of NIST-oriented protocols, as well as practices for technical verification of evidence (hashing, digital signing, audit logs). This combination of legal and technical characteristics enables comparing not only regulatory requirements, but also the actual level of technological readiness of documentation systems, and assessing how different models ensure the authenticity, integrity, and judicial suitability of digital and physical evidence.

The research questions were evaluated in accordance with the available information base and analytical parameters of the study. RQ1 was addressed through comparative analysis of regulatory acts and ISO/NIST-oriented standards; RQ2 was examined using the FDII parameters TD, PA, CC, and MS; RQ3 was tested through expert modelling and Delphi–AHP weighting; and RQ4 was assessed by comparing the Ukrainian results with the German and UK models. This structure ensured correspondence between the research questions, available sources, and measurable indicators.

The first stage involved a regulatory audit of international and national acts regulating the circulation of digital evidence in pre-trial proceedings. The analysis included the *Forensic Science Regulator's Code of Practice* [25], *Digital*

Forensics Science Strategy [26], *Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften* [27], *Instructions on the Peculiarities of Forensic Expert Activities by Certified Forensic Experts Not Working in State Specialized Expert Institutions* [28] and the *Criminal Procedure Code of Ukraine* [29]. The international standards ISO/IEC 27037:2012 and ISO/IEC 27041:2015 [30, 31], as well as the NIST IR 8387:2022 recommendations [16], which define the requirements for the authenticity, preservation and reproducibility of digital artifacts, were also studied. This stage enabled forming a legal framework for further comparative analysis and identifying common and distinctive features of approaches to the proceduralization of digital evidence.

The second stage provided for a functional and analytical modelling of procedures for documenting digital and physical evidence performed in typical scenarios: detection and capture; extraction and hashing; storage and transfer; procedural consolidation and expert verification. A chain of custody model was built for each country, reflecting the procedure for controlling the reliability of data and the procedures for verifying them.

The third stage involved a comparative assessment of the effectiveness of methodological systems carried out according to the following criteria: regulatory certainty, technical reproducibility, organizational integration, and evidentiary reliability. The results of the analysis identified the key structural elements of the conceptual model of methodological support for documenting digital and physical evidence, adapted to the Ukrainian system of pre-trial investigation, taking into account the requirements of international standards ISO/IEC 27000-series and NIST.

4.2. Research Methods

The study used a set of methods, each performing a separate function. The comparative legal method was used to compare the norms of Great Britain, Germany and Ukraine. It identified differences in admissibility standards, capture procedures, and chain of custody regulation. At the stage of regulatory audit, this method ensured the formation of the legal framework for the study and the identification of gaps in the regulation of digital evidence. Functional and analytical modelling was aimed at reconstructing documentation procedures in typical investigative scenarios — detection, hashing, storage, transfer. The result was the creation of chain of custody models for three countries and the identification of critical risk points. The method was applied at the second stage of the study. The Delphi method was used not as a survey, but as a tool for achieving expert consensus on the FDII weighting factors. It ensured the consistency of assessments, which was confirmed by a high concordance index. In the second round, experts specified parameters that reflect the technical, procedural, and organizational components. The AHP method was chosen as a parameter weighting technique, which allows checking the logical consistency of the pairwise comparison matrices. It was applied during the finalization of the integral index, which ensured the correctness of the TD, PA, CC and MS weights. Content analysis was used to identify repetitive procedures in ISO/IEC standards and NIST recommendations, which made it possible to form the technical element of the model. Statistical analysis (in particular, the concordance coefficient) confirmed the reliability of expert assessments and the stability of the obtained weights. The system-structural method was used to integrate technical, legal, and organizational blocks into a single conceptual model.

4.3. Evaluation Metrics

The effectiveness of the methodological support of forensic documentation was evaluated using the author's Forensic Documentation Integrity Index (FDII), which allows quantitatively determining the consistency between technical reliability, procedural admissibility, organizational integrity, and international standardization of procedures for working with evidence. Within the framework of this approach, four basic parameters were identified, covering the technical, legal, organizational and methodological aspects of forensic documentation. The criteria TD, PA, CC, and MS were selected because they correspond to the full life cycle of forensic documentation. TD reflects the technical reliability of capture, copying, hashing, and storage; PA reflects the procedural admissibility of evidence; CC reflects continuity and traceability of evidence movement; and MS reflects alignment with ISO/IEC, NIST, and national methodological requirements. Together, these criteria cover the main points at which evidence may lose reliability, reproducibility, or admissibility. A system of parameters was formed for quantitative evaluation, which is presented in Table 1.

Table 1: Metrics for evaluating forensic documentation systems

Parameter	Designation	Calculation method	Range	Interpretation
Technical reliability	TD (Technical Dependability)	Share of capture, copying, hashing and storage procedures performed in accordance with ISO/IEC 27037 and NIST IR 8387	0–1	Authenticity and reproducibility of digital evidence
Procedural admissibility	PA (Procedural Admissibility)	Percentage of actions that comply with the requirements of the Criminal Procedure Code of Ukraine, Forensic Science Regulator's Code (UK), StPO (DE)	0–1	Legality and evidentiary suitability
Chain of custody integrity	CC (Chain Consistency)	Level of continuity of chain of custody – availability of confirmed logs, digital signatures, audit logs	0–1	Control and traceability of evidence movement
Methodological standardization	MS (Methodological Standardization)	Degree of integration of ISO/IEC 27041, internal instructions of the Ministry of Justice (No. 3505/5) and national protocols	0–1	Compliance with international and national norms

Source: developed by the author based on Forensic Science Regulator's Code [25], Digital Forensics Science Strategy [26], Gesetz zur Fortentwicklung der Strafprozessordnung [27], Order of the Ministry of Justice of Ukraine No. 3505/5 [28], CPC of Ukraine [29], ISO/IEC 27037:2012 [30], ISO/IEC 27041:2015 [31] and NIST IR 8387 [16]

The resulting weights formed the basis for constructing the integral FDII, which was used to comparatively assess the effectiveness of national evidence documentation systems. The FDII integrates four dimensions – technical, procedural, organizational, and methodological – and reflects the level of comprehensive integrity of forensic procedures. The final indicator was calculated using the formula (1):

$$FDII = (0.30 \times TD) + (0.30 \times PA) + (0.25 \times CC) + (0.15 \times MS) \quad (1)$$

The weighting factors were determined through an expert survey of 27 specialists from forensic institutions, pre-trial investigation units, and academic centres in Ukraine, Germany, and the UK. The distribution of weights reflects the balance between technical reliability, procedural admissibility, and organizational consistency.

