




Kherson State University
West Ukrainian National University
Petro Mohyla Black Sea National University
Riga Nordic University

CYBERCRIME AND DIGITAL EVIDENCE: CROSS-DISCIPLINARY CHALLENGES AND PROSPECTS IN CONTEMPORARY LAW

Scientific monograph



2026

Recommended for publication and online distribution by the Academic Council of Kherson State University in accordance with Minutes No. 14 dated April 27, 2026 and by the Academic Council of West Ukrainian National University in accordance with Minutes No. 8 dated April 29, 2026.

Reviewers:
Fernando de Brito Alves – PhD, Professor, Professor of State University of North Paraná (UENP), Brazil;
Oleksii Oderii – DSc (Law), Professor, Professor at the Department of Criminal Procedure and Criminalistics, Donetsk State University of Internal Affairs;
Artem Kovalenko – PhD in Law, Associate Professor, Senior Lecturer at the Department of Law named after Academician of the Ukrainian Academy of Sciences Father Ivan Lutsky of the Faculty of Social and Applied Sciences, King Danylo University.

Editorial Board:
Head of the Editorial Board – **Stratonov Vasyl Mykolaiovych** – Doctor of Law, Professor, Honored Lawyer of Ukraine, Academician of the National Academy of Higher Education Sciences of Ukraine, Professor at the Department of National, International Law and Law Enforcement, Kherson State University;
Djakons Romans – Doctor of Engineering, Professor, Academician, Chairman of the Board of Riga Nordic University;
Havlovska Alina Oleksandrivna – PhD in Law, Associate Professor, Head of the Department of National, International Law and Law Enforcement, Kherson State University;
Dziurbel Andrii Dariiovych – PhD in Law, Assistant Professor at the Department of Criminal Law and Process, West Ukrainian National University;
Koval Alla Anatoliivna – Doctor of Law, Professor, Professor, Head of the Department of Constitutional and Administrative Law and Process, Petro Mohyla Black Sea National University.

Cybercrime and Digital Evidence: Cross-Disciplinary Challenges and Prospects in Contemporary Law : Scientific monograph. Riga, Latvia : "Baltija Publishing", 2026. 404 p.

© Kherson State University, 2026
© West Ukrainian National University, 2026
© Petro Mohyla Black Sea National University, 2026
© Riga Nordic University, 2026

ISBN 978-9934-26-686-7

CONTENTS

THE CONSTITUTIONAL BOUNDARIES OF DIGITAL EVIDENCE: INTRUSIVE MEASURES, CYBERSECURITY AND NATIONAL SECURITY IN ROMANIA (Safta, M., Stanciu, C. A. M.) 1
1. Data Retention and Structural Surveillance. Constitutional and European Standards 2
2. Technical Surveillance in Criminal Proceedings: Constitutional Limits and Safeguards 8
3. Cybersecurity and Structural Preventive Surveillance 13

AUTHENTICITY AND ADMISSIBILITY OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS THROUGH THE PRISM OF CRIMINAL PROCEDURE PRINCIPLES (Voloshyna V. K.) 21
1. Prerequisites for the problem of authenticity and admissibility of digital evidence 22
2. Legal nature and concept of digital evidence in criminal proceedings 26
3. Procedural principles for ensuring the admissibility of digital evidence 29
4. International standards of admissibility of digital evidence and the practice of the ECHR 32
5. Peculiarities of recording and ensuring the integrity of digital evidence in criminal proceedings 34

BASICS OF RECORDING CYBER OFFENSES THAT INFLUENCE THE MENTAL STATE OF COMPUTER OPERATORS (Gavrylenko Ye. V., Sakhanchuk A. D., Sakhanchuk T. I.) 42
1. Emergence of prerequisites and formulation of the problem 43
2. Method of cyber threats' influence on computer operators 43
3. List and scope of activities of global computer laboratories studying penetration testing 47
4. Leading research centers for the study of remote influence on the psyche of computer operators 47
5. Development and application of testers for recording optical influence on computer operators to secure digital evidence of cyber offenses 49
6. Influence of white light components on the mental state of computer operators through the subconscious mind 53

THE MAIN LAW ON INFORMATION PROTECTION (Hromyko I. O.) 57
1. Information activities of information carriers 58
2. Communicability as a unifying universal term 62
3. Classification of "communicabiliti of information carriers" 66

FEATURES OF THE RECORDING OF DIGITAL TRACES
DURING INVESTIGATIVE (SEARCH) ACTIONS (Dzyurbel A. D.) 71
1. The concept, classification and forensic characteristics
of digital traces in modern forensics 72
2. Procedural procedure for obtaining and international standards
for identifying and preserving electronic evidence 77
3. Техн Technical, forensic and tactical support for the extraction
of digital information 83
4. Typical errors and problems of recording digital traces
in judicial practice: ways of improvement 85

CYBERCRIME IN AREAS OF ARMED CONFLICT (THE CASE
OF UKRAINE): VICTIMIZATION FACTORS AND PREVENTION
STRATEGIES (Dumchikov M. O., Yanishevska K. D., Murach D. V.) 92
1. Ontogenesis and Pathogenesis of Cybercrime
in Ukrainian National Law 93
2. War as a Factor of Cybercrime Victimization 103
3. Cybercrime Prevention Strategies in Wartime
(Based on the Experience of Ukraine) 110

ON DETECTIVE (INVESTIGATIVE) ACTIVITY IN MILITARY
CRIMINALISTICS (NATIONAL AND INTERNATIONAL
DIMENSIONS) (Kaliuga K. V.) 128
1. General Characteristics of Detective Activity in Military Criminalistics 130
2. The System of Subjects of Detective Activity
in War Crimes Investigations 131
3. Identification of the Perpetrator and Documentation
of Command Responsibility 133
4. Analytical Detective Activity and Forensic Modeling 134
5. The Use of OSINT and Digital Evidence in War Crimes Investigations 136
6. Specific Features of Detective Activity
in Temporarily Occupied Territories 138
7. International Cooperation in Detective Activity 140
8. Challenges and Prospects for the Development of Detective Activity 142

CRIMINAL PROCEDURAL AND FORENSIC ASPECTS
OF PROVING HATE SPEECH IN THE DIGITAL ENVIRONMENT
(Koval A. A., Kazarian E. H.) 149
1. Theoretical and Legal Foundations for Countering Hate Speech 150
2. Specific Features of Proving Hate Speech in the Digital Environment 156

FORENSIC TOOLS FOR OBTAINING EVIDENTIARY INFORMATION IN CRIMINAL INVESTIGATIONS IN THE DIGITAL ERA (Kurman O. V.) 166
1. Artificial intelligence in the analysis of digital traces: innovative perspectives and challenges of application 167
2. Digital traces of mobile communication devices in criminalistic practice ... 175

MODERN CHALLENGES OF CRIMINAL LAW REGULATION OF CYBERCRIME: NATIONAL AND INTERNATIONAL DIMENSIONS (Larchenko M. O.) 186
1. The problem's prerequisites emergence and the problem's formulation 186
2. Law enforcement issues regarding cyberattacks on critical infrastructure 188
3. Liability for the distribution of malicious software 192
4. Current cases of international cooperation in the fight against cybercrime 194

OSINT TECHNOLOGIES IN LAW ENFORCEMENT: INNOVATIONS AND AREAS OF APPLICATION DURING MARTIAL LAW AND THE COUNTRY'S POST-WAR RECOVERY (Nehrebetskyi V.V.) 201
1. Challenges of Regulating the Use of Digital Evidence Technologies During Wartime 202
2. Using Digital Technologies and Open-Source Data in Investigating War Crimes 206
3. Ensuring Authenticity and Admissibility of Digital Open-Source Evidence in Criminal Justice 212

ELECTRONIC EVIDENCE IN CIVIL PROCEEDINGS: CONCEPTUAL FOUNDATIONS AND PROCEDURAL REQUIREMENTS (Perunova O. M.) 220
1. The Concept of Electronic Evidence in Civil Proceedings 221
2. Requirements and the Special Significance of Electronic in Civil Proceedings 226

THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME AS THE BASIS FOR CRIMINAL LAW PROTECTION OF PUBLIC RELATIONS IN CYBERSPACE IN UKRAINE (Politova A. S.) 239
1. The Concept of Electronic Evidence in Civil Proceedings 240
2. Cybercrime: concept and types of criminal offenses 244
3. Implementation of the provisions of the Council of Europe Convention on Cybercrime in the Criminal Code of Ukraine 249

COUNTERING CYBERCRIME: USING ELECTRONIC EVIDENCE
IN THE INVESTIGATION PROCESS (Ryashko O. V.) 262
1. The role and place of electronic evidence
in cybercrime investigations 263
2. Typical investigative situations and characteristics
of a cybercriminal 268

INTERNATIONAL MECHANISM FOR COMBATING
CYBERCRIME (Syroid T. L.) 275
1. International Legal Framework for Combating Cybercrime 276
2. International Institutional Framework for Combating Cybercrime 286

CONSTITUTIONAL AND LEGAL GUARANTEES OF MEDIA
FREEDOM AND JOURNALISTIC ACTIVITY IN THE DIGITAL
ENVIRONMENT: THE PRACTICE OF THE ECTHR IN THE CONTEXT
OF CYBER OFFENCES (Slinko T. M., Slinko K. M.) 296
1. Media Freedom as a Fundamental Value of Constitutionalism
in the Conditions of the Digital Society 297
2. Constitutional and Legal Foundations for Guaranteeing
Freedom of Speech and Media Activity in Ukraine 303
3. Case Law of the European Court of Human Rights on Media Freedom
and Journalistic Activity in the Digital Environment 313

INSTITUTIONALIZATION OF THE NATIONAL CYBERSECURITY
SYSTEM: LEGAL STATUS AND POWERS OF THE SECURITY
AND DEFENSE SECTOR ACTORS (Spivak M. V., Dubina O. M.) 322
1. Cybersecurity as a multifaceted phenomenon:
diverse approaches to definition and protection measures 323
2. Legislative regulation of cybersecurity in Ukraine:
analysis of implementation and strategic directions 326
3. Classification and mechanisms of cyber incident management:
synergy of scientific approaches and state standards 330
4. Interaction of cybersecurity stakeholders in digital evidence
collection and cyber incident neutralization:
empirical analysis of law enforcement activities 334

SOME PROBLEMS OF DIGITAL INFORMATION
AND THE RELIABILITY, ADMISSIBILITY OF DIGITAL EVIDENCE
(Stratonov V. M., Basysta I. V., Hutnyk A.) 343
1. Information or evidence? Electronic, digital, electronic-digital? 344
2. Reliability and admissibility, how to achieve? 347
3. Verification and confirmation of the reliability of digital information 350

DIGITAL CRIMINALISTICS AS A STRATEGIC DIRECTION
FOR THE DEVELOPMENT OF MODERN CRIMINALISTICS
(Shevchuk V. M., Zatenatskyi D. V., Kolesnikova I. A.) 361
1. Digital transformation of criminalistics – a scientific prerequisite and
methodological basis for the formation of new criminalistic knowledge 362
2. Digital criminalistics: concepts and significance in the formation
of evidentiary information in the conditions of hybrid warfare..... 367
3. The role of digital criminalistics tools in the detection, recording
and investigation of war crimes in Ukraine 372

DIGITAL EVIDENCE IN COUNTERING CYBERCRIME:
LEGAL, TECHNICAL, AND FORENSIC ASPECTS
(Homon V. O., Miroshnyk R. O., Khivrenko D. V.) 384
1. Digital evidence as an interdisciplinary legal category..... 385
2. Cybercrime and the specifics of its proof..... 386
3. Blockchain analyzers and artificial intelligence
in forensic cryptocurrency investigations..... 387
4. Procedural and methodological aspects of handling digital evidence..... 389
5. Prospects for development 391

DOI https://doi.org/10.30525/978-9934-26-686-7-1

THE CONSTITUTIONAL BOUNDARIES OF DIGITAL EVIDENCE: INTRUSIVE MEASURES, CYBERSECURITY AND NATIONAL SECURITY IN ROMANIA

Safta, M., Stanciu, C. A. M.

INTRODUCTION. THEORETICAL FRAMEWORK

In any legal system, evidence constitutes the cornerstone of the administration of justice. The establishment of truth represents the ultimate objective of jurisdictional proceedings, while the legitimacy of judicial decisions depends directly upon the legality and integrity of the methods employed in its ascertainment. From this perspective, evidentiary matters cannot be reduced merely to their effectiveness in proving factual circumstances; rather, they inherently engage considerations relating to the protection of fundamental rights and freedoms. Within a state governed by the rule of law, judicial truth cannot be pursued at any cost. Accordingly, evidentiary mechanisms must remain strictly subject to the principles of legality, necessity, and proportionality.

The rapid development of information and communication technologies has profoundly reshaped the law of evidence, positioning digital evidence at the core of contemporary procedural systems. As social and economic interactions increasingly unfold in digital environments, they inevitably leave behind informational traces– such as traffic, location, identification, and content data–that may be collected and processed by public authorities. This expanded technological capacity significantly enhances the state's ability to access intimate aspects of individual life, thereby requiring a careful constitutional reassessment of the limits of public intervention.

Within the framework of criminal proceedings, this issue finds its most profound expression through technical surveillance measures, which represent some of the most intrusive instruments available to criminal investigation bodies. The interception of communications, access to traffic and location data, or the use of technical infrastructure to collect information involve direct interferences with the right to intimate, family, and private life and the secrecy of correspondence, guaranteed by the Romanian Constitution under Article 26 and Article 28. The expansion of the state's technological capabilities thus generates a structural tension between the necessity of combating crime–including cybercrime–and the constitutional obligation to protect the substance of fundamental rights.

Beyond the sphere of criminal proceedings, however, the issue of digital evidence and technical surveillance transcends the strictly judicial framework, fitting into a broader dimension–that of cybersecurity and, implicitly, national security. In the context of hybrid threats, cyberattacks, and the vulnerabilities of critical infrastructures, the collection and processing of data acquire a strategic dimension, transforming surveillance from a procedural tool into a mechanism for protecting the fundamental interests of the state. This functional expansion, however, raises

additional concerns regarding the delimitation of the authorities' competences and the constitutional standards applicable to interferences with fundamental rights.

Within this framework, the present research seeks to analyse–by capitalizing on the evolution and chronological development of the case law of the Constitutional Court of Romania (CCR)–three distinct yet interconnected dimensions of the issue: the general dimension of digital evidence, its application in criminal proceedings through technical surveillance measures, and, finally, its extension into the field of national security. The analysis will highlight the manner in which constitutional case law has progressively developed a coherent set of standards concerning the legality, foreseeability, necessity, and proportionality of interferences, in a judicial dialogue with the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). In accordance with the relevant constitutional provisions–namely Articles 20 and 148–the research will further consider the interpretation of fundamental rights in harmony with the international treaties Romania is a party to and in compliance with the principle of the primacy of European Union law.

Without claiming to provide an exhaustive analysis of an issue characterized by growing normative density and technological dynamism, the proposed analysis seeks to outline the constitutional landmarks of surveillance in the digital age and to highlight the contribution of Romanian case law to the configuration of a genuine digital constitutionalism, situated at the intersection of fundamental rights protection and security imperatives in a democratic society.

