

7. Крижановський О. О. Діяльність органів внутрішніх справ в умовах надзвичайних станів. *Юридичний вісник*. 2020. № 2. С. 45-52.

Годорожа О.,
здобувач ступеня вищої освіти бакалавра
Донецького державного
університету внутрішніх прав
Консультант з мови: Березенко Н.

STANDARDS AND PRACTICES OF DIGITAL FORENSICS: COMPARATIVE ANALYSIS OF NIST, ISO, AND ENFSI GUIDELINES FOR ENSURING THE ADMISSIBILITY OF DIGITAL EVIDENCE

Digital forensics has become increasingly relevant in today's society due to the rapid growth of cybercrime, the proliferation of digital devices, and the critical role of electronic evidence in legal proceedings. The relevance of this topic lies in the need to ensure that digital evidence is reliable, scientifically validated, and legally admissible, particularly in contexts where incorrect or incomplete analysis may compromise justice. The purpose of this study is to analyze international standards and best practices in digital forensics, identify their strengths and limitations, and propose recommendations for their implementation in national forensic practice to enhance the credibility and admissibility of digital evidence.

Modern digital forensics operates at the intersection of technical, legal, and methodological requirements, and therefore relies on international standards that ensure the reliability and admissibility of digital evidence in court. The report NIST IR 8354 "Digital Investigation Techniques" emphasizes that digital methods are based on well-established principles of computer science, yet they possess inherent limitations related to data incompleteness, loss of artifacts, and the possibility of obtaining fragmented or partially corrupted information [1, pp. 9–10]. These considerations highlight the need for scientific validation of forensic tools, as well as the documentation of

error rates during data recovery or analysis, since these factors directly influence the evidentiary value of digital information.

The international standard ISO/IEC 27037:2012 defines the core principles of identifying, collecting, acquiring, and preserving digital evidence, establishing a globally recognized procedure that significantly strengthens the reliability of forensic artifacts. Pages 8–12 outline the requirements for documenting the chain of custody, ensuring process repeatability, and confirming the competence of personnel responsible for evidence collection and initial handling [2, pp. 8–12]. These requirements guarantee the integrity of digital evidence and minimize the risk of manipulation or unintentional data alteration.

The European document ENFSI Best Practice Manual for the Forensic Examination of Digital Technology (BPM-FIT-01) provides detailed practical guidelines for the operation of forensic laboratories. Pages 6–11 describe procedures for the seizure, packaging, transportation, and initial examination of digital devices [ENFSI BPM-FIT-01, pp. 6–11]. Further sections emphasize verification and uncertainty assessment: page 22 sets out the requirement to identify and document potential errors accumulated throughout the forensic process [3, p. 22], while section 6.5 (page 25) establishes mandatory verification for all critical forensic actions [p. 25]. Additionally, the manual requires regular proficiency testing and technical verification of forensic tools, as detailed in section 12.5 (page 38), ensuring stability and reproducibility of results [3 p. 38].

Taken together, these standards demonstrate that NIST provides the scientific foundation of digital forensic methods, ISO sets procedural requirements for evidence handling and preservation, and ENFSI delivers practical algorithms and quality-assurance mechanisms. The combined implementation of these approaches in Ukrainian law-enforcement practice would significantly enhance the trustworthiness of digital evidence and ensure its unquestionable admissibility in judicial proceedings, supporting the broader goal of strengthening the integrity and efficiency of the criminal justice system.

In conclusion, the analysis of NIST, ISO, and ENFSI standards confirms that the adoption of international best practices is essential for reliable digital investigations. By integrating scientific validation, rigorous procedural safeguards, and practical quality-assurance measures, law enforcement agencies can ensure that digital evidence is

credible, reproducible, and fully admissible in court. Therefore, the implementation of these standards should be considered a priority for improving both the effectiveness of forensic investigations and the overall fairness of the judicial process.

References:

1. NIST. Digital Investigation Techniques (NIST IR 8354). National Institute of Standards and Technology, 2022. pp. 9–10. URL: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf>
2. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012. pp. 8–12. URL: <https://www.iso.org/standard/44381.html>
3. 3.ENFSI. Best Practice 3. Manual for the Forensic Examination of Digital Technology (BPM-FIT-01). *European Network of Forensic Science Institutes*, 2016. pp. 6–38. URL: https://enfsi.eu/wp-content/uploads/2016/09/1._pdf
- 4.

Горячов О.,

здобувач ступеня вищої освіти бакалавра
Криворізького навчально-наукового
інституту Донецького державного
університету внутрішніх справ
Консультант з мови: Снісаренко І.

LANGUAGE POLICY AND THE FUNCTIONING OF THE STATE LANGUAGE IN UKRAINE: LEGAL AND SOCIAL ASPECTS

The issue of language policy in Ukraine is closely connected to the processes of national identity formation, social integration, and state-building. The Ukrainian language, as the only state language, performs not only communicative but also symbolic and unifying functions in society. At the same time, the question of ensuring its full functioning remains one of the most sensitive socio-political topics. The