The degree of harmonization (HG) indicator was used to assess the compliance of national procedures with the international requirements of ISO/IEC 27037, ISO/IEC 27041 and recommendations of NIST IR 8387. This indicator reflects the level of consistency of technical and procedural actions with key standards of authenticity and integrity of digital evidence. The HG value was obtained based on expert evaluation (Delphi, n = 27) and calculated using Formula (2), where the ST (standardization completeness), PR (procedural robustness) and TC (technical compliance) parameters were evaluated using the criteria for compliance with ISO/IEC 27037 and 27041, the requirements of NIST IR 8387 for chain of custody and the availability of technical means of authenticity control. The calculation formula has the form (2):

$$HG = (0.40 \times ST) + (0.35 \times PR) + (0.25 \times TC) \quad (2)$$

The weighting coefficients were determined by experts and confirmed by a high level of agreement of estimates (W = 0.79), which ensures the reliability of comparative values for Ukraine, Germany, and the UK.

The experts were selected by purposeful sampling according to the criteria of professional competence, practical experience in the field of digital forensics for at least 10 years, participation in the preparation of forensic expert opinions or regulatory acts, as well as academic publications on evidence provision issues. The sample included: 9 experts from Ukraine (representatives of the Expert Service of the Ministry of Internal Affairs, the Scientific Research Institute of Forensic Expertise and specialized departments of law universities); 9 experts from Germany (Bundeskriminalamt, Kriminaltechnisches Institut, universities of Münster and Berlin); 9 experts from the UK (Forensic Science Regulator's Office, National Police Chiefs' Council, King's College London).

The survey was conducted in two stages using the Delphi method, which allowed for consistent expert assessments. In the first stage (February–March 2025), respondents were sent an online questionnaire via the Google Forms platform,

which contained 10 questions — seven close-ended (on a five-point Likert scale) and three open-ended. The questions concerned the assessment of the importance of the parameters of technical reliability, procedural admissibility, integrity of the chain of custody and methodological standardization, as well as the justification of which procedures for capturing, hashing, logging and transferring evidence should be basic for the integral FDII. Experts assessed the relative importance of each parameter of the FDII index (TD, PA, CC, MS), determined an acceptable compromise between the accuracy of capture and legal suitability, and also proposed their own formulations of the indicators. In the second stage (April–May 2025), the results of the first round were summarized and discussed during online focus group discussions (three groups per country). Using the pairwise comparison method (Analytic Hierarchy Process, AHP), the participants agreed on the final weighting coefficients. The level of agreement of the estimates was checked using the Kendall concordance coefficient (W = 0.81), which indicates a high degree of stability of the results. The error of expert agreement did not exceed σ = 0.10, which ensures the statistical reliability of the created model.

The validity of the study was ensured through the alignment of research parameters, expert procedures, and international standards. Construct validity was supported by the correspondence between FDII parameters and ISO/IEC 27037, ISO/IEC 27041, and NIST IR 8387 requirements. Internal validity was strengthened by the Delphi procedure, AHP weighting, and Kendall concordance coefficient. External validity is limited by the selected jurisdictions and expert sample, but the comparison of Ukraine, Germany, and the UK provides a relevant basis because these countries represent different levels of legal codification and forensic digitalization.

4.4. Conceptual Model of Methodological Support for Documenting Evidence

The proposed model consists of three interconnected levels:

1. Technical level – defines the procedure for detecting, capturing, copying, hashing, and storing digital artifacts in accordance with ISO/IEC 27037 and NIST IR 8387 standards;

2. Organizational level – ensures chain of custody control, separation of roles of experts, investigators and prosecutors, as well as digital verification of each stage of evidence transfer;

3. Legal level – guarantees the admissibility and procedural purity of evidence in accordance with the Code of Criminal Procedure of Ukraine, StPO (DE) and Forensic Science Regulator's Code (UK). The structure of the proposed conceptual model of methodological support for documenting evidence is presented in Figure 1.

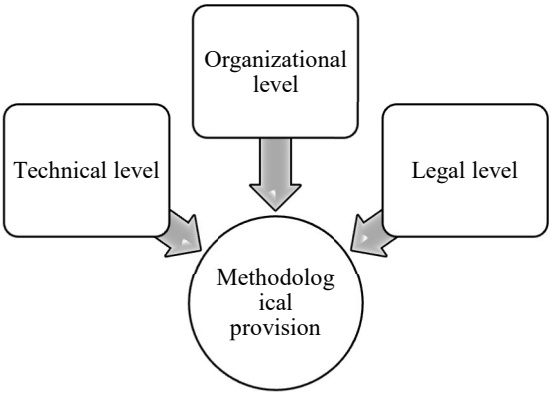

Figure 1: Structure of the proposed conceptual model of methodological provision of documenting evidence
Source: developed by the author

The model is modular: it allows for the integration of national protocols with international ISO and NIST benchmarks, ensuring reproducibility and mutual recognition of examination results across jurisdictions.

Its implementation creates the basis for a unified digital and physical evidence management system that combines technical reliability, legal admissibility, and procedural transparency.

4.5. Technical Environment

Data analysis and modelling were performed in Python 3.12 using Pandas, NumPy, SciPy, and Matplotlib libraries. Verification of FDII results was performed in Microsoft Excel 2025, and visualization was performed in Power BI. The regulatory and legal acts of the studied countries were processed through Legislation.gov.uk, Gesetze-im-Internet.de, and zakon.rada.gov.ua. International standards were verified through ISO.org and NIST.gov. This approach ensured the reproducibility of calculations and the transparency of methodological comparison between the three legal systems.