I. Data Retention and Structural Surveillance. Constitutional and European Standards

1. The Unconstitutionality of the National Transposition of Directive 2006/24/EC ("Big Brother")

Without providing extensive detail on this case law within the current framework, given its comprehensive presentation in other studies[1], we mention it as a landmark not only at the national level but also at the level of the European Union (EU). This includes its role in the dialogue between constitutional courts and the subsequent effects regarding the shaping of fundamental rights protection standards.

From the perspective of EU law, this moment was one of tension between Romania's obligation to comply with the European legal order (the transposition of a directive) and the obligation to adhere to the fundamental rights protection standards enshrined in the Romanian Constitution. This tension arose from the intrusive nature of the measures established by the European act in question, namely Directive 2006/24/EC (the so-called "Big Brother Directive")[2]. Essentially, it imposed a

[1] C. F. Stoica, M. Safta, '*Theoretical and practical issues relating to the right to the protection of personal data*' (2015) 5(2), Juridical Tribune – Review of Comparative and International Law 88–10, available at https://www.tribunajuridica.eu/arhiva/An5v2/6%20Stoica.pdf.

[2] Directive 2006/24/EC (Data Retention Directive).

general obligation on Member States to store traffic and location data held by telephone and internet service providers for a specified period, for the purpose of combating serious crime and terrorism. However, the manner in which this obligation was regulated faced critical positions, both publicly and in legal literature, where it was argued that it permitted generalized and undifferentiated surveillance, establishing what Stefano Rodotà named "total surveillance," which alters the balance of power between the state and the individual. In his view, the functioning of the rule of law is based on a clear rule: state power must be transparent, while the individual's life must be opaque[3]–more precisely, the requirements of the right to privacy must be respected. The same thesis is developed in legal doctrine by Orla Lynskey, who states that generalized data retention policies undermine the foundation of liberal democracy, transforming citizens into subjects of constant monitoring[4]. The issue of undifferentiated data collection lies in the creation of an informational asymmetry between the state and the citizen. In the absence of robust safeguards, the state's control capacity is liable to exceed the requirements of the proportionality test. Lynskey emphasizes that data protection is more than an individual right, being a structural component of the rule of law.

The Directive in question was transposed in Romania through Law No 298/2008[5], which was challenged before the CCR and found unconstitutional by Decision No1.258/2009[6]. While the Constitutional Court acknowledged, in principle, "*the legislator's possibility to limit the exercise of certain fundamental rights and freedoms, as well as the necessity of regulating measures that provide law enforcement authorities with specific duties in criminal investigation with efficient and adequate instruments for preventing and uncovering terrorism-related crimes, in particular, as well as serious crimes*", it emphasized the imperative of respecting "*all the safeguards that such an interference requires*." Subsequently, the Romanian legislator adopted Law No 82/2012[7], attempting to remedy the identified unconstitutionality flaws and to establish new standards for the protection of personal data. However, this law was also found unconstitutional by Decision No 440/2014[8], which reaffirmed the necessity of real, not illusory, safeguards for the fundamental rights affected by the transposition of the directive. We shall briefly highlight below these safeguards as they emerge from the aforementioned decisions.

[3] S. Rodotà, *Technopolitics. Democracy and the New Communication Technologies*, 2nd Edition, Laterza Publishing, Rome-Bari, 2004, pp. 3–15.

[4] O. Lynskey, The Foundations of EU Data Protection Law, Oxford University Press, Oxford, 2015, pp. 175-180.

[5] Official Gazette no. 780 of 21 November 2008.

[6] Official Gazette no. 798 of 23 November 2009.

[7] Official Gazette no. 211 of 25 March 2014.

[8] Official Gazette no. 883 of 9 November 2014.

2. Constitutional Safeguards Governing Data Retention and Access

2.1. Quality of Law

The Court emphasized that the limitation of the exercise of fundamental rights (in this case, the right to intimate life, the secrecy of correspondence, and the freedom of expression) must occur in a clear, predictable, and unequivocal manner, so as to eliminate, as far as possible, the possibility of arbitrariness or abuse by the authorities in this field. However, "*the lack of precise legal regulation, which would exactly determine the scope of those data necessary for identifying natural or legal persons who are users, opens the possibility for abuses in the retention, processing, and use of data stored by providers of publicly available electronic communications services or public communications networks*". In the same logic, the Court held that the legislator does not define what is meant by "*threats to national security*"; thus, in the absence of precise delimitation criteria, various ordinary, routine actions, information, or activities of natural and legal persons can be arbitrarily and abusively assessed as being of the nature of such threats. Consequently, "*the subjects of the law may be included in the category of suspected persons without knowing this and without being able to prevent, through their conduct, the consequence of applying the rigors of the law*".

With reference to the same constitutional requirements, the Court sanctioned the ambiguous terminology, noting, *inter alia*, that Article 1 (2) of the law extended the retention obligation to "*related data necessary for identifying the subscriber*", without, however, providing a legal definition of this concept. In the absence of an explanation of what the legislator understands by "*related data*", the legal provision failed to establish with precision the scope of information subject to storage.

2.2. The State's Negative Obligation to Refrain from Interference with the Exercise of Rights or Freedoms

The Court found that the law established an obligation for providers of publicly available electronic communications services or public communications networks to retain data continuously for a period of 6 months from the moment of interception, thereby depriving the principle of personal data protection and confidentiality of its substance (enshrined at the legislative level by Law No 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as well as Law No 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector). The excessive nature of these limitations was further highlighted by invoking the provisions of Article 91^1 of the Code of Criminal Procedure, regarding which the Court held that it "*respects the exceptional nature of audio or video interceptions and recordings, as these are allowed under certain strict conditions, from the moment of obtaining a reasoned authorization from a judge, for a limited period of time which cannot exceed, in total, for the same person and the same act, 120 days*". The Court concluded that the regulation of a positive obligation concerning the continuous limitation of the exercise of the right to intimate life and the secrecy of correspondence "*causes the very essence of the right to disappear, by removing the safeguards regarding its exercise*".

2.3. Proportionality of the Interference

2.3.1. The Unconstitutionality of General and Continuous Data Retention

In essence, the Court emphasized that it is not the justified use, under the conditions regulated by Law No 298/2008, that in itself unacceptably prejudices the exercise of the right to intimate life or the freedom of expression, but rather the continuous, generally applicable legal obligation to store data–thus, an interference lacking proportionality. Storage affects the subjects of the law "*regardless of whether or not they have committed criminal acts or whether or not they are the subject of criminal investigations, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communications services or public communications networks into persons suspected of committing terrorism-related or serious crimes*".

2.3.2. Sanctioning the Absence of Effective Judicial Oversight of Access to Retained Data

While Decision No 1.258/2009 primarily examined the bulk collection of data, Decision No 440/2014[9]–which sanctioned a new attempt to transpose the same aforementioned Directive–focused particularly on the access to the collected information. The Court found that "*requests for access to retained data for the purpose of their use as provided by law, formulated by state authorities with duties in the field of national security, are not subject to authorization or approval by a court of law, thus lacking the guarantee of effective protection of the stored data against the risks of abuse as well as against any illicit access and use of such data. This circumstance is likely to constitute an interference with the fundamental rights to intimate, family, and private life and the secrecy of correspondence and, therefore, infringes the constitutional provisions that enshrine and protect these rights*".

The need for such review was reasoned by pointing out that in the case of retention and storage of electronic information, the interference with the fundamental rights regarding intimate, family, and private life, the secrecy of correspondence, and the freedom of expression is extensive and must be regarded as being particularly serious. Furthermore, the circumstance that the retention of data and their subsequent use are carried out without the subscriber or registered user being informed thereof is likely to generate for the persons concerned the feeling that their private life is the subject of constant surveillance. Likewise, the Court emphasized that the information which can be retained or stored by providers of electronic communications networks or services, although predominantly technical in nature, is likely to provide relevant information regarding the individual and their private life. These data aim at identifying subscribers or customers, namely the user and the recipient of information communicated electronically, the source, destination, date, time, and duration of a communication, the type of communication, the communication equipment or devices used by the user, the location of mobile communications equipment, the payment methods used by users, as well as the history of access logs with the corresponding timestamps for an IP address. Such data are likely to affect the free

[9] Official Gazette no. 653 of 4 September 2014.

exercise of the right to correspondence or freedom of expression, as well as the person's intimate, family, and private life; "*specifically, the data in question allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, conclusions which may concern daily habits, permanent or temporary places of residence, daily or other movements, activities carried out, personal interests, social relationships of those persons and the social environments attended by them*"[10].

Using the same reasoning, the Court held the lack of an effective control mechanism over the activity of communications providers–namely, the entities that actually stored the data. Although the law appointed supervisory authorities, it did not provide them with the necessary levers to effectively verify whether operators complied with security standards, making it impossible to carry out an actual verification of the manner in which data were stored, protected, or destroyed; furthermore, no transparent information was provided regarding the institutions permitted to access these data[11]. Additionally, the majority of the established violations were sanctioned with an administrative fine rather than a criminal one, leaving the citizen vulnerable to the risks of potential abuses. At the same time, the law only defined as a criminal offense the intentional access, alteration, or transfer of retained data without authorization, while all other illicit acts were considered administrative offenses[12]. According to the Court, the failure to regulate a real control mechanism over electronic communications service providers was tantamount to a lack of safeguards.

Moreover, at the time the Decision No 440/2014 was issued, the Court of Justice of the European Union (CJEU) had already invalidated Directive 2006/24/EC through its Judgment of 8 April 2014; consequently, the Constitutional Court of Romania (CCR) found Law No 82/2012–which transposed the Directive as unconstitutional. Simultaneously, the Court found that the activities of retaining and using data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks "*become devoid of legal basis, both from the perspective of European and national law*"[13].

2.4. Lack of Adequate Safeguards for the Protection of Fundamental Rights. "Undermining or Destroying Democracy on the Ground of Defending It"[14]

The aforementioned decisions of the Constitutional Court also established the infringements upon the exercise of the right to freedom of movement, the right to intimate, private, and family life, and the interference with the secrecy of correspondence and freedom of expression caused by Law No 298/2008. Referring to the case-law of the ECtHR in Case *Klass and Others v. Germany*[15] (1978) or

[10] Decision no. 440/2014, para. 56.
[11] Ibidem, para. 68.
[12] Ibidem.
[13] Ibidem., para. 78.
[14] ECtHR Judgment of 6 September 1978, *Klass and Others v. Germany*, Application no. 5029/71, para. 49.
[15] Ibidem

Dumitru Popescu v. Romania[16] (2007), the Court established, through Decision No 1.258/2009, that interferences with private life can only be justified by the existence of robust legal safeguards, aimed at ensuring effective protection against the risk of abuse by state authorities. In accordance with the principles enshrined in *Klass* Case, the Court found that the adoption of surveillance measures, in the absence of adequate and sufficient safeguards, risks leading to the very destruction of democracy under the alleged reason of defending it.

2.5. European Jurisprudential Coherence on Electronic Communications Surveillance

With reference to the aforementioned sequence of decisions and the interference of EU law, it should be noted that other Constitutional Courts have also sanctioned, using similar reasoning, the transposition of the directive, and that it was ultimately invalidated by the CJEU in the joined cases *Digital Rights Ireland* (C-293/12) and *Seitlinger and Others* (C-594/12). Among the arguments upheld by the Court was the fact that no distinction was made between the categories of collected data based on their potential usefulness in achieving the pursued objective or based on the persons concerned. Directive 2006/24/EC did not provide clear and precise rules governing the scope of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Furthermore, the imposition of a storage period of at least six months and a maximum of 24 months, without specifying that the determination of the retention duration must be based on objective criteria to guarantee its limitation to what is strictly necessary, contravened constitutional standards[17].

The approach of constitutional judges–whether referring to national constitutional courts or the CJEU–was based on a common objective: ensuring the highest possible standard of protection for human rights in the context of electronic communications surveillance. This remains in recent constitutional history as a valuable endeavor to defend constitutional values against technology and the risks involved in its improperly controlled use. Regarding the actual judicial relations between the courts, there have also been criticisms raising from the fact that the CCR did not address the CJEU with a preliminary ruling request in that context. In this regard, we share the opinion that the dialogue between judges in the EU must be strengthened and the preliminary ruling mechanism utilized to its full potential[18].

[16] ECtHR, Judgment of 26 April 2007, *Dumitru Popescu v. Romania (no. 2)*, Application no. 71525/01.

[17] CJEU, Judgment of 8 April 2014, *Digital Rights Ireland Ltd*, joined cases C-293/12 and C-594/12, EU:C:2014:238, paras. 63-65.

[18] Ibidem.

II. Technical Surveillance in Criminal Proceedings: Constitutional Limits and Safeguards

1. The Legality of Technical Surveillance Measures[19] – Criteria and Remedies

Over time, a rich case-law of the CCR has emerged in response to criticisms brought against the provisions of Chapter IV, marginally titled "Special Surveillance Methods[20]", under Title IV, "Evidence, Means of Evidence, and Evidentiary Procedures", of the Code of Criminal Procedure. In its rulings, relying on the landmark case law of the ECtHR, the Court has specified and described the criteria for assessing the legality of surveillance measures, as well as the remedies that the law must provide to persons against whom technical surveillance measures have been ordered. Thus, the CCR held that, in analyzing compliance with the safeguards for the right to private life provided by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, the ECtHR considers–besides the aspects regarding the definition of categories of persons subject to technical surveillance–the nature of the offenses (types of offenses), the duration of the measure's execution, the authorization procedure, the conditions for drafting the summary report of intercepted conversations (transcription procedures), the precautions taken to communicate intact and complete recordings for judicial review, and aspects concerning the circumstances under which such interceptions can or must be destroyed (referring, for example, to the Judgment of 24 April 1990, *Huvig v. France*, paragraph 34; the Judgment of 18 February 2003, *Prado Bugallo v. Spain*, paragraph 30; the Judgment of 4 December 2015, *Roman Zakharov v. Russia*, paragraph 231).

At the same time, the CCR has contributed to "*shaping*" the incident regulatory framework by delivering rulings that eliminated a series of unconstitutionality flaws. As will be seen in the following analysis, these rulings applied the standards already defined in the "*Big Brother*" case law, thus marking a jurisprudential continuity within the specific field of criminal procedure regulation.

2. Legislative Precision in Defining Competent Authorities Empowered to Execute Technical Surveillance Warrants

2.1. The Separation of Criminal Investigation and Intelligence Functions in the Execution of Technical Surveillance Warrants

Applying the standard of quality of law extensively developed in its case law–which involves rigorous requirements in criminal matters–the CCR sanctioned the criminal procedure provisions that established, in a vague and imprecise manner, the

[19] See also Gianina-Anemona Radu, 'Theoretical and Practical Aspects Regarding Technical Surveillance in the Criminal Trial' (2023) *Valahia University Law Study* SI 216–223 https://www.ceeol.com/search/article-detail?id=1353109

[20] For references see Mihail Udroiu, 'A posteriori control of the legality of technical surveillance in Romanian criminal proceedings' (Studia Universitatis Babeș-Bolyai Iurisprudentia, Vol 68 No 2, 23 Dec 2023) https://doi.org/10.24193/SUBBiur.68(2023).2.6

category of authorities competent to enforce technical surveillance warrants, thereby allowing their execution by authorities not expressly specified by law.