5. RESULTS

5.1. Comparative Analysis of Regulatory Frameworks for Documenting Digital and Physical Evidence

A comparative analysis of the national systems of Ukraine, Germany, and the UK has shown significant differences in the structure of legal regulation of forensic evidence documentation. Although all three states recognize digital artifacts as a full-fledged source of evidentiary information, the level of their procedural formalization and technical standardization varies significantly. The study assessed the degree of harmonization of regulatory acts with the provisions of international standards ISO/IEC 27037:2012, ISO/IEC 27041:2015 and NIST IR 8387:2022, which determine the procedure for identifying, storing, and verifying digital evidence. The obtained results shown in Table 2 reflect the degree of regulatory consistency of forensic evidence documentation systems in the three states according to key criteria — legislative certainty, standardization of procedures, the availability of a digital chain of custody, and the integration of international ISO and NIST standards.

Table 2: Comparison of regulatory requirements for evidence documentation in the studied countries

Criterion	Ukraine	Germany	UK
Basic law	Criminal Procedure Code (as amended in 2024)	Strafprozessordnung (StPO, ed. 2021)	Police and Criminal Evidence Act (as amended in 2022)
Special act/instruction	Order of the Ministry of Justice No. 3505/5 (2011, as amended in 2024)	Gesetz zur Fortentwicklung der StPO (2021)	Forensic Science Regulator's Code (2021)
Availability of ISO/NIST standards in the legal framework	Partial implementation of ISO/IEC 27037 in the internal instructions of the Expert Service of the Ministry of Internal Affairs	Official reference to ISO/IEC and NIST in federal BKA recommendations	Full integration of ISO/IEC and NIST into Digital Forensics Science Strategy (2023)
Chain of custody regulations	Provided, but there is no single digital register	Formalized through KTI and BKA	Electronic register and digital signatures implemented in Home Office
Authentication and hashing requirements	Declared at the level of guidelines	Clearly stated in StPO and departmental instructions	Required under Forensic Regulator's Code and ACPO Guidelines
Procedural status of digital evidence	Equated to material, requires expert confirmation	Fully recognized as an independent source	Fully admissible with chain of custody
Degree of harmonization with ISO/NIST	0.68	0.82	0.91

Source: calculated by the author based on Forensic Science Regulator's Code [25], Digital Forensics Science Strategy [26], Gesetz zur Fortentwicklung der Strafprozessordnung [27], Order of the Ministry of Justice of Ukraine No. 3505/5 [28], CPC of Ukraine [29], ISO/IEC 27037:2012 [30], ISO/IEC 27041:2015 [31] and NIST IR 8387 [16]

The results of Table 2 show that the UK demonstrates the highest level of harmonization (0.91) due to a harmonized regulatory framework – the Forensic Science Regulator's Code [25] and the Digital Forensics Science Strategy (2023), which integrate the ISO/IEC 27000 series and NIST recommendations. Germany (0.82) ensures high standardization through the legislative consolidation of digital procedures in the StPO and federal BKA recommendations. Ukraine (0.68) demonstrates the gradual implementation of international norms, but remains fragmented in the application of digital authenticity control mechanisms. The comparative analysis data confirm that clear technical and legal standards directly affect the authenticity and reproducibility of digital evidence. In Ukraine, there is potential for increasing harmonization through the development of unified digital protocols and the implementation of ISO/IEC 27037 and NIST IR 8387 requirements in the internal regulations of forensic institutions.

5.2. Functional and Analytical Assessment of Documentation Procedures

The functional and analytical assessment showed that the effectiveness of forensic documentation is determined not by individual operations, but by the degree of standardization and consistency of procedures at all stages — from the moment of

detection of a digital artifact to its expert verification and submission to court. The study assessed four key stages: detection and initial capture; hashing and authentication; storage and transfer (chain of custody); expert verification and processing. The value of each stage was determined on a scale of 0–1, where 1 reflects full compliance with the requirements of ISO/IEC 27037, ISO/IEC 27041 and NIST IR 8387. The objectivity of the assessment was ensured by using an operationally structured scheme. The scheme provided that the experts analysed specific actions: correctness of media isolation, use of write-block, initial logging and creation of photo tables; selection and duplication of hash functions, capture of time stamps and independent logging; continuity of chain of custody, availability of digital signatures, audit logs and access control; reproducibility of expert methods, compliance with the conclusion of ISO/IEC 27041 and procedural accuracy of recording actions. The assessment was carried out according to a criteria matrix of 18 operational indicators, grouped into four blocks (recording, hashing, storage, proceduralization) and agreed within the Delphi–AHP procedure. To minimize subjectivity, standardized ISO checklists were used (ISO/IEC 27037 Annex A; ISO/IEC 27041 Annex C), which provided uniform criteria for all experts. The consistency of the assessments was confirmed by the concordance coefficient W = 0.79, which indicates the stability of the obtained results summarized in Table 3.

Table 3: Comparative effectiveness of digital evidence documentation procedures in the studied countries

Documentation stage	Ukraine	Germany	UK
Detection and initial capture	0.74	0.86	0.89
Hashing and authentication	0.68	0.88	0.91
Chain of custody	0.61	0.84	0.93
Expert verification and processing	0.72	0.81	0.88
Average performance (FDII-stage)	0.69	0.85	0.90

Source: calculated by the author based on the regulatory acts Forensic Science Regulator's Code [25], Digital Forensics Science Strategy [26], Gesetz zur Fortentwicklung der Strafprozessordnung [27], Order of the Ministry of Justice of Ukraine No. 3505/5 [28], CPC of Ukraine [29], ISO/IEC 27037:2012 [30], ISO/IEC 27041:2015 [31] and NIST IR 8387 [16] and expert survey (Delphi–AHP, n = 27)

The results show that the UK demonstrates the highest efficiency at all stages of documentation, which is explained by the full digitalization of the chain of custody and the use of centralized audit systems within the Forensic Science Regulator's Code. Germany has a stable reproducibility of procedures, especially at the hashing stage (0.88), thanks to the clear technical regulations of the Gesetz zur Fortentwicklung der Strafprozessordnung [27] and BKA standards. Ukraine demonstrates a relatively high level of fixation and expert verification, but the retention rates (0.61) remain lower due to the lack of a single digital evidence movement register and an automated chain of custody monitoring system.