Having been called upon to rule on the provisions of Article 142 (1) of the Code of Criminal Procedure, according to which "*The prosecutor shall execute the technical surveillance or may order it to be carried out by the criminal investigation body or by specialized workers within the police or by other specialized state bodies*", the CCR found that the phrase "*or by other specialized state bodies*" is unconstitutional[21].

In the reasoning of its decision, the Court emphasized the inherently intrusive nature of technical surveillance measures, underscoring the necessity of a clear, precise, and foreseeable legal framework. Such regulation must provide sufficient safeguards not only for the individual subject to the measure, but also clear guidance for prosecutorial authorities and courts, thereby ensuring protection against arbitrary or abusive implementation and against unjustified interference with fundamental rights, including the right to private and family life and the confidentiality of communications. However, through the aforementioned general phrasing, the legislator included within Article 142 (1) of the Code of Criminal Procedure, in addition to the prosecutor, the criminal investigation body, and specialized workers within the police, other specialized state bodies, such as the Romanian Intelligence Service (SRI) referenced by the authors of the exception, other services with duties in the field of national security, or specialized state bodies with duties in various fields, such as the National Environmental Guard, the Forest Guards, the National Authority for Consumer Protection, the State Inspectorate in Construction, the Competition Council, or the Financial Supervisory Authority, none of which possess criminal investigation powers. According to the CCR, "*the legislator's option for the technical surveillance warrant to be executed by the prosecutor and the criminal investigation bodies, which are judicial bodies according to Article 30 of the Code of Criminal Procedure, as well as by specialized workers within the police–insofar as they may hold the certification of judicial police officers under Article 55 (5) of the Code of Criminal Procedure–is justified",* but *not that of other bodies whose scope is not specified*. With reference to the opinions regarding the involvement of the SRI in criminal investigations–a flashpoint of both legal and public debate–the opinions of the Venice Commission[22] are noteworthy, as is the distinction made in legal literature[23] between intelligence gathering for national security and criminal prosecution activities. Intelligence agencies have specific duties and different operational rules, which do not overlap with the procedural safeguards of the criminal process. By allowing their involvement in the execution of common law technical surveillance warrants without establishing a clear legal framework, the citizen has no guarantee that the digital evidence against them was obtained by a legally authorized body.

[21] Decision no. 51/2016, Official Gazette, Part I, no. 190 of 14 March 2016, para. 20.

[22] See Venice Commission, *Report on the Democratic Oversight of the Security Services* (CDL-AD(2007)016), Strasbourg, 11 June 2007, para. 199 et seq.

[23] Popa, A.-N., *CCR Case-law regarding the notion of "national security"*, published on Juridice.ro on 10.02.2020.

In addition to the constant reference to ECtHR standards, it is interesting to note the manner in which the Court correlates the national regulatory framework with that of the EU, by specifically referring to provisions of the codes of criminal procedure from other states; regarding these, it notes that "*when regulating technical surveillance activities and their execution, they do so through clear and predictable rules and target only judicial bodies. In this sense, national codes of criminal procedure expressly provide that technical surveillance activities are carried out by the investigating judge, prosecution bodies, and police bodies, and that, from a technical standpoint, legal entities in the field of telecommunications services or other fields expressly and limitedly provided for by the law of criminal procedure are obliged to collaborate, if necessary, in their implementation*"[24]. From this perspective, it can be stated that this decision also finds its place within the space of jurisdictional dialogue that contributes to the strengthening of the European architecture for the protection of fundamental rights.

2.2. Remedies in Case of Breach of Competence by Prosecution Bodies

In this context, given its importance from the perspective of remedies for the violation of fundamental rights (including within the complex context of technical surveillance), we mention Decision No 302/2017[25]. Through this ruling, the CCR found that the legislative solution contained in the provisions of Article 281 (1) letter b) of the Code of Criminal Procedure–which does not include the breach of provisions regarding the material competence and personal competence (*ratione personae*) of the prosecution body within the category of absolute nullities–is unconstitutional. In essence, the CCR held that proving an injury to a person's rights solely through the prosecution body's failure to comply with provisions regarding subject-matter or personal competence "*turns into a proof difficult to achieve by the interested party, which amounts, in fact, to a genuine probatio diabolica, and implicitly leads to a violation of the fundamental right to a fair trial*". It is therefore required that, in this situation, the procedural injury to be presumed *juris et de jure*.

The logical link between Decision No 51/2016 and Decision No 302/2017 regarding remedies is expressly mentioned in the subsequent case law of the CCR, to which we shall briefly refer in the following section[26].

3. Technical Surveillance Activities. The Unconstitutionality of Granting the Status of Special Criminal Investigation Body to the Romanian Intelligence Service (SRI)

Following the delivery of Decision No 51/2016, Government Emergency Ordinance no. 6/2016 was adopted, aiming to align the provisions of the Code of Criminal Procedure with this CCR decision. Thus, the phrase found unconstitutional was removed from the provisions of Article 142 (1) of the Code of Criminal Procedure. Furthermore, Article 57 (2) of the Code of Criminal Procedure was amended to specify that "*special criminal investigation bodies may, in the case of*

[24] Decision no. 51/2016, para. 36.
[25] Official Gazette no. 566 of 17 July 2017.
[26] Official Gazette no. 193 of 12 March 2019.

offenses against national security provided for in Title X of the Criminal Code and terrorism offenses, upon the prosecutor's order, implement technical surveillance warrants" *(Article I point 1)*. Additionally, Article 13 of Law No 14/1992 on the organization and functioning of the SRI was amended to state that "*SRI bodies cannot perform criminal investigation acts, cannot take the measure of detention or preventive arrest, nor have their own arrest facilities. By way of exception, SRI bodies may be designated as special criminal investigation bodies according to Article 55 (5) and (6) of the Code of Criminal Procedure for the execution of technical surveillance warrants, in accordance with the provisions of Article 57 (2) final thesis of the Code of Criminal Procedure*" *(Article IV point 2)*. Through the same normative act, the role of the National Center for Communications Interception (CNIC) within the Romanian Intelligence Service (SRI) was established as a mandatory infrastructure for prosecution bodies in order to conduct technical surveillance activities[27].

Reiterating the reasoning that grounded its case-law in this matter and placing its analysis within a broad framework of European law, the CCR found that granting the status of special criminal investigation body to the SRI violates the constitutional provisions. The Court noted, *inter alia*, the aspects highlighted by the European Union Agency for Fundamental Rights, according to which "*an organizational separation between secret services and law enforcement authorities is usually considered a safeguard against the concentration of powers in a single service and the risk of arbitrary use of information obtained in secret*"[28].

Regarding the aforementioned technical structure, the Court held that the provisions concerning the execution of technical surveillance warrants through the C.N.I.C. are norms adopted to regulate a transitional situation in the period immediately following the publication of Decision No 51 of 16 February 2016, with the aim of adopting a precise regulation in the field that complies with constitutional requirements. Although six years have passed since the adoption of Government Emergency Ordinance no. 6/2016, the legislator, through its approval law, limited itself to approving the "*emergency solution*" without regulating a procedure compliant with constitutional norms, and established the C.N.I.C. as the sole entity executing both the authorization acts issued under Article 13 of Law No 51/1991 on Romania's national security and the technical surveillance warrants issued according to the Code of Criminal Procedure. The Court sanctioned this regulation, holding that regarding the execution of technical surveillance warrants issued under the Code of Criminal Procedure, it is not sufficient to indicate the name of a structure, entity, institution, or body that does not benefit from regulation at the level of law; "*although, according to Article 285 (2) of the Code of Criminal Procedure, the procedure during the criminal investigation is non-public, this does not mean the procedure is secret, but only that in this phase of the criminal process, the publicity specific to the trial phase does not exist*"[29].

[27] According to Art. 4 of Government Emergency Ordinance no. 6 of 11 March 2016 on certain measures for the execution of technical surveillance warrants ordered in criminal proceedings, published in the Official Gazette, Part I, no. 190 of 14 March 2016.

[28] Decision no. 55/2022, para. 155.

[29] Ibidem., para. 204.

The CCR case law, consistent with the dynamics of legislative amendments that essentially enshrined the same normative solution, responded to criticisms, also present in legal literature[30], according to which the mere reconfiguration of the SRI as a technical body does not change its nature as an intelligence service–militarized and subordinated to the executive–which is structurally incompatible with the safeguards of judicial independence. Regarding the field analyzed herein, that of digital evidence, the cited case law is particularly relevant from the perspective of the principle that control over the technical infrastructure determines the validity of the evidence. The dependence on the SRI's technical infrastructure turned judicial bodies into mere passive beneficiaries of data whose integrity was impossible to verify, in violation of the safeguards of the right to a fair trial. In the context of technological developments and the remodeling of evidence in criminal proceedings, it is essential that the modernization of the means of evidence–namely the introduction of digital evidence in building the prosecution's case–be achieved without compromising the independence of criminal investigation bodies and fundamental rights.

4. Convergence of European and National Jurisprudence on Data Protection and Technical Surveillance. Sanctioning the Cooperation Protocols between the Public Ministry and the SRI

As in the *Big Brother* precedent, the CCR case law regarding the execution of technical surveillance warrants correlates with the relevant CJEU case law. In the joined cases *Tele2 Sverige AB and Watson*[31], the CJEU emphasized that national legislation must provide objective criteria establishing a connection between the collected data and the pursued goal[32]. Reiterating the reasoning used in the *Digital Rights Ireland* case[33], the Court held that the continuous and undiscriminated use of communication storage and interception mechanisms is liable "*to generate in the minds of the persons concerned the feeling that their private life is the subject of constant surveillance*"[34]. Furthermore, generalized surveillance is incompatible with the foundations of a democratic society, affecting the very essence of freedom of expression. This same interpretation was reconfirmed by the CJEU several years later in the *VD and SR* judgment (Joined Cases C-339/20 and C-397/20)[35], where the Court established that not even the combating of economic offenses, such as market abuse, can justify the generalized storage of personal data[36]. The Court ruled that

[30] Cristescu, D. I., *Vademecum on the investigation of illicit manifestations against national security (III)*, published on Juridice.ro on December 8, 2023.

[31] CJEU, Grand Chamber, Judgment of 21 December 2016 delivered in joined cases C-203/15 *Tele2 Sverige AB v. Post- och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v. Tom Watson and Others*, ECLI:EU:C:2016:970.

[32] Ibidem, para. 110.

[33] CJEU, Grand Chamber, Judgment of 8 April 2014 in joined cases C-293/12 *Digital Rights Ireland Ltd* and C-594/12 *Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238, para. 37.

[34] CJEU, Judgment in *Tele2 Sverige and Watson* (C-203/15 and C-698/15), para. 100.

[35] CJEU, Judgment of 20 September 2022, *VD and SR*, Joined Cases C-339/20 and C-397/20, EU:C:2022:703.

[36] French legislation provided for "on a preventive basis, the generalized and undifferentiated retention of traffic data by electronic communications service providers for one

national courts may not maintain, on a provisional basis, the effects of a non-compliant law for the purpose of saving digital evidence in ongoing criminal cases. Information and evidence obtained as a result of generalized surveillance must be excluded[37]–a point on which we also note the CCR case law, which ruled to the same effect, this time within the framework of a legal dispute of a constitutional nature.

Thus, through Decision No 26/2019[38] on the request for the settlement of the legal dispute of a constitutional nature between the Romanian Parliament, on the one hand, and the Public Ministry–the Prosecutor's Office attached to the High Court of Cassation and Justice, the High Court of Cassation and Justice, and the other courts of law, on the other hand, the CCR essentially established the obligation of the High Court of Cassation and Justice and the other courts, as well as the Public Ministry–the Prosecutor's Office attached to the High Court of Cassation and Justice and its subordinate units–to verify, in pending cases, the extent to which a breach of the provisions regarding the competence *ratione materiae* and *ratione personae* of the prosecution body occurred through the conclusion of Protocols between the Public Ministry and the SRI, and to order the appropriate legal measures.

The aforementioned sequence of decisions marks a landmark moment in the evolution of the regulatory framework amidst the challenges posed by the technical complexity of digital evidence, such as the lack of adequate technical infrastructure highlighted even in the public communication of the Public Ministry at that time[39]. Although the primary focus of national and European debates was the involvement of intelligence services in the judiciary, our intention is to emphasize the complexity of the technical management of digital evidence and the rigorous requirements for the protection of fundamental rights in an increasingly technology-driven environment. Indeed, these aspects are also noted in EU rule of law evaluation documents, which consistently mention the need for a predictable legislative framework that guarantees effective judicial review[40].

III. Cybersecurity and Structural Preventive Surveillance

Technological development and risks to national security have led to the adoption of laws aimed at addressing new regulatory needs. In this regard as well, Romania's legislation has followed a sinuous path, in which the CCR's intervention has constituted a significant shaping factor.

---

year from the date of recording, with a view to combating market abuse offenses, including the unlawful use of inside information." – Court of Justice of the European Union (Research and Documentation Directorate), *Thematic Factsheet – Personal Data Protection*, July 2024, available at , pp. 53-57.

[37] Ibidem, p. 57.

[38] Official Gazette no. 193 of 12 March 2019.

[39] See National Anticorruption Directorate Press Release no. 252/VIII/3 of 9 March 2016, requesting the Ministry of Justice to increase the number of positions and the institution's budget to ensure the technical infrastructure necessary for the execution of surveillance warrants, available online at: https://www.dna.ro/faces/comunicat.xhtml?id=7206.

[40] See the Report from the Commission to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism (CVM) of 2017 and 2018, as well as the 2022 Rule of Law Report – Country Chapter on the rule of law situation in Romania, Luxembourg, 13.7.2022, SWD(2022) 523 final.

Thus, in 2015, the Cybersecurity Law was found unconstitutional in its entirety, primarily due to its unclear and imprecise manner of regulation[41], namely because it regulated its scope of application in a very general way, without distinguishing between the categories of persons who own, organize, administer, or use computer networks and systems. Beyond the technical aspects and the issues specific to the regulation of cyber infrastructure and the authorities with competence in the field, the Court also sanctioned the absence of any provision within the law ensuring the possibility for a person–whose rights, freedoms, or legitimate interests were affected by acts or deeds based on the provisions of the Cybersecurity Law of Romania–to appeal to an independent and impartial court of law. The Court held that this omission fails to comply with the provisions of Article 1 (3) and (5), Article 21 of the Constitution, as well as Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Subsequently, however, the legislator incorporated the requirements established by the Court, so that a new Cybersecurity Law passed the constitutionality test and is currently in force. Through Decision No 70/2023[42], the CCR held that the adopted law is clear; regarding the specific component of data retention and use, it assessed that the mechanisms for notifying cybersecurity incidents and those for communicating cybersecurity risks, threats, and vulnerabilities ensure, in each individual case, determined timeframes/intervals–spanning from the moment of incident notification to the communication of additional data and information regarding the said incident. These timeframes are established to allow any concerned legal subject the physical, technical, and operational capacity to transmit the information in question to the competent authorities. The Court provided further clarification regarding the reporting obligation established by law, specifying that not every cybersecurity incident is capable of triggering the reporting mechanisms provided for by the law. For instance, not every propaganda or disinformation campaign is envisioned by the legislator, but only those of extreme gravity that represent a threat to national security[43].