Data analysis shows that the most critical link in all three systems is the stage of evidence preservation and transfer, which determines the overall level of integrity of evidentiary information. At the same time, the British model is distinguished by the highest level of process automation, the German model — by the legal clarity of procedures, and the Ukrainian model — by the potential for rapid adaptation of international standards ISO/IEC 27037 and NIST IR 8387 into national practice through the update of methodological instructions of the Ministry of Justice and the implementation of a unified system of digital evidence monitoring.

5.3. Testing the conceptual model of methodological support for documenting evidence

The developed three-level model – technical, organizational and legal levels – was tested based on expert modelling of procedures in three jurisdictions: Ukraine, Germany, and the UK. The purpose of the test was to verify the impact of the model implementation on increasing the consistency and reliability of the processes of documenting digital and physical evidence. For this purpose, the values of the TD, PA, CC and MS parameters were calculated before and after the model implementation. The obtained data are presented in Table 4.

Table 4: Dynamics of changes in FDII parameters after the model implementation

Country	TD (before)	TD (after)	PA (before)	PA (after)	CC (before)	CC (after)	MS (before)	MS (after)	FDII (before)	FDII (after)

Ukraine	0.68	0.81	0.70	0.84	0.61	0.78	0.66	0.80	0.66	0.81
Germany	0.84	0.90	0.85	0.91	0.84	0.90	0.80	0.88	0.83	0.90
UK	0.88	0.93	0.89	0.95	0.93	0.96	0.86	0.91	0.89	0.94

Source: calculated by the author based on expert modelling data (Delphi–AHP, n = 27)

To verify the non-randomness of the changes between the indicators "before" and "after" the implementation of the model, a t-test for dependent samples was used. The analysis showed a statistically significant increase in the values of TD, PA, CC, and MS in all three jurisdictions ($p < 0.05$), which confirms the reality and systematicity of the recorded changes and indicates the validity of the impact of the proposed model on the consistency of forensic procedures. As Table 4 shows, a noticeable increase in the indicators of technical reliability (TD), procedural admissibility (PA), chain of custody integrity (CC) and methodological standardization (MS) was recorded in all three countries after the implementation of the conceptual model. The largest increase is observed in Ukraine — the average increase is about 0.15 points, which indicates a significant improvement in the procedures for recording, hashing, and chain of custody control. In Germany and the UK, the dynamics are more moderate (≈ 0.06–0.07 points), which is explained by the high basic level of development of their forensic systems and standardized documentation procedures. The results of the testing show that the application of the proposed model made it possible to significantly increase the level of methodological consistency and integrity of procedures.

The largest increase in the integral FDII is observed in Ukraine — from 0.66 to 0.81, which is due to the introduction of digital chain of custody audit and standardization of hashing stages according to ISO/IEC 27037 and NIST IR 8387. In Germany, the increase is moderate (from 0.83 to 0.90), as most procedures have already been codified, and the improvement mainly concerned the automation of evidence integrity control. In the UK, the integral index increased from 0.89 to 0.94, indicating an increase in analytical reproducibility and accuracy of procedures due to the improvement of digital data verification protocols and interaction between the Forensic Science Regulator's Office and police agencies. So, the dynamics of the FDII increase is most intense in systems with a previously lower level of standardization – in particular, in Ukraine. This supports the hypothesis that the structured methodological integration of technical, legal and organizational components significantly improves the reproducibility and admissibility of digital evidence in pre-trial proceedings, ensuring the transition to a comprehensive evidence management system, consistent with international ISO and NIST standards.

5.4. Correlation and Structural Analysis of the Relationship between FDII Parameters

A correlation and structural analysis was conducted to assess the interaction between the components of the Forensic Documentation Integrity Index (FDII) – technical reliability (TD), procedural admissibility (PA), chain of custody integrity (CC), and methodological standardization (MS). The average values of the correlation coefficients for the three countries are shown in Figure 2.

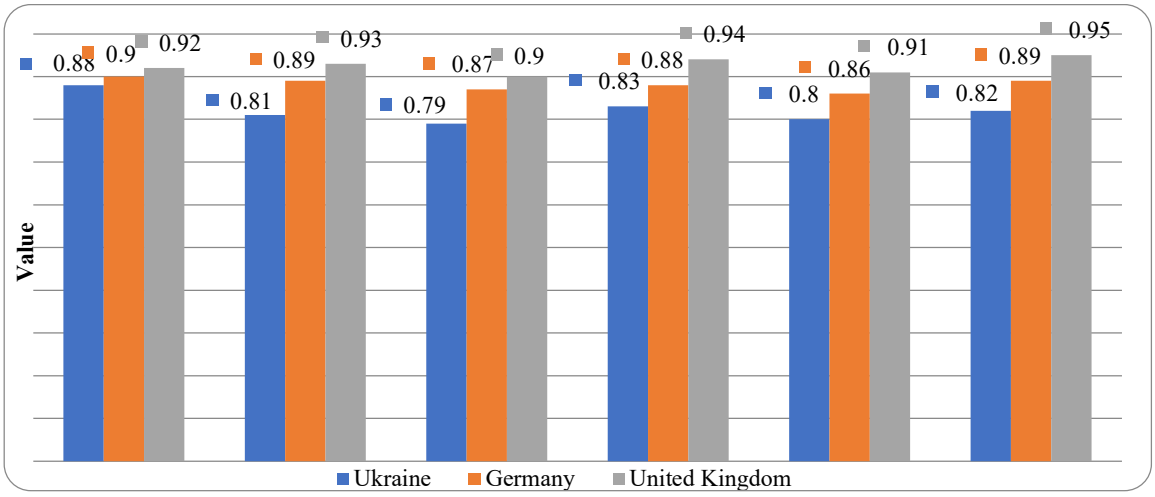

Figure 2: Correlation structure of FDII parameters in the studied countries
Source: calculated by the author based on expert modelling data (Delphi–AHP, n = 27)