Regarding the criticism that including all computer networks and systems within the national security protection system–specifically within the cybersecurity sector of national security–violates the right to intimate, family, and private life, as well as the freedom of expression, the Court found that the analyzed legislative solution does not target computer networks and systems in their materiality. Instead, the object of national security interest consists of the negative effects produced by cyberattacks and threats, as well as hybrid threats in cyberspace that affect the state's resilience capacity, namely propaganda and disinformation campaigns in cyberspace that affect the constitutional order.

In the reasoning of its decision, the Court mandated the necessity of a balance between cybersecurity protection needs and individual rights, placing particular emphasis on the protection of the right to privacy. The Court's interpretation sought to establish a distinction between technical data, necessary for the analysis of the

[41] Decision no. 17/2015, Official Gazette no. 79 of 30 January 2015.
[42] Official Gazette no. 131 of 15 February 2023.
[43] Decision no. 70/2023, Official Gazette no. 211 of 14 March 2023, para. 143.

cybersecurity incident, and content data. The Court held that the challenged law clearly specified that the information requested from cybersecurity technical service providers does not target personal data or content data[44]. The Court emphasized that the law did not authorize access to the content of users' private communications. The reporting obligation provided for by the legal text was strictly limited to the technical elements necessary for identifying and counteracting cyber threats.

This case-law, and the manner in which it has guided the adoption of a law essential in the context of current technological developments and the complex risks to which societies are subjected, reveals a fundamental requirement of the rule of law: cybersecurity, even when subsumed under national security, cannot constitute a regulatory space exempted from the constitutional rigors of clarity, proportionality, and effective judicial review. The analyzed legislative evolution demonstrates that the Court's intervention played an essential shaping role in defining the constitutional limits of state interference in the digital sphere. While the first regulation was sanctioned for its general, imprecise nature and lack of effective safeguards, the new cybersecurity law was validated precisely to the extent that it integrated clear criteria for determining its scope of application, established predictable procedural mechanisms, and expressly excluded access to the content data of private communications. From the perspective of digital evidence, this case law is of particular importance. Cyberspace currently represents one of the primary sources of data liable to become means of evidence in criminal proceedings or other proceedings relevant to national security. Thus, the classification and delimitation of this data–between technical data and content data–acquires a constitutional value. The Court has imposed the principle that the analysis of security incidents may justify the processing of strictly necessary technical data, but it cannot fail into a generalized mechanism for surveillance or for the collection of communication content in the absence of the specific safeguards of criminal procedural law and judicial authorization.

CONCLUSIONS

The analysis conducted in the present study was intended to outline the constitutional limits of digital evidence by referring to three interdependent levels: the retention of and access to data resulting from electronic communications, the use of technical surveillance measures in criminal proceedings, and the expansion of data collection mechanisms in the fields of cybersecurity and national security. This structure reflects the profound transformation of evidentiary matters in the digital age and the necessity of reconfiguring the safeguards of the rule of law in the face of technological expansion.

As regards data retention and access, the case law of the Constitutional Court of Romania– established by Decision No 1.258/2009 and subsequently consolidated– marked a defining moment in the process of constitutionalizing the digital space. The Court rejected the logic of generalized and undifferentiated surveillance, reaffirming

[44] Article 21 (5) of Law No 58/2023 on the cybersecurity and cyber defense of Romania: "*The data and information provided for in para. (1) do not target, through the purpose of the request, personal data and content data*."

that the efficiency of combating crime or terrorism cannot justify the establishment of continuous and global data storage obligations. The imposed standards–the quality of the law, the clear definition of competences, time limitations, effective judicial review, and the proportionality of the interference–have shaped a protection framework that transcends the strict field of electronic communications and projects itself onto the entire architecture of digital evidence.

In the field of technical surveillance within criminal proceedings, the Court transferred and consolidated these standards, insisting on the necessity of legislative precision in defining the bodies empowered to execute warrants, on the clear demarcation between intelligence activities and criminal investigation activities, and on the existence of effective remedies in case of breach of legal competence. The case law regarding the involvement of intelligence services and the management of technical infrastructure highlights an essential thesis for the digital evidence regime: the legality and fairness of evidence do not depend exclusively on the formal authorization of the measure, but also on the institutional and technical framework in which it is executed. In this context, control over the infrastructure becomes an intrinsic component of the guarantees of a fair trial.

Regarding cybersecurity and national security, the analysis reveals a refinement of the constitutional approach. While in the matter of generalized retention the Court sanctioned the lack of adequate safeguards, in recent decisions it has upheld the constitutionality of regulations that differentiate between technical data and content data and that limit reporting obligations to serious and concrete threats. This evolution confirms that not every interference is, by its nature, incompatible with constitutional requirements, but only that which exceeds the limits of necessity and proportionality or which operates within an imprecise regulatory framework devoid of effective control.

Thus, the constitutional limits of digital evidence in the field of cybersecurity are structured around three essential coordinates:

a) The legality and predictability of the norm, in the sense of clearly defining the categories of targeted entities, the types of relevant incidents, and the nature of the data that may be requested;

b) The proportionality of the interference, by restricting reporting obligations to serious incidents capable of affecting national security, and by excluding access to content data;

c) Effective jurisdictional safeguards, allowing the person concerned to challenge any potential abusive measures and ensuring the control of an independent court over the interference with fundamental rights.

Viewed as a whole, the Romanian experience highlights a progressive process of constitutionalizing digital evidence, achieved through a continuous dialogue with the case law of the CJEU and the ECtHR. The convergence of European and national standards confirms the existence of a common matrix of digital constitutionalism, founded on the rejection of generalized surveillance, the supremacy of judicial review, and the protection of the essence of fundamental rights.

In accordance with the premises set forth in the introduction, the central conclusion of the study is that the legitimacy of digital evidence does not arise from the technological performance of the collection means, but from their integration into

a clear, predictable regulatory framework subject to genuine jurisdictional control. In a rule of law, technology cannot become a substitute for constitutional safeguards, nor an instrument for the discretionary exercise of power. Judicial truth remains inseparable from the legality of the means by which it is obtained.

Beyond constitutional adjudication and doctrinal debates, the practical implementation of online surveillance measures in Romania reveals additional structural challenges. Recent analyses from legal practice emphasize that the interception of electronic communications, access to traffic and subscriber data, and cooperation obligations imposed on service providers operate at the intersection between criminal procedural law, data protection law, and national security legislation. From a practical standpoint, online surveillance does not concern only traditional telecommunication operators, but increasingly digital platforms, internet service providers, and entities managing electronic communications infrastructure. This technological expansion intensifies the need for clear delimitation of competences, especially in relation to the authorization procedure, the execution of surveillance warrants, and the preservation and integrity of digital evidence. In the perspective of accelerated technological developments–artificial intelligence, algorithmic data analysis, the interconnection of information databases–the challenges regarding digital evidence will continue to test the capacity of constitutional law to protect the balance between liberty and security. Precisely for this reason, the consolidation of a coherent digital constitutionalism, anchored in the principles of proportionality, subsidiarity, and effective control, represents not only a theoretical requirement but a structural condition for maintaining the rule of law in a more digitalized environment.

Abstract

This study examines the constitutional boundaries of the use of data resulting from electronic communications or technical surveillance measures across three distinct yet interconnected levels. Firstly, it examines the decisions of the Constitutional Court of Romania regarding data retention and access, which have outlined general protection standards applicable regardless of the nature of the proceedings–whether civil or criminal. Secondly, the analysis focuses on technical surveillance measures within criminal proceedings as some of the most intrusive evidentiary tools, highlighting the requirements of legality, foreseeability, proportionality, and effective judicial oversight. Thirdly, the research addresses the expansion of data collection mechanisms in the fields of cybersecurity and national security, where surveillance acquires a structural dimension, transcending a strictly procedural purpose.

Building on the chronological evolution of constitutional case law, the study highlights how the Court has sanctioned generalized or insufficiently regulated surveillance and mandated the clear statutory definition of competent authorities and the safeguards applicable to interferences with private life and the secrecy of communications. The analysis demonstrates that, in a state governed by the rule of law, neither the efficiency of criminal investigations nor the imperatives of national security can justify surveillance mechanisms lacking adequate and sufficient safeguards.

Recent Romanian case law reveals a process of progressive constitutionalization of the digital space, where the legitimacy of digital evidence resides from its integration into a clear, restrictive normative framework subject to real jurisdictional control, ensuring that technology does not become an instrument for the discretionary exercise of power. Far from conducting an exhaustive examination of such a complex field, this research calls for a comparative law approach within the framework of contemporary digital constitutionalism.

Key words: digital evidence; rule of law; technical surveillance; proportionality; right to privacy; secrecy of communications; constitutional court.

References

I. Decisions of the Constitutional Court of Romania

1. Decision No 1.258 of October 8, 2009, regarding the exception of unconstitutionality of the provisions of Law No 298/2008 on the retention of data generated or processed by electronic communications service providers, published in the Official Gazette no. 798 of 23 November 2009.

2. Decision No 440 of 8 July 2014, regarding the exception of unconstitutionality of the provisions of Law No 82/2012 on data retention, published in the Official Gazette no. 653 of 4 September 2014.

3. Decision No 51 of 16 February 2016, regarding the exception of unconstitutionality of the provisions of Article 142 (1) of the Code of Criminal Procedure, published in the Official Gazette no. 190 of 14 March 2016.

4. Decision No 26 of 16 January 16, 2019, on the request for the settlement of the legal conflict of a constitutional nature between the Romanian Parliament, on the one hand, and the Public Ministry – the Prosecutor's Office attached to the High Court of Cassation and Justice, the High Court of Cassation and Justice, and the other courts of law, on the other hand, published in the Official Gazette no. 193 of 12 March 2019.

5. Decision No 55 of 16 February 2022, regarding the objection of unconstitutionality of the Law for the approval of Government Emergency Ordinance no. 6/2016 on certain measures for the execution of technical surveillance warrants ordered in criminal proceedings, published in the Official Gazette no. 590 of 17 June 2022.

6. Decision No 295 of 18 May 2022, regarding the objection of unconstitutionality of the Law for the amendment and completion of certain normative acts in the field of electronic communications and for the establishment of measures to facilitate the roll-out of electronic communications networks, published in the Official Gazette no. 533 of 31 May 2022.

7. Decision No 70 of 28nFebruary 2023, regarding the objection of unconstitutionality of the provisions of the Law on the cybersecurity and cyber defense of Romania, published in the Official Gazette no. 211 of 14 March 2023.

II. CJEU and ECtHR

8. CJEU, Judgment of 8 April 2014, Digital Rights Ireland Ltd, Joined Cases C-293/12 and C-594/12, EU:C:2014:238.

9. CJEU, Judgment of 21 December 2016, Tele2 Sverige AB and Watson, Joined Cases C-203/15 and C-698/15, EU:C:2016:970.

10. CJEU, Judgment of 20 September 2022, VD and SR, Joined Cases C-339/20 and C-397/20, EU:C:2022:703.

11. ECtHR, Judgment of 6 September 1978, Klass and Others v. Germany, Application no. 5029/71.

12. ECtHR, Judgment of 26 April 2007, Dumitru Popescu v. Romania (no. 2), Application no. 71525/01.

III. Normative Acts and International Documents

13. The Constitution of Romania, republished in the Official Gazette (*M. Of.*) no. 767 of 31 October 2003.

14. The Convention for the Protection of Human Rights and Fundamental Freedoms, ratified by Romania through Law no. 30/1994, published in the Official Gazette (*M. Of.*) no. 135 of 31 May 1994.

15. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, published in the *OJ* L 105 of 13 April 2006.

16. Government Emergency Ordinance (GEO) no. 6 of March 11, 2016, on certain measures for the execution of technical surveillance warrants ordered in criminal proceedings, published in the Official Gazette (*M. Of.*) no. 190 of 14 March 2016.

17. European Court of Human Rights, *Thematic Factsheet – Personal Data Protection*, July 2024.

18. Venice Commission, *Report on the Democratic Oversight of the Security Services* (CDL-AD(2007)016), Strasbourg, 11 June 2007.

19. European Commission, *Report to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism (CVM)*, COM(2017) 44 final, Brussels, 25.01.2017.

20. European Commission, *Report to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism (CVM)*, COM(2018) 778 final, Strasbourg, 13.11.2018.

21. European Commission, *Commission Staff Working Document – 2022 Rule of Law Report, Country Chapter on the rule of law situation in Romania*, SWD(2022) 523 final, Luxembourg, 13.07.2022.

22. Charter of Fundamental Rights of the European Union, published in the *Official Journal of the European Union*, C series, no. 83 of 30.03.2010 (2010/C 83/02).

23. European Parliament, Council and Commission, *European Declaration on Digital Rights and Principles for the Digital Decade*, published in the *Official Journal of the European Union*, C series, no. 23 of 23 January 2023 (2023/C 23/01).

24. Law No 58 of 14 March 2023 on the cybersecurity and cyber defense of Romania, published in the Official Gazette (*M. Of.*) no. 214 of 15 March 2023.

IV. Papers

25. Popa, A.-N., *CCR Case-law regarding the concept of "national security"*, published on Juridice.ro on 10.02.2020, available online at: https://www.juridice.ro/712215/jurisprudenta-ccr-cu-privire-la-notiunea-de-securitate-nationala.html#_ftn10.

26. Cristescu, D. I., *Vademecum on the investigation of illicit manifestations against and contrary to national security (III)*, published on Juridice.ro on December 8, 2023, available online at: https://www.juridice.ro/716980/vademecum-privind-investigarea-manifestarilor-ilicite-la-adresa-si-contra-securitatii-nationale-iii.html.

27. National Anticorruption Directorate, *Press Release no. 252/VIII/3 of March 9, 2016*, available online at: https://www.dna.ro/faces/comunicat.xhtml?id=7206.

28. C. F. Stoica, M. Safta, *Theoretical and practical issues relating to the right to the protection of personal data*, 5(2), Juridical Tribune – Review of Comparative and International Law 88–10, 2015.

29. Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.