The results presented in Figure 2 showed that all pairs of parameters demonstrate high positive correlations (0.79–0.95), indicating a systemic interdependence of technical, procedural, and methodological components of evidence documentation. The highest values are observed in the UK, where the combination of a digitalized chain of custody and full integration of ISO/NIST standards provides maximum consistency between PA–CC (0.94) and CC–MS (0.95). In Germany, correlations remain consistently high (0.86–0.90), which is explained by the codified nature of the StPO and standardized BKA procedures. Ukraine demonstrates correlations at the level of 0.79–0.88, which reflects a gradual approach to the structural model of evidence management typical of the EU and the UK.

The chain of custody integrity (CC) parameter is of particular importance, which acts as a systemic "core" that influences other components in the analysis. Increasing the controllability of CoC leads to an increase in the procedural admissibility of evidence (PA), as it is CoC that determines the transparency of the origin, movement, and authenticity of digital artifacts. At the same time, CC correlates with methodological standardization (MS), as the implementation of ISO/IEC 27037 and NIST IR 8387 provides for unified protocols for verification, logging, and capture of digital traces. This creates a situation in which the improvement of CC triggers a "domino effect" – strengthens TD, stabilizes PA, and contributes to the growth of MS.

The cause-and-effect relationships were clearly presented using the developed simplified structural model (Figure 3), which illustrates the central role of the CC parameter in shaping the overall integrity of the documentation process.

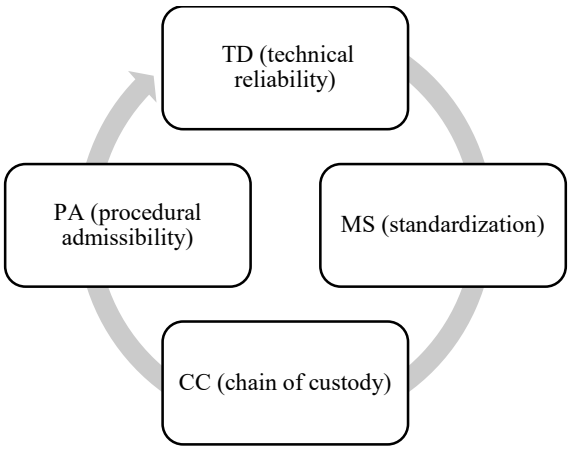

Figure 3: Diagram of causal and structural relationships
Source: created by the authors

The logic of the model presented in Figure 3 is that the chain of custody (CC) parameter determines the transparency and controllability of the movement of digital and physical evidence. The ability to confirm the origin of data, its immutability, and the correctness of the transfer procedures depends on it. The further influence of CC is traced in the procedural admissibility (PA), as judicial practice directly assesses the continuity and reliability of the chain of custody. In the event of any break or unclearly documented stage, the evidence may be declared inadmissible, even if its technical parameters remain impeccable. Methodological standardization (MS) enhances the value of CC, as the application of ISO/IEC 27037, ISO/IEC 27041 and NIST recommendations provides for unified protocols for hashing, logging, recording actions, and access control. This ensures structural stability of the procedures and minimizes the risks of subjective decisions at the stages of evidence processing. Technical reliability (TD) also shows dependence on CC, as the authenticity of digital artifacts is determined by the correctness of the procedures for hashing, duplicating checksums, introducing time stamps, and maintaining audit logs. If the chain of custody functions stably, the technical parameters of the evidence remain reproducible and verifiable. In general, this approach allows not only to record the level of correlations between the FDII parameters, but also to identify the mechanisms of their structural influence, which form the overall consistency of the evidence documentation systems in the three countries.

5.5. Scientific and Analytical Interpretation of Research Results and Directions for Methodological Improvement

The results of the comprehensive analysis confirm that the effectiveness of forensic documentation systems for digital and physical evidence is determined by the level of regulatory harmonization, the degree of automation of procedures, and the quality of inter-institutional interaction. A comparative study of Ukraine, Germany, and the UK has revealed significant differences in the structure and maturity of national models, as well as identifying areas for improving Ukrainian practice, taking into account international experience. In the UK, a holistic model has been formed in which technical reliability, procedural admissibility, integrity of the chain of custody, and methodological standardization form a single integrated digital evidence management system. Its effectiveness is ensured by the regulatory complex of the Forensic Science Regulator's Code and the Digital Forensics

Science Strategy, which integrate ISO/IEC 27000-series standards and NIST recommendations. This provides a stable level of correlations between parameters (0.90–0.95) and ensuring the highest reproducibility of evidentiary processes. Germany demonstrates a balanced system, combining a codified legal framework (StPO, Gesetz zur Fortentwicklung der StPO) and a centralized technical infrastructure of the BKA. The high correlation between technical reliability, procedural admissibility and chain of custody integrity (0.88–0.90) indicates a stable synergy between legal norms and technical procedures, while the development of digital platforms for expert units strengthens chain of custody control. Ukraine is at the stage of active integration of international standards into national practice. After testing the proposed three-level model, the FDII indicator increased from 0.66 to 0.81, which confirms the effectiveness of the methodological approach focused on combining technical, organizational, and legal mechanisms. The main achievements were the standardization of the fixation and hashing processes, as well as the development of the concept of a single digital chain of custody registry. At the same time, the fragmentation of the regulatory framework, the limited level of audit automation, and the lack of a full-fledged mechanism for independent verification of evidence remain the key challenges.

The results of the study enable identifying priority areas for improving the Ukrainian system of documenting digital and physical evidence. First of all, it is necessary to ensure the full implementation of the ISO/IEC 27037, ISO/IEC 27041, and NIST IR 8387 standards in the regulatory documents of the Ministry of Justice, the Ministry of Internal Affairs and forensic institutions. An important task is to create a single electronic register of evidence movement, integrated with information systems of pre-trial investigation, which will guarantee the continuity of the chain of custody and transparency of control. It is necessary to introduce digital verification of hash identifiers to confirm the authenticity of artifacts and introduce an independent audit of forensic processes in order to increase the level of reproducibility and trust in expert conclusions. It is also advisable to create a national system for training digital forensic experts, focused on the practical application of international evidence management standards.

Summarizing the results, it can be stated that the introduction of a comprehensive methodological model, built on the principles of international standardization ISO and NIST, provides a significant increase in the reliability, reproducibility and legal stability of digital evidence in pre-trial proceedings. This creates the basis for the establishment of an integrated forensic evidence management system in Ukraine compatible with European and British practices.

6. DISCUSSION

The results confirm that the effectiveness of forensic documentation systems is determined not only by the quality of individual operations, but primarily by the level of regulatory integration, procedural consistency, and standardized digital chain of custody control.

The original contribution of this study lies in the transition from descriptive comparison to an index-based assessment of forensic documentation systems. The proposed FDII model improves prior approaches by integrating technical, legal, organizational, and methodological dimensions into one measurable framework. This additional knowledge enables cross-jurisdictional comparison and helps identify the weakest structural elements of evidence documentation systems.

In terms of IT knowledge enhancement, the obtained results demonstrate that the main value of the proposed model lies in the integration of existing best practices rather than in the isolated introduction of a single new technical procedure. ISO/IEC and NIST standards already define important requirements for digital evidence preservation, hashing, logging, and verification. However, the FDII model extends this knowledge by showing how these requirements interact with procedural admissibility, organizational accountability, and chain of custody integrity. Thus, the study contributes new analytical knowledge by converting dispersed technical and legal requirements into a measurable framework for comparing and improving forensic documentation systems.

This is consistent with the findings of Nath et al. [24], Khan and Ahmed [22], who indicate that the authenticity of digital evidence is ensured only if all stages of its life cycle are formalized and technical and legal verification mechanisms are combined [23].

The high FDII score in the UK (0.94) demonstrates the effectiveness of the model that combines ISO/IEC and NIST requirements with procedural norms enshrined in the Forensic Science Regulator's Code [25] and the Digital Forensics Science Strategy [26]. As White [32], Gillett and Fan [33] emphasize, the combination of technical

reproducibility with independent regulatory control is a key factor in the trust in digital evidence. The German system (StPO, BKA) is also characterized by stable integration of technical and legal procedures, which is confirmed by correlation indicators (r = 0.88–0.90) and is consistent with the findings of Bharati et al. [34].

Ukraine, despite the lower starting level, demonstrated the greatest dynamics of FDII growth (+0.15) after the implementation of the three-level model, which confirms the effectiveness of gradual harmonization with ISO/IEC 27037 and NIST IR 8387. This correlates with the findings of Allah Rakha [35], Gupta and Husain [20], Ismail and Ariffin [21] regarding the critical role of international standards and independent auditing in the formation of a reliable evidentiary infrastructure.

At the same time, some positions in the literature partially disagree with the obtained results. Brown [17] notes that excessive regulation can create procedural barriers and slow down the extraction of digital artifacts. Kasper and Laurits [18] emphasize that strict formalization does not always automatically increase evidential value, while Marcinauskaitė [12] indicates that in some jurisdictions courts admit electronic evidence even without a full set of hash procedures. These statements partially contradict the above approach. However, the obtained empirical data demonstrate that it is structured standardization that provides the greatest increase in technical reliability and procedural admissibility: the increase in FDII in Ukraine by +0.15 confirms the practical effectiveness of unified procedures and compensates for the potential risks of "excessive formalization".

Correlation values (r = 0.79–0.95) confirm the concept of a "digital evidentiary ecosystem" by Kuczyńska [36], which implies that technical protocols, regulations, and expert procedures function as an interconnected and interdependent mechanism for ensuring the authenticity and reproducibility of digital artifacts. The high correlation between TD, PA, CC, and MS indicates that a change in any of the parameters automatically affects the others, forming a stable structural configuration of the evidence management system. The highest performance is demonstrated by models where legal norms, digital infrastructure and ISO/NIST standards work not in a fragmented manner, but in an integrated manner – when the processes of fixation, hashing, storage and verification are regulated by a single methodological framework and controlled by similar protocols.

Ukrainian experience confirms that it is the gradual standardization – from the synchronization of hash algorithms to the implementation of digital audit chain of custody – that gradually brings national practice closer to European and British models. The growth of FDII by +0.15 demonstrates that the effect of standardized integration is not only normative, but also measurable in the form of an increase in the technical reliability and procedural admissibility of evidence. The results presented in the study give grounds for further research aimed at automated monitoring of the movement of evidence, the development of algorithms for independent digital verification and the creation of models of international compatibility of evidence management systems in transnational criminal proceedings.

7. LIMITATIONS

The study has certain limitations related to the sample size and availability of empirical data. Expert modelling was based on assessments of 27 experts from three countries, which may affect the generalizability of the results due to differences in national procedures for documenting evidence. Access to internal regulations of forensic institutions remains limited, especially in the UK, where some protocols are confidential. In addition, the assessment of FDII parameters was carried out using aggregated indicators that do not take into account industry specifics (cybercrime, financial investigations, etc.). Despite this, the obtained results have high analytical reliability and can serve as the basis for further research with an expanded empirical base and the involvement of additional indicators, in particular, parameters of automated audit, interagency interaction, and independent verification of evidence. The main threats to validity are related to expert selection, construct simplification, and the limited number of jurisdictions. Purposeful expert sampling may reflect institutional experience, while the FDII reduces complex forensic procedures to four measurable parameters. These risks were mitigated by the Delphi–AHP procedure, Kendall concordance testing, and the linkage of each parameter to ISO/IEC, NIST, and national procedural requirements. The strength of the study lies in the integration of legal, technical, and organizational criteria into one analytical model. Its weakness is the reliance on expert modelling rather than large-scale operational datasets from real criminal cases.