30. Gianina-Anemona Radu, 'Theoretical and Practical Aspects Regarding Technical Surveillance in the Criminal Trial' (2023) *Valahia University Law Study* SI 216–223 https://www.ceeol.com/search/article-detail?id=1353109

31. Rodotà, S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Ediția a II-a, Ed. Laterza, Roma-Bari, 2004.

32. T. Toader, M. Safta, 'Constitutional Identity and Relations Between EU Law and Romanian Law' in András Zs Varga and Lilla Berkes (eds), *Common Values and Constitutional Identities – Can Separate Gears Be Synchronised?* (Central European Academic Publishing 2023) 271–352

33. Mihail Udroiu, 'A posteriori control of the legality of technical surveillance in Romanian criminal proceedings' (Studia Universitatis Babeș-Bolyai Iurisprudentia, Vol 68 No 2, 23 Dec 2023) https://doi.org/10.24193/SUBBiur.68(2023).2.6

Information about the authors:
Safta Marieta,
Professor at the Faculty of Law, "Titu Maiorescu" University of Bucharest,
Associate Professor at the Faculty of Law,
Bucharest University of Economic Studies,
187 Calea Văcărești, 040051, Bucharest, Romania

Stanciu Claudia Ana Maria,
PhD Student at the Doctoral School of Law,
Bucharest University of Economic Studies,
Lawyer, Bucharest Bar,
7 Piața Romană, 010374, Bucharest, Romania

DOI https://doi.org/10.30525/978-9934-26-686-7-2

АВТЕНТИЧНІСТЬ І ДОПУСТИМІСТЬ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ КРІЗЬ ПРИЗМУ ПРИНЦИПІВ КРИМІНАЛЬНОГО ПРОЦЕСУ

Волошина В. К.

ВСТУП

Стрімкий розвиток цифрових технологій наприкінці XX – на початку XXI століття суттєво трансформував характер суспільних відносин, способи комунікації та форми соціальної взаємодії. Ці процеси безпосередньо вплинули і на сферу кримінального судочинства, оскільки значна частина суспільно небезпечних діянь почала вчинятися із використанням інформаційно-комунікаційних технологій або залишати після себе цифрові сліди. У таких умовах традиційні уявлення про докази, джерела доказової інформації та механізми їх процесуальної оцінки зазнали істотного переосмислення.

Цифрові докази поступово перетворилися на один із ключових елементів доказування у кримінальному провадженні. Дані електронних пристроїв, серверів, телекомунікаційних мереж, хмарних сховищ, соціальних платформ та інформаційних систем дедалі частіше використовуються для встановлення фактичних обставин кримінальних правопорушень. Водночас особлива природа такої інформації зумовлює підвищену вразливість цифрових доказів до втручання, модифікації, копіювання та знищення, що ускладнює процес підтвердження їх достовірності та процесуальної надійності.

На відміну від матеріальних чи письмових доказів, цифрові дані не мають стабільної фізичної форми, а їх сприйняття можливе виключно за допомогою спеціальних технічних засобів і програмного забезпечення. Ця обставина зумовлює необхідність застосування особливих процесуальних та технічних механізмів для забезпечення незмінності інформації з моменту її виявлення до безпосереднього дослідження судом. У протилежному випадку виникають обґрунтовані сумніви щодо автентичності цифрових доказів, що прямо впливає на можливість їх використання у процесі доказування.

Особливої актуальності проблема автентичності та допустимості цифрових доказів набуває у контексті дотримання фундаментальних принципів кримінального процесу. Принцип законності вимагає, щоб отримання електронної інформації здійснювалося виключно в межах та у спосіб, передбачений законом. Презумпція невинуватості покладає на сторону обвинувачення обов'язок довести не лише факт існування цифрового доказу, але й його достовірність, цілісність та зв'язок із конкретною подією кримінального правопорушення. Принцип змагальності сторін передбачає реальну можливість перевірки та оскарження цифрових доказів стороною захисту, у тому числі шляхом проведення альтернативних експертиз.

Окремої уваги потребує співвідношення використання цифрових доказів із правом особи на повагу до приватного життя та таємниці комунікацій.

Отримання доступу до електронних пристроїв, особистих акаунтів або хмарних сервісів нерідко пов'язане з глибоким втручанням у приватну сферу особи, що вимагає ефективного судового контролю та чіткого процесуального регулювання. Недотримання цих вимог може призвести до порушення стандартів справедливого судового розгляду, навіть за наявності технічно достовірної доказової інформації.

У зв'язку з цим проблема забезпечення автентичності та допустимості цифрових доказів виходить за межі суто технічних питань і набуває комплексного правового характеру. Вона охоплює доктринальні підходи до розуміння природи цифрових доказів, процесуальні гарантії їх отримання та оцінки, а також практику національних і міжнародних судових інституцій. Саме в цій площині формується необхідність вироблення цілісного підходу до цифрових доказів як елементу сучасного кримінального процесу.

Метою даного дослідження є комплексний аналіз автентичності та допустимості цифрових доказів у кримінальному процесі крізь призму принципів кримінального судочинства, а також визначення основних напрямів удосконалення процесуальних механізмів роботи з електронною доказовою інформацією з урахуванням сучасних викликів цифрового середовища.

1. Передумови виникнення проблеми автентичності та допустимості цифрових доказів

Формування проблематики автентичності та допустимості цифрових доказів у кримінальному процесі є прямим наслідком глибинних змін у способах фіксації, зберігання та передачі інформації в сучасному суспільстві. Якщо в «класичному» кримінальному судочинстві доказова діяльність ґрунтувалася переважно на матеріальних об'єктах і безпосередньо сприйманих джерелах інформації, то в умовах цифровізації дедалі більша частина релевантних відомостей існує у нематеріальній формі й опосередковується технічними системами[1].

Поява цифрових слідів як результату функціонування інформаційних систем істотно розширила доказовий простір кримінального провадження. Електронні журнали подій, мережеві логи, метадані файлів, дані геолокації, цифрові записи комунікацій та інша електронна інформація дедалі частіше стають важливими джерелами даних про підготовку, вчинення та приховування кримінальних правопорушень[2]. Водночас використання таких даних у процесі доказування супроводжується низкою специфічних проблем від складності технічної фіксації до невизначеності процесуальних стандартів їх оцінки.

Однією з базових передумов виникнення досліджуваної проблеми є відсутність матеріальної стабільності цифрових доказів. На відміну від речових доказів, цифрова інформація не має сталої фізичної форми, її існування

[1] Петрик В.В. Використання електронних доказів у кримінальному провадженні // *Науковий вісник Ужгородського Національного Університету*. Серія «Право». Випуск 87: частина 4. (2025)// URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/03/19-3.pdf

[2] ResearchGate. (2025). Electronic evidence in criminal proceedings of Ukraine. URL: https://www.researchgate.net/publication/392347214_Electronic_evidence_in_criminal_proceedings_of_Ukraine

залежить від технічного середовища та умов зберігання. Будь-яке втручання в інформаційну систему як навмисне, так і випадкове може призвести до зміни змісту даних без очевидних зовнішніх слідів, що ускладнює відтворення їх первісного стану та породжує сумніви щодо автентичності. Саме тому в літературі наголошується на необхідності розроблення чітких процедур збирання, збереження й верифікації цифрових доказів [3].

Ще однією суттєвою передумовою проблеми є опосередкований характер сприйняття цифрових доказів судом. Суд, як правило, не має можливості «безпосередньо» дослідити цифрову інформацію без залучення технічних засобів або спеціалістів, а отже значною мірою покладається на результати експертиз, висновки фахівців і внутрішні процедури провайдерів послуг. За відсутності чітко визначених процесуальних стандартів така довіра ризикує бути суто декларативною й не гарантує належного рівня процесуальної справедливості, зокрема права сторони захисту на ефективну перевірку доказів.

Важливим чинником загострення проблеми є транснаціональний характер цифрового середовища. Дані, що мають доказове значення, часто зберігаються на серверах за межами національної юрисдикції або перебувають під контролем приватних транснаціональних компаній. Це ускладнює дотримання національних процесуальних вимог щодо їх отримання, створює ризики порушення принципу законності та ставить під сумнів допустимість таких доказів у межах внутрішнього кримінального процесу. Додаткові питання виникають у зв'язку з необхідністю узгодження вимог кримінального процесуального законодавства з режимом захисту персональних даних та стандартами права на приватне життя.

Окремо слід відзначити, що чинне кримінальне процесуальне законодавство України, як і законодавство багатьох інших держав, здебільшого не містить комплексного регулювання, спрямованого саме на роботу з цифровими доказами. Наявні норми мають загальний характер і нерідко застосовуються за аналогією до матеріальних або письмових доказів, що не враховує специфіку електронної інформації, її крихкість та залежність від технічного середовища. Унаслідок цього правозастосовна практика набуває фрагментарного характеру, а критерії допустимості цифрових доказів тлумачаться судами по-різному.

У науковій доктрині також немає єдності щодо самого поняття «цифровий (електронний) доказ». Частина авторів пропонує розглядати його як різновид електронного документа, інші як окрему, самостійну категорію доказових

[3] Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні // *Law and Safety*. 2024. № 2 (93) // URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653; Шульга В., Калюжна, Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення //*Теорія та практика судової експертизи і криміналістики*. Вип. 3 (40). С. 136–152. DOI: 10.32353/khrife.3.2025.10. ; Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility // *Journal of Law and Social Policy*. 2025.

засобів, що потребує автономного процесуального режиму[4]. Така доктринальна розбіжність ускладнює вироблення уніфікованих підходів до встановлення автентичності цифрових доказів і створює передумови для суперечливої судової практики, зокрема щодо визначення належного джерела, способу отримання й допустимого рівня технічного втручання.

У сукупності зазначені обставини свідчать, що проблема автентичності та допустимості цифрових доказів має системний характер і не може бути вирішена виключно за рахунок удосконалення технічних методів роботи з електронними даними. Вона потребує комплексного правового осмислення з урахуванням засад кримінального процесу, які визначають межі допустимого втручання держави у сферу приватних прав і свобод особи, а також стандартів справедливого судового розгляду, сформованих, зокрема, у практиці ЄСПЛ.

Саме в цій площині постає наукова проблема, що полягає у відсутності цілісного процесуального підходу до забезпечення автентичності цифрових доказів як передумови їх допустимості у кримінальному судочинстві. Невирішеність цієї проблеми створює ризики як для ефективності кримінального переслідування (через втрату або дискредитацію важливої цифрової інформації), так і для дотримання стандартів справедливого судового розгляду, включно з правом на захист і правом на повагу до приватного життя [5].

Вважаємо, що ускладнення роботи з цифровими доказами зумовлене не лише їх технічною специфікою, але й невідповідністю класичних процесуальних конструкцій новим формам доказової інформації. Традиційні підходи до доказування формувалися в умовах, коли джерело доказу та носій інформації були тісно пов'язані між собою. У цифровому середовищі такий зв'язок втрачає стабільність, оскільки одна й та сама інформація може одночасно існувати на кількох носіях, змінювати форму відображення та передаватися без фізичного контакту з оригінальним пристроєм.

Ця особливість зумовлює виникнення принципово нового для кримінального процесу питання, що саме слід вважати "оригіналом" цифрового доказу. На відміну від матеріальних об'єктів, де автентичність пов'язується з фізичною унікальністю предмета, у цифровому середовищі копія може бути технічно ідентичною первинному файлу. Як зазначає S. Mason, «it is important to obtain

[4] Квашук О.Д. Використання електронних доказів у кримінальному провадженні // *Центральноукраїнський вісник права та публічного управління.* Випуск/ Issue 2(10),2025.С. 50–56.; Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні // *Law and Safety*. 2024. № 2 (93) // URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653 ; Шульга В., Калюжна, Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення// *Теорія та практика судової експертизи і криміналістики.* Вип. 3 (40). С. 136–152. DOI: 10.32353/khrife.3.2025.10.; Метелев О.П., Цифрові докази у кримінальному процесі: видова характеристика // *Вісник кримінального судочинства* № 1–2, 2023. С.42-53. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/42-53

[5] The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. 2022. SSRN.

the item in the native format… as this is the only way… integrity… can be proven»[6]. За відсутності чітких процесуальних критеріїв це створює підґрунтя для сумнівів щодо достовірності доказів та відкриває можливості для зловживань у процесі їх подання і дослідження.

Ще одним важливим аспектом є розрив між технічною та юридичною автентичністю цифрових доказів. Навіть за умови, що з технічної точки зору дані не зазнали змін (що підтверджується, наприклад, хеш-значенням), це саме по собі не гарантує їх допустимості у кримінальному процесі. Юридична автентичність передбачає встановлення походження інформації, законність способу її отримання, а також дотримання процесуальних гарантій прав учасників провадження. Як зазначає І. Липкан, «інформація… має специфічну технічну природу, що забезпечує її автентичність і можливість дослідження».[7] Таким чином, технічна цілісність даних є лише однією з умов їх допустимості, але не може розглядатися як самодостатній критерій.

У цьому контексті особливої ваги набуває принцип законності, який виступає фундаментальною засадою кримінального процесу. Отримання цифрових доказів поза межами процесуальної форми, навіть за наявності їх фактичної достовірності, ставить під сумнів можливість їх використання у судовому розгляді. Практика свідчить, що порушення процедури доступу до електронних пристроїв або інформаційних систем часто призводить до визнання відповідних доказів недопустимими, оскільки такі порушення мають істотний характер і впливають на баланс між публічним інтересом та правами особи. Міжнародні стандарти підтверджують цю позицію: держави повинні забезпечувати процедури отримання електронних даних із дотриманням гарантій прав людини, включаючи «judicial or other independent supervision… limitation of the scope and the duration».[8]

Не менш значущою передумовою формування проблеми є обмежена здатність сторони захисту впливати на процес перевірки цифрових доказів. Європейський суд з прав людини наголошує, що «electronic evidence has become ubiquitous in criminal trials», а тому його оцінка повинна здійснюватися з урахуванням принципу справедливого судового розгляду.[9] У багатьох випадках цифрові дані вилучаються, копіюються та аналізуються без активної участі захисту, що ускладнює реалізацію принципу змагальності сторін. За відсутності належних процесуальних механізмів контролю за діями сторони

[6] Mason S. Electronic Evidence and Electronic Signatures. 5th ed. London: Institute of Advanced Legal Studies, 2021. URL: https://sas-space.sas.ac.uk/9564/1/9781911507246_min.pdf

[7] Липкан І.І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій: дис. … д-ра юрид. наук. Київ, 2025. URL: https://dpu.edu.ua/images/Documents/NAUKA/Doktorski%20specializovani%20vceni%20radi/Specializovana%20vcena%20rada%20D%2027.855.03/Lipkan%20Igor%20Ivanovic/Disertacia%20Lipkana%20I.I.pdf

[8] Convention on Cybercrime (Budapest Convention). Council of Europe, 2001. URL: https://rm.coe.int/1680081561

[9] European Court of Human Rights. Background Paper for the Judicial Seminar 2025. Strasbourg, 2024. URL: https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng

обвинувачення виникає ризик одностороннього формування доказової бази, що суперечить засадам справедливого судового розгляду.

Особливу складність становить і питання оцінки цифрових доказів судом. Як зазначають А. Політова та Т. Чехлай, «КПК України не містить згадки щодо електронних доказів», що створює прогалини у правовому регулюванні[10]. Судова практика демонструє відсутність єдиних підходів до визначення критеріїв допустимості електронної інформації. В одних випадках пріоритет надається технічним характеристикам доказу, в інших процесуальним аспектам його отримання. Така непослідовність створює правову невизначеність і підриває передбачуваність судових рішень, що є несумісним із принципом правової визначеності.

З огляду на викладене, проблема автентичності та допустимості цифрових доказів не може бути зведена до окремих недоліків правового регулювання чи прогалин у технічному забезпеченні слідчої діяльності. Вона має комплексний характер, охоплюючи доктринальний, нормативний і правозастосовний рівні кримінального процесу. Відсутність узгодженого підходу до розуміння цифрових доказів і стандартів їх оцінки негативно впливає як на ефективність розслідування кримінальних правопорушень, так і на рівень гарантій прав людини.