8. CONCLUSIONS

The study showed that the quality of forensic documentation of digital and physical evidence

depends not only on technical tools, but primarily on the extent to which the norms, procedures and standards used by investigators, experts and prosecutors are consistent with each other. A comparison of Ukraine, Germany, and the UK showed that the level of compliance with international ISO/IEC and NIST standards directly affects the reliability and admissibility of digital materials. The highest system integrity indicator (FDII = 0.94) was recorded in the UK, where the digital chain of custody, ISO standards and the requirements of the Forensic Science Regulator's Code work as a single model of evidence management. Germany (FDII = 0.90) maintains high stability due to the codification of procedures in the StPO and the technical infrastructure of the BKA. Ukraine (FDII = 0.81) demonstrates rapid growth in indicators, but the regulatory framework and digitalization of processes remain incomplete. Correlation analysis confirmed the close relationship between technical reliability, procedural admissibility and chain of custody controllability (r = 0.79–0.95). This means that strengthening any of these elements automatically increases the overall reliability of the evidentiary process. This is most clearly evident in the British model, where strict fixation of the chain of custody directly strengthens the judicial admissibility of digital artifacts. Testing of the author's three-level model confirmed its effectiveness: in Ukraine, the integral FDII increased from 0.66 to 0.81. This proves that the unification of technical, organizational, and legal procedures can significantly increase the reliability of digital evidence. Further development of the Ukrainian system requires:

- full implementation of ISO/IEC 27037 and NIST IR 8387 standards;
- creation of a single electronic chain of custody registry;
- introduction of independent digital verification and audit;
- development of professional training of digital forensics experts.

The main contribution of the study is the development and testing of the FDII-based model as a measurable tool for assessing forensic documentation systems. Unlike previous descriptive approaches, the model integrates technical reliability, procedural admissibility, chain of custody integrity, and methodological standardization within one analytical framework. This provides additional knowledge for digital forensics by showing how the weakest elements of evidence documentation can be identified and improved across different legal systems.

In relation to the problem statement, the study showed that the main weakness of forensic documentation systems lies in the fragmentation between technical standards, procedural requirements, and organizational control mechanisms. In relation to previous literature, the study contributes by moving beyond separate discussions of digital evidence admissibility, chain of custody, and ISO/NIST compliance. The proposed FDII-based model integrates these dimensions into one measurable framework and therefore provides a structured tool for assessing and improving forensic documentation systems. Future research should test the model on real case files, expand the number of jurisdictions, and develop automated audit indicators for digital chain of custody control.

The obtained results give grounds for the modernization of the national evidentiary infrastructure and its approximation to European and British standards.

Future research should test the FDII model on real case files, expand the number of jurisdictions, and develop automated audit indicators for digital chain of custody control. Further studies should also examine the applicability of the model to specific categories of proceedings, including cybercrime, financial investigations, and transnational evidence exchange.

REFERENCES

[1] Y. Tymoshenko, D. Kyslenko, E. Kuzmichova-Kyslenko, I. Leonenko and I. Servetsky, "Features of the pre-trial investigation of air pollution", *Environment and Ecology Research*, Vol. 10, No. 2, 2022, pp. 133–145. https://doi.org/10.13189/eer.2022.100203

[2] T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk and S. Podolyaka, "Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine", *Journal of Information Technology Management*, Vol. 13, 2021, pp. 75–90. https://doi.org/10.22059/JITM.2021.80738

[3] O. M. Omelchuk, I. Y. Haiur, O. G. Kozytska, A. V. Prysiazhna and N. V. Khmelevska, "Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences", *Journal of Money Laundering*

Control, Vol. 25, No. 3, 2022, pp. 700–716. https://doi.org/10.1108/JMLC-07-2021-0073

[4] B. Y. Chalyi, "Technical and forensic support of the investigation of criminal offences related to raiding", *Bulletin of Criminological Association of Ukraine*, Vol. 35, No. 2, 2025, pp. 317–326. https://doi.org/10.32631/vca.2025.2.26

[5] B. Rappert, D. Wilson-Kovacs, H. Wheat and S. Leonelli, "Evincing offence: How digital forensics turns big data into evidence for policing sexual abuse", *Engaging Science, Technology, and Society*, Vol. 8, No. 3, 2022. https://doi.org/10.17351/ests2022.1049

[6] P. Van Schaik, A. Irons and K. Renaud, "Privacy in UK police digital forensics investigations", in *Proceedings of the Hawaii International Conference on System Sciences (HICSS 2024)*, 2024. https://pureportal.strath.ac.uk/en/publications/privacy-in-uk-police-digital-forensics-investigations/

[7] C. Karagiannis and K. Vergidis, "Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal", *Information*, Vol. 12, No. 5, 2021, Art. no. 181. https://doi.org/10.3390/info12050181

[8] P. Anderson, D. Sampson and S. Gilroy, "Digital investigations: Relevance and confidence in disclosure", *ERA Forum*, Vol. 22, 2021, pp. 587–599. https://doi.org/10.1007/s12027-021-00687-1

[9] T. Göbel, H. Baier and F. Breitinger, "Data for digital forensics: Why a discussion on 'how realistic is synthetic data' is dispensable", *Digital Threats: Research and Practice*, Vol. 4, No. 3, 2023, pp. 1–18. https://doi.org/10.1145/3609863

[10] A.-M. Yu. Anheleniuk, "Legal evaluation of electronic evidence in the criminal process of Ukraine through the prism of court decisions", *Countering Crime: Practical Issues and Scientific and Methodological Support*, Vol. 1, 2024. https://doi.org/10.32850/sulj.2024.1.4

[11] V. V. Romaniuk and S. Ye. Ablamskyi, "Criteria for the admissibility of digital (electronic) evidence in criminal proceedings", *Law and Safety*, Vol. 93, No. 2, 2024, pp. 140–150. https://doi.org/10.32631/pb.2024.2.13