У зв'язку з цим наукова проблема дослідження полягає у необхідності вироблення цілісної процесуальної концепції забезпечення автентичності цифрових доказів, яка б ґрунтувалася на принципах кримінального судочинства та враховувала особливості цифрового середовища. Формулювання такої концепції є передумовою створення єдиних критеріїв допустимості електронної доказової інформації та підвищення якості судової оцінки цифрових доказів.

Таким чином, виникнення передумов проблеми та її формулювання свідчать про необхідність переходу від фрагментарного використання технічних інструментів до системного правового підходу, який поєднує технічні, процесуальні та правозахисні елементи. Саме цей підхід дозволяє розглядати цифрові докази не як виняток із загальних правил доказування, а як повноцінний інститут сучасного кримінального процесу.

2. Правова природа та поняття цифрових доказів у кримінальному процесі.

Правова природа та поняття цифрових (електронних) доказів у кримінальному процесі України є одним з найбільш актуальних і динамічних напрямів сучасного кримінально-процесуального права. Розвиток інформаційних технологій, масове використання цифрових пристроїв, мереж Інтернет, мобільних застосунків, хмарних сервісів та соціальних платформ призвели до появи принципово нових джерел доказової інформації, які не завжди вписуються в традиційну систему процесуальних джерел доказів, передбачену ч. 2 ст. 84 Кримінального процесуального кодексу України (далі КПК України). Процес доказування супроводжує всю стадію досудового розслідування від внесення

[10] Політова А.С., Чехлай Т.О. Допустимість цифрових доказів у кримінальному провадженні: аналіз судової практики. *Вісник МДУ. Серія: Право*. 2025. № 29. С. 104–115.

відомостей до Єдиного реєстру досудових розслідувань до прийняття остаточного рішення у кримінальному провадженні. Перевірка, оцінка та належне закріплення доказів здійснюється особою, яка проводить розслідування, з метою забезпечення того, щоб зібрані матеріали лягли в основу законного та обґрунтованого рішення. Якщо традиційні докази (показання, речові докази, документи, висновки експертів) переважно мають матеріальну або паперову форму, то електронні (цифрові) докази існують у нематеріальній, цифровій формі, що створює суттєві труднощі щодо їх фіксації, збереження цілісності, перевірки автентичності та оцінки допустимості. Питання правової природи, поняття та використання електронних (цифрових) доказів активно вивчаються українськими науковцями. Серед ключових праць дослідження О. Сіренко, В. Хахановського та М. Гуцалюка, А. Столітнього та І. Каланчі, О. Козицької, О. Метелєва, Д. Алексєєвої-Працюк, М. Гуцалюка та П. Антонюка, А. Коваленка, Л. Перцової-Тодорової, Г. Татаренка та ін., А. Антонюка та В. Русецької, В. Школьнікова.

Після 2021 р. дискусія набула нового імпульсу завдяки прийняттю Закону України від 15.03.2022 № 2137-IX «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам», який суттєво розширив можливості роботи з електронними доказами в умовах кіберзлочинності та воєнного стану. Сучасні дослідження підкреслюють необхідність визнання електронних доказів самостійною групою джерел доказів, матеріали круглих столів та монографій з цифровізації кримінального провадження.

Інформаційні технології зумовили постійну необхідність передачі та обміну даними. Використання електронних пристроїв стало щоденною практикою, але паралельно зросла кількість правопорушень у цифровій сфері. Оскільки дані існують в електронній формі, механізм їх фіксації як доказів має процедурні особливості.

У доктрині сформувалося кілька підходів до розуміння правової природи та поняття цифрових (електронних) доказів.

Перший (розширений, функціональний) підхід розглядає електронні докази як будь-яку інформацію в цифровій формі, що має значення для встановлення обставин провадження, незалежно від конкретного джерела. О. Козицька визначала їх як цифрові об’єкти, що були засобом чи знаряддям вчинення злочину, зберегли електронно-цифрові сліди, були предметом чи об’єктом правопорушення або містять відомості, які можуть бути використані як доказ[11]. Аналогічно О. Сіренко наголошувала на необхідності законодавчого закріплення поняття «електронні докази» в КПК[12] .

Другий (техніко-ознаковий) підхід акцентує специфічні властивості: нематеріальний вигляд; неможливість існування поза технічним носієм або каналом зв’язку; вільне переміщення в мережі; сприйняття лише за допомогою

[11] Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні // *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.

[12] Сіренко О.В. Електронні докази у кримінальному провадженні // *Міжнародний юридичний вісник*. 2019. № 14. С. 208–214.

техніки та ПЗ; потреба в спеціальному порядку збирання, перевірки, оцінки; можливість дистанційного внесення змін чи видалення[13].

Третій (інтеграційний, сучасний) підхід пропонує визнати електронні докази окремою самостійною групою, відмінною від показань, речових доказів, документів та висновків експертів[14]. О. Метелєв наголошував на необхідності виділення спеціальних слідчих дій «цифровий огляд інформаційного середовища» та «цифрове копіювання»[15]. Пропонується закріпити окрему статтю КПК (наприклад, ст. 99-1) з визначенням цифрових доказів як відомостей або документів у цифровій/електронній формі, отриманих під час досудового розслідування чи ОРД.

У сучасній доктрині переважає погляд, що електронні (цифрові) докази – це інформація в електронній (цифровій) формі про факти та обставини кримінального провадження, зафіксована в електронних документах, текстових, мультимедійних, голосових повідомленнях, метаданих, базах даних тощо, яка зберігається на електронних носіях (мобільні пристрої, сервери, карти пам'яті, USB-накопичувачі, хмарні сховища), вільно переміщується в мережі, не має нерозривного зв'язку з матеріальним носієм, потребує спеціального порядку збирання, перевірки та оцінки, сприймається лише за допомогою технічних засобів і ПЗ.

Авторське визначення, запропоноване в сучасних дослідженнях[16]: електронний доказ у кримінальному процесі це інформація про факти та обставини кримінального провадження, зафіксована в електронній (цифровій) формі, отримана в передбаченому КПК порядку, відмінна від доказів в електронному вигляді та така, що характеризується нематеріальною природою, залежністю від технічних засобів та специфічними ризиками зміни/втрати цілісності.

Джерела електронних доказів багатоманітні та не вичерпні: електронні документи (за Законом «Про електронні документи та електронний документообіг»; сайти, електронні бази даних, файли, електронна пошта, чати, сервери; записи з камер відеоспостереження, реєстраторів, застосунків на мобільних пристроях; дані з відкритих джерел (OSINT); матеріали з міжнародної правової допомоги тощо.

---

[13] Алексєєва-Працюк Д. та ін. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування // *Науковий вісник публічного та приватного права*. 2018. № 2. С. 252.; Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерел доказів у кримінальному провадженні // *Криміналістичний вісник*. 2020. № 1. С. 42.

[14] Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України // *Проблеми законності*. 2019. № 146. С. 179.; Антонюк А.Б., Русецька В.А. Електронні докази в кримінальному провадженні // *Міжнародний науковий журнал «Інтернаука».* 2020. № 10. С. 85.

[15] Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження // *Науковий вісник Ужгородського національного університету*. 2020. № 60. С. 177.

[16] Мілімко Л.В. Електронні докази в кримінальному судочинстві України // *Науковий вісник УжНУ*. Серія «Право». 2025. (або рік видання за фактом публікації).

Принципи, що характеризують електронні докази: допустимість, справжність (автентичність), повнота, надійність, зрозумілість, правдоподібність[17].

Правова природа цифрових доказів є комплексною: вони поєднують ознаки документа (якщо оформлені належним чином), речового доказу (якщо вилучено носій) та специфічної інформаційної категорії, що потребує самостійного регулювання. Відсутність легального визначення в КПК України (на відміну від ЦПК, ГПК, КАС) залишається ключовою проблемою, яка ускладнює єдність практики, особливо в умовах воєнного стану та зростання кіберзлочинності.

Отже, електронні (цифрові) докази є невід'ємною частиною сучасного кримінального провадження, їх роль зростає в розслідуванні кіберзлочинів, воєнних злочинів, злочинів проти національної безпеки. Вони характеризуються нематеріальною формою, залежністю від технічних засобів, ризиками маніпуляцій, потребують спеціальних процедур збирання, фіксації (з дотриманням chain of custody), перевірки та оцінки.

Вважаємо, що доцільно доповнити КПК України окремою статтею про електронні (цифрові) докази, визначити їх поняття, ознаки, порядок збирання, перевірки, оцінки та використання, передбачити спеціальні слідчі дії щодо роботи з цифровою інформацією, врахувати міжнародні стандарти. Це дозволить усунути невідповідності, підвищити ефективність розслідування та забезпечити права учасників провадження.

3. Процесуальні принципи забезпечення допустимості цифрових доказів

Подальший розвиток процесуально-правового підходу до оцінки цифрових доказів неможливий без поглибленого аналізу принципу законності як базового критерію їх допустимості. У сфері цифрових доказів цей принцип набуває специфічного змісту, оскільки будь-яке втручання у функціонування електронних пристроїв, інформаційних систем або мереж пов'язане з потенційним обмеженням конституційних прав особи. Законність у такому контексті передбачає не лише наявність формальної правової підстави для проведення слідчої (розшукової) дії, а й реальне дотримання визначеної законом процедури доступу до цифрових даних, включно із судовим контролем, фіксацією кожного етапу роботи з інформацією та дотриманням принципу пропорційності[18].

Порушення процесуальної форми під час отримання електронної інформації нерідко має латентний характер і не завжди очевидне на стадії судового розгляду. Тому вимога законності виступає не лише критерієм оцінки діяльності органів досудового розслідування, а й ключовою гарантією захисту

[17] Метелев О.П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі // *Вісник кримінального судочинства*. 2019. № 3. С. 234–235.

[18] Квашук О.Д. Використання електронних доказів у кримінальному провадженні // *Центральноукраїнський вісник права та публічного управління.* Випуск/ Issue 2(10), 2025. С. 50–56.

від свавільного втручання в приватну сферу. Якщо цифрові докази здобуті без належного судового контролю чи з перевищенням повноважень, їх використання в кримінальному провадженні суперечить змісту принципу законності незалежно від їх доказової ваги.

Тісно пов'язаний із законністю принцип презумпції невинуватості визначає загальну логіку розподілу тягаря доказування. У контексті цифрових доказів він означає, що будь-які обґрунтовані сумніви щодо автентичності, походження чи цілісності електронної інформації мають тлумачитися на користь особи, щодо якої здійснюється кримінальне переслідування. Відповідно, саме сторона обвинувачення повинна довести, що відповідні цифрові дані не зазнали несанкціонованих змін, не були сфальсифіковані й отримані з дотриманням процесуальних вимог, а ланцюг їх збереження є безперервним.

Особливість цифрових доказів полягає в тому, що їх технічна складність і залежність від спеціальних знань створюють відчутну асиметрію між сторонами кримінального провадження. Органи досудового розслідування зазвичай мають доступ до значно ширших технічних ресурсів і експертного потенціалу, ніж сторона захисту. У таких умовах презумпція невинуватості фактично виконує компенсаторну функцію, покликану запобігти перекладанню на захист обов'язку доводити недостовірність чи фальсифікацію цифрових доказів до того, як їх автентичність буде належним чином обґрунтована стороною обвинувачення.

Не менш важливим у цьому контексті є принцип змагальності сторін, який передбачає реальну, а не формальну можливість кожної зі сторін брати участь у дослідженні доказів. Стосовно цифрових доказів це означає забезпечення доступу захисту до копій відповідних електронних носіїв, інформації про використані методи й програмні засоби, а також створення умов для ініціювання альтернативних чи повторних експертиз. За відсутності таких можливостей змагальність перетворюється на декларацію, а висновки експертів набувають характеру фактично неоспорюваних, що підриває довіру до результатів судового розгляду.

На практиці обмеження доступу захисту до цифрових доказів часто мотивується міркуваннями безпеки або ризиком втручання у дані. Водночас подібні аргументи не можуть мати універсального характеру і автоматично виправдовувати істотне звуження процесуальних прав захисту. Баланс між необхідністю збереження цілісності цифрових даних і забезпеченням реальної змагальності має досягатися через запровадження чітких процесуальних гарантій (створення форензичних копій, використання сертифікованих інструментів, фіксацію кожної операції), а не шляхом односторонніх заборон.

Окремого розгляду потребує право на захист як комплексна процесуальна гарантія, що охоплює можливість своєчасного ознайомлення з доказами, участі в слідчих діях, використання спеціальних знань та залучення фахівців для критичної оцінки цифрової інформації. У сфері цифрових доказів реалізація цього права ускладнюється як технічними бар'єрами, так і відсутністю деталізованих процедур, які б регламентували доступ захисника до електронних даних та його участь у їх дослідженні. У підсумку існує ризик, що

суттєві цифрові докази фактично залишаться поза дієвим судовим контролем, навіть за формального дотримання процесуальної форми.

Узагальнюючи викладене, слід констатувати, що наявні підходи до вирішення проблеми автентичності та допустимості цифрових доказів є фрагментарними і не забезпечують повної реалізації засад кримінального процесу. Технічні засоби фіксації та захисту даних, хоч і відіграють важливу роль, не можуть замінити процесуальні гарантії й самі по собі не гарантують справедливості судового розгляду. Ефективна модель оцінки цифрових доказів можлива лише за умови органічного поєднання технічних і правових елементів у межах цілісного процесуального підходу.

У цьому зв'язку завдання дослідження полягає у виробленні узгодженого підходу до допустимості цифрових доказів, який поєднував би вимоги технічної автентичності з принципами законності, презумпції невинуватості, змагальності сторін та належної реалізації права на захист. Запровадження такого підходу має сприяти підвищенню рівня правової визначеності, зменшенню ризику довільного тлумачення критеріїв допустимості й забезпеченню балансу між ефективністю кримінального переслідування та дотриманням прав людини.

Завершуючи аналіз існуючих підходів до проблеми автентичності та допустимості цифрових доказів, варто наголосити, що жоден із них у відокремленому вигляді не відповідає всім викликам сучасного кримінального процесу. Техніко-орієнтований підхід, попри очевидні переваги у сфері фіксації та збереження електронної інформації, недостатньо відображає процесуальний вимір доказування. Процесуально-правовий підхід, навпаки, спирається на фундаментальні засади судочинства, але часто лишається занадто загальним і не враховує особливостей цифрового середовища.

Саме тому особливого значення набуває питання узгодження технічних стандартів роботи з цифровими даними з процесуальними вимогами кримінального провадження. Цифрові докази мають оцінюватися не лише з погляду їх інформаційної цінності чи технічної цілісності, а й з урахуванням того, чи був дотриманий належний процесуальний порядок на всіх етапах від виявлення й вилучення до дослідження в суді. Відсутність уніфікованих критеріїв допустимості, які послідовно застосовувалися б як слідчими, так і судами, породжує правову непевність: у подібних ситуаціях ідентичні за природою цифрові дані можуть оцінюватися по-різному.