[12] R. Marcinauskaitė, "Electronic evidence in criminal proceedings", in *Towards Coherence in Criminal Justice: Challenges, Discussions and/or Solutions*, 2024, pp. 183–201. https://doi.org/10.3726/b22750

[13] H. O. Abdullah, M. Maqsood and A. Nadeem, "Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era", *Research Journal for Social Affairs*, Vol. 3, No. 5, 2025, pp. 795–805. https://doi.org/10.71317/RJSA.003.05.0375

[14] T. Göbel, H. Baier and D. Wolf, "Scenario-based data set generation for use in digital forensics: A case study", in *INFORMATIK 2024*, Gesellschaft für Informatik e.V., 2024, pp. 355–370. https://doi.org/10.18420/inf2024_25

[15] A. Abdul-Samad, M. M. Siraj, S. H. Othman, M. H. Rahman and M. Z. A. Darus, "Comprehensive review on data preservation models and standards in digital forensics", in *Proceedings of the 2024 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, 2024, pp. 277–282. https://people.utm.my/hajar/conference-proceedings/

[16] B. Guttman, D. R. White and T. Walraven, *NIST Interagency Report 8387: Digital Evidence Preservation*. National Institute of Standards and Technology, 2022. https://doi.org/10.6028/NIST.IR.8387

[17] C. S. Brown, "Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice", *International Journal of Cyber Criminology*, Vol. 9, No. 1, 2015, pp. 55–119. https://doi.org/10.5281/zenodo.22387

[18] A. Kasper and E. Laurits, "Challenges in collecting digital evidence: A legal perspective", in *The Future of Law and eTechnologies*, Cham: Springer International Publishing, 2016, pp. 195–233. https://doi.org/10.1007/978-3-319-26896-5_10

[19] Z. Illési, "Digital evidence management for organizational legal compliance", *Interdisciplinary Description of Complex Systems: INDECS*, Vol. 23, No. 3, 2025, pp. 217–229. https://doi.org/10.7906/indecs.23.3.3

[20] G. Gupta and A. Husain, "Digital evidence in police investigation: A comparative analysis of challenges faced in India, the UK and the United States", *Journal of Victimology and Victim Justice*, Vol. 6, No. 2, 2023. https://doi.org/10.1177/25166069231184977

[21] I. Ismail and K. A. Z. Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance", *PLOS ONE*, Vol. 20, No. 9, 2025, Art. no. e0331683. https://doi.org/10.1371/journal.pone.0331683

[22] M. N. I. Khan and I. Ahmed, "A systematic review of judicial reforms and legal access

strategies in the age of cybercrime and digital evidence", *International Journal of Scientific Interdisciplinary Research*, Vol. 5, No. 2, 2025, pp. 1–29. https://doi.org/10.63125/96ex9767

[23] M. N. I. Khan, "Legal documentation and case management: A systematic review of digitization trends and cybersecurity challenges in legal support roles", *Review of Applied Science and Technology*, Vol. 2, No. 1, 2023, pp. 1–25. https://doi.org/10.63125/21hf4w52

[24] S. Nath, K. Summers, J. Baek and G. J. Ahn, "Digital evidence chain of custody: Navigating new realities of digital forensics", in *Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, IEEE, 2024, pp. 11–20.

[25] Forensic Science Regulator, *Forensic Science Regulator's Code of Practice*. UK Home Office, 2021. https://www.gov.uk/government/publications/forensic-science-regulator-code-of-practice

[26] National Police Chiefs' Council, *National Digital Forensic Science Strategy*. National Police Chiefs' Council, 2020. https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf

[27] Bundesministerium der Justiz, *Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften (BGBl. I S. 3932)*. Bundesgesetzblatt, 2021. https://dip.bundestag.de/vorgang/gesetz-zur-fortentwicklung-der-strafprozessordnung-und-zur-%C3%A4nderung-weiterer-vorschriften/272971

[28] Ministry of Justice of Ukraine, *On Approval of the Instruction on the Specifics of Forensic Expert Activity by Certified Forensic Experts Who Do Not Work in State Specialized Expert Institutions: Order No. 3505/5*. Legislation of Ukraine, Verkhovna Rada of Ukraine, 2011. https://zakon.rada.gov.ua/go/z1431-11

[29] Verkhovna Rada of Ukraine, *Criminal Procedure Code of Ukraine: Law No. 4651-VI*. Legislation of Ukraine, 2012. https://zakon.rada.gov.ua/laws/show/4651-17#Text

[30] International Organization for Standardization, *ISO/IEC 27037:2012. Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. ISO, 2012. https://www.iso.org/standard/44381.html

[31] International Organization for Standardization, *ISO/IEC 27041:2015. Information Technology — Security Techniques — Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods*. ISO, 2015. https://www.iso.org/standard/44407.html

[32] E. White, "Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism", *Leiden Journal of International Law*, Vol. 37, No. 1, 2024, pp. 228–250. https://doi.org/10.1017/S0922156523000444

[33] M. Gillett and W. Fan, "Expert evidence and digital open source information: Bringing online evidence to the courtroom", *Journal of International Criminal Justice*, Vol. 21, No. 4, 2023, pp. 661–693. https://doi.org/10.1093/jicj/mqad050

[34] R. Bharati, P. G. Khodke, C. P. Khadilkar and D. S. Bawiskar, "Forensic bytes: Admissibility and challenges of digital evidence in legal proceedings", *International Journal of Scientific Research in Science and Technology*, Vol. 11, No. 16, 2024, pp. 24–35. https://doi.org/10.2139/ssrn.4896874

[35] N. Allah Rakha, "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations", *Mexican Law Review*, Vol. 16, No. 2, 2024, pp. 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

[36] H. Kuczyńska, "The ICC enters into the future: The digital-evidence revolution or evolution?", *Revista Brasileira de Direito Processual Penal*, Vol. 10, No. 3, 2024, Art. no. e1073. https://doi.org/10.22197/rbdpp.v10i3.1073