Міжнародний вимір проблеми зумовлений тим, що цифрові докази дедалі частіше мають транснаціональний характер. Доступ до даних, що зберігаються за кордоном або контролюються іноземними сервіс-провайдерами, ставить перед правозастосовними органами складні завдання, пов'язані з дотриманням принципу законності та міжнародних стандартів захисту прав людини. За таких умов оцінка допустимості цифрових доказів повинна здійснюватися з урахуванням не лише внутрішнього процесуального законодавства, а й відповідних міжнародних зобов'язань держави.

Важлива роль у цій системі належить суду як остаточному арбітру у питаннях допустимості цифрових доказів. Судова перевірка не може обмежуватися виключно формальним контролем наявності ухвал, протоколів

чи технічних звітів. Її змістом має стати з'ясування того, чи забезпечено у конкретній справі реальне дотримання засад справедливого судового розгляду, рівності сторін та права на ефективний захист. Такий підхід дозволяє уникнути надмірного формалізму і підтримати баланс між інтересами правосуддя та правами особи.

З огляду на це завдання даного дослідження полягає у формуванні інтегрованого процесуального підходу до автентичності та допустимості цифрових доказів, який поєднає технічні механізми забезпечення цілісності електронних даних із вимогами основних принципів кримінального процесу. Такий підхід має ґрунтуватися на чітких критеріях законності отримання цифрової інформації, обґрунтованому розподілі тягаря доказування автентичності між сторонами, а також на реальному забезпеченні змагальності й права на захист при дослідженні цифрових доказів у суді. Його впровадження створює підґрунтя для підвищення ефективності кримінального судочинства в умовах цифровізації та одночасно гарантує належний рівень захисту прав людини, дозволяючи розглядати цифрові докази як повноцінний інститут сучасного кримінального процесу.

4. Міжнародні стандарти допустимості цифрових доказів та практика ЄСПЛ

Стрімкий розвиток цифрових технологій спричинив не лише трансформацію національних підходів до доказування у кримінальному процесі, а й формування міжнародних стандартів роботи з електронними доказами. З огляду на транснаціональний характер кіберпростору та глобальну природу цифрових даних, питання їх отримання, фіксації та оцінки дедалі частіше виходять за межі національної юрисдикції[19]. У таких умовах узгодження внутрішніх процесуальних механізмів із міжнародними правовими стандартами набуває критичного значення.

Одним із фундаментальних міжнародних актів у сфері боротьби з кіберзлочинністю та роботи з цифровими доказами є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.)[20]. Цей документ став першим універсальним інструментом, що визначив правові засади міжнародного співробітництва у виявленні, збереженні та отриманні електронних доказів. Статті 16–22 Конвенції детально регламентують принципи оперативного збереження комп'ютерних даних, процедури доступу до інформації в комп'ютерних системах, а також механізми транскордонної взаємодії при розслідуванні злочинів у цифровому середовищі[21].

Особливістю Будапештської конвенції є системний підхід до цифрових доказів як об'єкта, що вимагає одночасного дотримання як технічних, так і правозахисних стандартів (ст. 15)[22]. Конвенція прямо передбачає необхідність

[19] Гутник Х. М., Хитра О. В. Цифрові докази у кримінальному процесі : монографія. Львів: ЛДУВС України, 2022. 248 с.

[20] Конвенція Ради Європи про кіберзлочинність від 23.11.2001 № 185 (ETS № 185). Ратифікована Законом України № 608-III від 21.09.2005.

[21] Там само, ст. 16–22.

[22] Там само, ст. 15.

пропорційності втручання у приватне життя, що унеможливлює використання електронної інформації, отриманої з порушенням базових процесуальних гарантій.

Подальший розвиток міжнародних стандартів пов'язаний із правом Європейського Союзу, зокрема Регламентом (ЄС) 2023/1543 про Європейську виробничу ордерну систему (e-Evidence Regulation)[23]. Цей документ запровадив концепцію європейських ордерів на отримання електронних доказів, що передбачає спрощені процедури транскордонного доступу до даних, зберігаючи при цьому високі стандарти захисту прав людини. Допустимість електронної інформації тут оцінюється комплексно через призму як технічної цілісності (хеш-сум, ланцюг збереження), так і законності отримання з належним судовим контролем[24].

Важливе місце посідають і міжнародні стандарти поводження з цифровими доказами, розроблені INTERPOL та ENFSI. Зокрема, ISO/IEC 27037:2012 (Guidelines for identification, collection, acquisition and preservation of digital evidence) наголошує на безумовній незмінності інформації та детальному документуванні кожного етапу роботи з нею[25]. Ці стандарти, попри технічний характер, тісно переплітаються з процесуальними гарантіями, забезпечуючи суду обґрунтовану довіру до цифрових доказів.

Практика Європейського суду з прав людини формує ключові критерії допустимості цифрових доказів через призму статей 6 (право на справедливий суд) та 8 Конвенції (повага до приватного життя)[26]. Хоча ЄСПЛ не розробив спеціальної доктрини «цифрових доказів», його позиція чітка: допустимість є прерогативою національного права, але загальна справедливість провадження залишається під контролем Конвенції[27].

У рішенні *Demirhan v. Turkey* (2025)[28] Суд визнав порушення ст. 6 §1 через використання мобільних метаданних без належного судового контролю, попри їх технічну достовірність. ЄСПЛ підкреслив, що масове отримання електронних даних без конкретизації обґрунтування є непропорційним втручанням у приватне життя.

У справі *Benedittini and Others v. Italy* (2023)[29] Суд встановив порушення принципу рівності сторін: обвинувачення надало експертний звіт про аналіз

[23] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 June 2023 on European Production and Preservation Orders for electronic evidence in criminal matters // *Official Journal of the European Union.* 2023. L 168.

[24] Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. Commonwealth Secretariat. London, 2025.

[25] Information technology -Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

[26] Конвенція про захист прав людини і основоположних свобод від 04.11.1950 // URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

[27] *Schatschaschwili v. Germany* [GC], № 30362/08, ECHR 2015, § 101. // URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159566%22]}

[28] Demirhan v. Turkey, № 13115/21, ECHR 2025 // URL : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-117601%22]}

[29] Benedittini and Others v. Italy, № 22152/13, ECHR 2023, § 45–52 // URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98442%22]}

телефонних з'єднань, але відмовило захисту в доступі до сирцевих даних і програмного забезпечення. ЄСПЛ наголосив, що у цифрових доказах реальна можливість оскарження передбачає доступ до первинних носіїв та методології аналізу.

Значущою є позиція щодо доказів від приватних суб'єктів. У *Kablis v. Russia* (2021)[30] ЄСПЛ підкреслив, що отримання IP-логів від провайдера за запитом поліції не звільняє державу від обов'язку забезпечити процесуальні гарантії. Навпаки, потрібна подвійна перевірка: законність запиту до приватної компанії та пропорційність втручання.

Узагальнюючи, міжнародні стандарти та практика ЄСПЛ вимагають від національних судів комплексної оцінки цифрових доказів за такими критеріями:

1. Законність отримання (судовий контроль, пропорційність);
2. Технічна автентичність (ланцюг збереження, хеш-сум);
3. Змагальність (доступ захисту до первинних даних);
4. Загальна справедливість провадження.

Ці принципи слугують орієнтиром для гармонізації українського КПК, зокрема щодо транскордонного доступу до даних та критеріїв допустимості електронних доказів.

5. Особливості фіксації та забезпечення цілісності цифрових доказів у кримінальному провадженні

Ефективність використання цифрових доказів у кримінальному процесі значною мірою залежить від належної організації їх фіксації, збереження та подальшої перевірки. На відміну від традиційних доказових об'єктів, цифрова інформація характеризується високою динамічністю, можливістю миттєвого копіювання та ризиком непомітної модифікації. Саме ці властивості зумовлюють необхідність застосування спеціальних процедур, спрямованих на забезпечення незмінності електронних даних від моменту їх виявлення до дослідження судом.

Однією з ключових особливостей роботи з цифровими доказами є необхідність точної фіксації первісного стану інформації. Така фіксація передбачає не лише копіювання даних, але й документування технічних параметрів їх зберігання, структури файлової системи, метаданих та інших характеристик, що дозволяють відтворити контекст функціонування інформаційної системи. Без належної фіксації цих параметрів цифрові докази можуть втратити свою доказову цінність, оскільки стає неможливим підтвердити їх незмінність.

Важливим інструментом забезпечення цілісності цифрових доказів є створення точних цифрових копій носіїв інформації, яке здійснюється із застосуванням спеціалізованих технічних засобів. Такий процес дозволяє працювати з копією даних без ризику зміни оригінального носія. Принцип збереження оригіналу у незмінному стані є одним із базових у цифровій

[30] Kablis v. Russia, № 46118/13, ECHR 2021, § 98. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-192769%22]}

криміналістиці, оскільки будь-яке втручання в первинний носій може поставити під сумнів автентичність інформації.

Не менш важливу роль відіграє фіксація метаданих, які містять інформацію про створення, зміну та використання цифрових файлів. Метадані дозволяють встановити часові межі існування інформації, ідентифікувати користувачів, які мали доступ до даних, та відстежити історію їх змін. У багатьох випадках саме метадані виступають ключовим джерелом доказової інформації, що підтверджує або спростовує обставини кримінального правопорушення.

З метою підтвердження незмінності цифрових доказів широко застосовуються криптографічні методи контролю цілісності, зокрема використання хеш-функцій. Хеш-значення є унікальним цифровим відбитком інформації, який змінюється при будь-якому втручанні у дані. Порівняння хеш-значень, отриманих на різних етапах роботи з цифровими доказами, дозволяє встановити факт збереження або порушення їх цілісності.

Водночас технічні засоби забезпечення незмінності даних повинні доповнюватися процесуальним документуванням усіх дій, пов'язаних із цифровими доказами. Це передбачає складання протоколів вилучення, фіксацію осіб, які мали доступ до інформації, а також зазначення умов її зберігання. Така процедура формує так званий ланцюг зберігання доказів, який дозволяє простежити весь шлях цифрової інформації від моменту її виявлення до судового розгляду.

Ланцюг зберігання відіграє вирішальну роль у забезпеченні довіри до цифрових доказів. Його порушення або неповнота документування можуть створити підстави для сумнівів щодо автентичності інформації. У цьому контексті важливо забезпечити безперервність контролю за доступом до цифрових носіїв та виключити можливість несанкціонованого втручання у дані.

Особливу складність становить фіксація цифрових доказів, що зберігаються у віддалених інформаційних системах та хмарних сервісах. У таких випадках органи досудового розслідування не мають фізичного доступу до носіїв інформації, а отримання даних здійснюється через провайдерів електронних послуг. Це створює додаткові ризики втрати частини інформації або неможливості перевірки її первісного стану. У зв'язку з цим особливого значення набуває оперативність збереження даних та чітке документування процедур їх отримання.

Не менш важливим є питання забезпечення процесуальної прозорості роботи з цифровими доказами. Сторона захисту повинна мати можливість перевірити достовірність технічних процедур, що застосовувалися під час вилучення та аналізу інформації. Це передбачає доступ до копій цифрових носіїв, результатів експертних досліджень та методик, використаних при обробці даних. Забезпечення такої прозорості є необхідною умовою реалізації принципу змагальності сторін.

Важливим аспектом є також зберігання цифрових доказів протягом усього кримінального провадження. Неналежні умови зберігання можуть призвести до пошкодження носіїв інформації або втрати даних, що унеможливить їх використання у судовому розгляді. Саме тому до цифрових доказів

застосовуються підвищені вимоги щодо контролю доступу, резервного копіювання та захисту від несанкціонованого втручання.

Узагальнюючи викладене, можна зробити висновок, що забезпечення цілісності цифрових доказів є комплексним процесом, який поєднує технічні та процесуальні елементи. Лише за умови їх узгодженого застосування можливо гарантувати достовірність електронної інформації та її допустимість у кримінальному судочинстві. Відсутність належної фіксації, документування або контролю за цифровими доказами створює ризик втрати їх доказового значення та може призвести до порушення принципів справедливого судового розгляду.

Таким чином, особливості фіксації та забезпечення цілісності цифрових доказів свідчать про необхідність формування спеціалізованих процесуальних стандартів, які враховують специфіку електронної інформації та спрямовані на забезпечення балансу між ефективністю кримінального переслідування і захистом прав людини.

ВИСНОВКИ

Проведене дослідження дозволяє дійти висновку, що цифрові докази стали невід'ємним елементом сучасного кримінального процесу та істотно вплинули на трансформацію традиційних уявлень про доказування. Їх поява зумовлена не лише розвитком інформаційних технологій, але й зміною способів вчинення кримінальних правопорушень, значна частина яких супроводжується утворенням цифрових слідів. У таких умовах забезпечення автентичності та допустимості цифрових доказів набуває ключового значення для ефективності та справедливості кримінального судочинства.

У роботі обґрунтовано, що специфіка цифрових доказів полягає у їх нематеріальній природі, опосередкованості технічними системами та підвищеній вразливості до змін. Ці особливості зумовлюють необхідність застосування спеціальних процесуальних і технічних механізмів для підтвердження достовірності електронної інформації. Водночас встановлено, що технічна автентичність цифрових даних не може розглядатися як самодостатній критерій їх допустимості у кримінальному процесі без належного врахування процесуальних гарантій.

Аналіз передумов формування проблеми автентичності та допустимості цифрових доказів свідчить про наявність системних суперечностей між класичними процесуальними конструкціями та новими формами доказової інформації. Відсутність чітко визначеного понятійного апарату, єдиних критеріїв допустимості та уніфікованих стандартів судової оцінки цифрових доказів призводить до фрагментарності правозастосовної практики та правової невизначеності. Це, у свою чергу, негативно впливає на реалізацію принципів кримінального процесу.

У ході дослідження встановлено, що ключову роль у забезпеченні допустимості цифрових доказів відіграють принципи законності, презумпції невинуватості, змагальності сторін та забезпечення права на захист. Принцип законності визначає межі допустимого втручання держави у сферу приватних прав особи під час отримання цифрової інформації та виступає первинною

умовою використання електронних даних у процесі доказування. Порушення процесуальної форми отримання цифрових доказів, незалежно від їх фактичної достовірності, підриває легітимність таких доказів у судовому розгляді.

Презумпція невинуватості у контексті цифрових доказів виявляється у покладенні тягаря доведення їх автентичності та допустимості на сторону обвинувачення. Будь-які сумніви щодо походження, цілісності або незмінності електронної інформації мають тлумачитися на користь особи, щодо якої здійснюється кримінальне переслідування. Такий підхід сприяє підтриманню процесуальної рівноваги між сторонами та запобігає необґрунтованому використанню технічно складних доказів як засобу тиску на захист.

Принцип змагальності сторін та право на захист набувають особливої ваги у сфері цифрових доказів, оскільки їх технічна складність може створювати асиметрію процесуальних можливостей. Забезпечення реального доступу сторони захисту до цифрових носіїв, результатів експертиз і методів обробки даних є необхідною умовою ефективного судового контролю за доказами. Обмеження таких можливостей перетворює змагальність на формальність і ставить під сумнів справедливість судового розгляду.

Дослідження існуючих підходів до вирішення проблеми показало, що техніко-орієнтовані та процесуально-правові концепції мають застосовуватися не ізольовано, а у взаємозв'язку. Технічні інструменти фіксації та збереження цифрових даних повинні бути інтегровані у чітко визначену процесуальну форму, яка забезпечує дотримання прав учасників кримінального провадження. Лише за таких умов можливе формування довіри до цифрових доказів як повноцінного елементу доказової системи.

Особливу увагу в роботі приділено необхідності врахування міжнародного та транснаціонального виміру використання цифрових доказів. Зберігання електронної інформації за межами національної юрисдикції, а також участь приватних транснаціональних суб'єктів у контролі за даними вимагають адаптації національних процесуальних підходів до міжнародних стандартів захисту прав людини. У цьому контексті практика міжнародних судових інституцій слугує важливим орієнтиром для формування критеріїв допустимості цифрових доказів.

Узагальнюючи результати дослідження, можна констатувати, що забезпечення автентичності та допустимості цифрових доказів потребує формування цілісної процесуальної концепції, яка поєднує технічні, правові та правозахисні елементи. Така концепція має ґрунтуватися на принципах кримінального процесу та бути спрямованою на досягнення балансу між ефективністю кримінального переслідування і дотриманням прав людини. Реалізація зазначених підходів сприятиме підвищенню якості судового розгляду та зміцненню довіри до правосуддя в умовах цифровізації.

Проведений аналіз міжнародних стандартів допустимості цифрових доказів та практики Європейського суду з прав людини дозволяє дійти висновку, що сучасні підходи до використання електронної доказової інформації ґрунтуються на пріоритеті процесуальних гарантій прав людини. Міжнародні правові акти та судова практика формують комплексну модель оцінки цифрових доказів, відповідно до якої технічна достовірність електронних даних

не може розглядатися ізольовано від законності способу їх отримання та загальної справедливості кримінального провадження.

Встановлено, що Будапештська конвенція та інші міжнародні стандарти закріплюють принцип пропорційності втручання у приватне життя під час отримання електронної інформації, що є ключовою умовою допустимості цифрових доказів у кримінальному процесі. Практика Європейського суду з прав людини підтверджує, що навіть технічно достовірні докази можуть бути визнані несумісними зі стандартами справедливого судового розгляду у разі порушення принципів законності, рівності сторін або права на ефективний захист.

Водночас аналіз особливостей фіксації та забезпечення цілісності цифрових доказів свідчить, що технічні методи контролю інформації відіграють важливу, але допоміжну роль у процесі доказування. Використання спеціалізованих засобів копіювання, хешування, документування метаданих та формування ланцюга зберігання дозволяє забезпечити незмінність електронних даних, однак саме по собі не гарантує їх процесуальної допустимості.

Доведено, що ключовою умовою забезпечення доказової сили цифрової інформації є поєднання технічних процедур із чітко визначеною процесуальною формою їх застосування. Відсутність належного документування дій із цифровими доказами, порушення ланцюга їх зберігання або обмеження доступу сторони захисту до інформації створюють ризик втрати доказової цінності електронних даних та можуть призвести до порушення принципів справедливого судового розгляду.

Узагальнюючи результати дослідження, можна констатувати, що ефективне використання цифрових доказів у кримінальному процесі можливе лише за умови інтеграції міжнародних стандартів, технічних механізмів контролю та процесуальних гарантій прав людини. Саме такий комплексний підхід дозволяє забезпечити баланс між потребами кримінального переслідування та необхідністю захисту фундаментальних прав особи в умовах цифровізації правосуддя.

АНОТАЦІЯ

У розділі монографії досліджуються теоретико-правові та процесуальні засади забезпечення автентичності й допустимості цифрових доказів у кримінальному процесі в умовах цифровізації суспільних відносин. Проаналізовано правову природу цифрових доказів, їх специфічні ознаки та місце в системі доказового права. Особливу увагу приділено передумовам виникнення проблеми автентичності електронної доказової інформації та чинникам, що ускладнюють її процесуальну оцінку. Розкрито вплив принципів законності, презумпції невинуватості, змагальності сторін і забезпечення права на захист на формування критеріїв допустимості цифрових доказів. Обґрунтовано, що технічна цілісність електронних даних не може розглядатися ізольовано від процесуальної форми їх отримання та дослідження. Зроблено висновок про необхідність формування інтегрованого процесуального підходу до оцінки цифрових доказів, який поєднує технічні та правові механізми з урахуванням стандартів справедливого судового розгляду. Визначено

напрями вдосконалення кримінального процесуального регулювання у сфері використання цифрових доказів.

Література:

1. Benedittini and Others v. Italy, № 22152/13, ECHR 2023, § 45–52. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98442%22]}
2. Convention on Cybercrime (Budapest Convention). Council of Europe, 2001. URL: https://rm.coe.int/1680081561
3. Demirhan v. Turkey, № 13115/21, ECHR 2025 (підтверджено у практиці ЄСПЛ). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-117601%22]}
4. European Court of Human Rights. Background Paper for the Judicial Seminar 2025. Strasbourg, 2024. URL: https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng
5. Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. Commonwealth Secretariat. London, 2025.
6. Information technology -Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.
7. Kablis v. Russia, № 46118/13, ECHR 2021, § 98. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-192769%22]}
8. Mason S. Electronic Evidence and Electronic Signatures. 5th ed. London: Institute of Advanced Legal Studies, 2021. URL: https://sas-space.sas.ac.uk/9564/1/9781911507246_min.pdf
9. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 June 2023 on European Production and Preservation Orders for electronic evidence in criminal matters. *Official Journal of the European Union.* 2023. L 168.
10. ResearchGate. (2025). Electronic evidence in criminal proceedings of Ukraine. URL:https://www.researchgate.net/publication/392347214_Electronic_evidence_in_criminal_proceedings_of_Ukraine
11. *Schatschaschwili v. Germany* [GC], № 30362/08, ECHR 2015, § 101. URL : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159566%22]}
12. Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility. *Journal of Law and Social Policy.* 2025. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.46
13. The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. 2022. SSRN.
14. Алексєєва-Працюк Д. та ін. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. № 2. С. 247–253 DOI: 10.32842/2078-3736/2025.6.59
15. Антонюк А.Б., Русецька В.А. Електронні докази в кримінальному провадженні // *Міжнародний науковий журнал «Інтернаука»*. 2020. № 10. С. 78–87. DOI: 10.25313/2520-2308-2020-10-6437
16. Гутник Х. М., Хитра О. В. Цифрові докази у кримінальному процесі: монографія. Львів: ЛДУВС України, 2022. 248 с.

17. Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерел доказів у кримінальному провадженні. *Криміналістичний вісник*. 2020. № 1. С. 37–49.

18. Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та «протидії кібератакам» від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20

19. Квашук О.Д. Використання електронних доказів у кримінальному провадженні. *Центральноукраїнський вісник права та публічного управління.* Випуск/ Issue 2(10), 2025. С. 50–56. DOI https://doi.org/10.32782/cuj-2025-2-5

20. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.

21. Конвенція про захист прав людини і основоположних свобод від 04.11.1950// URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

22. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 № 185 (ETS № 185). Ратифікована Законом України № 608-III від 21.09.2005.

23. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

24. Липкан І.І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій: дис. … д-ра юрид. наук. Київ, 2025. URL: https://dpu.edu.ua/images/Documents/NAUKA/Doktorski%20specializovani%20vceni%20radi/Specializovana%20vcena%20rada%20D%2027.855.03/Lipkan%20Igor%20Ivanovic/Disertacia%20Lipkana%20I.I.pdf

25. Метелев О.П., Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*. № 1–2, 2023. С. 42–53. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/42-53

26. Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. 2020. № 60. С. 177–181. DOI https://doi.org/10.32782/2307-3322/2020.60.39

27. Метелев О.П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процес. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238. DOI: https://doi.org/10.17721/2413-5372.2019.3/224-238

28. Мілімко Л.В. Електронні докази в кримінальному судочинстві України. *Науковий вісник УжНУ. Серія «Право».* 2025.

29. Петрик В.В. Використання електронних доказів у кримінальному провадженні. *Науковий вісник Ужгородського Національного Університету. Серія «Право»*. Випуск 87: частина 4. (2025). URL: https://visnyk-jurisuzhnu.com/wp-content/uploads/2025/03/19-3.pdf DOI https://doi.org/10.24144/2307-3322.2025.87.4.17

30. Політова А.С., Чехлай Т.О. Допустимість цифрових доказів у кримінальному провадженні: аналіз судової практики. *Вісник МДУ. Серія: Право*. 2025. № 29. С. 104–115. DOI https://doi.org/10.34079/2226-3047-2025-15-29-104-115

31. Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні. *Law and Safety*. 2024. № 2 (93). URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653 DOI: https://doi.org/10.32631/pb.2024.2.13

32. Сіренко О.В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник*. 2019. № 14. С. 208–214.

33. Стефанів Н. Критерії допустимості й достовірності електронних доказів у кримінальному процесі. *Судова влада України*. 2025. https://supreme.court.gov.ua/supreme/pres-centr/news/1751385/

34. Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України // *Проблеми законності.* 2019. № 146. С. 179–191.

35. Шульга В., Калюжна, Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення. *Теорія та практика судової експертизи і криміналістики*. Вип. 3 (40).2025. С. 136–152. DOI: https://doi.org10.32353/khrife.3.2025.10

Information about the author:
Voloshyna Vladlena Kostyantynivna,
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminal Procedure
of the National University "Odesa Law Academy",
23, Fontanska doroga, Odesa, 65009, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-3

ОСНОВИ ПРОЦЕСУ ФІКСАЦІЇ КІБЕРПРАВОПОРУШЕНЬ, ЩО ВПЛИВАЮТЬ НА ЗМІНУ ПСИХІЧНОГО СТАНУ ОПЕРАТОРІВ ЕОМ

Гавриленко Є. В., Саханчук А. Д., Саханчук Т. І.

ВСТУП

Розвиток комунікаційних технологій зумовив багато перетворень у галузі спілкування мільйонів людей. Завдяки широкому та якісному розвитку комп'ютерних технологій людство все більше присвячує свій час життя роботі в соціальних мережах[1]. Серед соціуму виділяється група фахівців системи кібербезпеки, які забезпечують комфорт та безпеку спілкування в ланцюжках інформаційної взаємодії: «людина – комп'ютер – інформаційна мережа – комп'ютер – людина».

Як і багато століть тому, – створювана, збирана, збережена та передана інформація піддається порушенням конфіденційності, цілісності, доступності сукупність яких названі в керівних документах «тріадою CIA»[2].

Правопорушники, які раніше використовували для своїх корисливих цілей матеріально-речові інформаційні канали, з розвитком технологій також перемістили акценти свого негативного впливу на електронну область носіїв інформації. Чим досконаліше розвиваються інформаційні системи, тим витонченішими діють правопорушники.

Перелікам загроз для інформації і її захисту присвячено сотні документів нормативно-правової бази, серед яких закони, постанови Кабінету Міністрів України, галузеві нормативні документи відповідних державних установ, підприємств та організацій, стандарти, кодекси, й ін., як профілактичного, так і «виховного» характеру[3].

Кіберправопорушення є основним деструктивним фактором, що формує сучасні загрози інформаційній безпеці. Їхня «роль» полягає у систематичному та навмисному порушенні властивостей інформації, тобто порушенні її конфіденційності, цілісності та доступності.

Передові країни змушені створювати міжнародні організації задля забезпечення кібербезпеки. Дії користувачів, працівників, програмістів та адміністраторів різного рівня спрямовані на профілактику та протидію кіберправопорушенням.

---

[1] How much time do we spend on social media? Mediakix. 2016. URL: http://mediakix.com/2016/12/how-much-time-is-spent-on-social-media-lifetime/#gs.rPNYGG8

[2] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР

[3] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР; Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII; Про інформацію : Закон України від 02.10.1992 № 2657-XII; Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX.

Список злочинних комп'ютерних технологій впливу на інформацію дуже великий. Він містить багато певних загроз, які можуть призвести не тільки до небажаних втрат, що визнані реалізацією тріади CIA, а й впливати на стан операторів ЕОМ, створюючи умови для реалізації негативних наслідків кіберправопорушень. Чому й присвячена дана наукова робота.

1. Виникнення передумов проблеми та формулювання проблеми

Комп'ютерні технології для роботи з інформацією дозволяють кіберправопорушникам створювати певні загрози, класифікація яких наведена на Рис.1[4].



Рис. 1. Класифікація кіберзагроз інформації

2. Вплив кіберзагроз на операторів ЕОМ

Звісно, що кібератака – це злочин який здійснюється проти широкого спектра цілей – від викрадення даних, для отримання фінансової вигоди, шпигунства або дестабілізації роботи як державних структур, інфраструктури, так й психічного стану окремих громадян.

Європейське дослідження за участю майже тисячі осіб показало: кібератаки спроможні погіршити ментальне здоров'я тих, хто зіткнувся з випадками реалізованих кіберзагроз. Зокрема, йдеться про підвищену тривожність, стрес, гнітюче почуття провини, сором і гнів.

[4] Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2019. с. 128.

Яка саме емоційна реакція може накрити жертву – залежить від типу кібератаки.

Крадіжка CVV-коду картки, злом додатку банку або витік фінансових даних викликають тривогу. Злом акаунта в соціальних мережах з усіма листуваннями і «нюансами» – гнів і відчуття безпорадності. Той, хто повівся на фейкові листи від знайомих (наприклад, «начальник» наказав скинути внутрішні документи компанії), відчуває сором і провину – в першу чергу через ризик нашкодити іншим.

Найгостріші реакції викликають кіберзлочини, пов'язані з чутливою приватною інформацією, – наприклад, крадіжка медичних даних. Жертви таких атак відчувають сильний стрес і втрату контролю над власним життям.

Такі наслідки цілком можна порівняти з емоційними реакціями жертв фізичних злочинів. Коли хтось вривається в приватний інтернет-простір, це мало чим відрізняється від злому і розграбування квартири.

Почуття вразливості і хронічна тривожність після пережитої кібератаки посилюються нездатністю людей ефективно впоратися з її наслідками – багатьом для цього просто не вистачає знань.

Кіберзлочинність має глибокий та багатогранний вплив на психічне здоров'я людини, що класифікується фахівцями як значна публічна загроза. Результати впливу варіюються від легкого стресу до важких клінічних станів.

На основі досліджень, що висвітлюються у контексті цифрової безпеки та ментального здоров'я (зокрема за даними інституцій, що співпрацюють з ВООЗ, наприклад, INTERPOL та UNODC), можна виділити такі основні наслідки: психологічні та емоційні наслідки:

- психологічна травма та симптоми, схожі на посттравматичний стресовий розлад;
- тривога та депресія;
- сором та почуття провини;
- гнів та самоізоляція.

Слід особливо зупинитись на вплив кіберзагроз на стан підлітків та, в цілому, молоді.

Кібербулінг (кіберзалякування) – це систематичне цькування, приниження або залякування людини з використанням цифрових технологій: соціальних мереж, месенджерів, ігрових платформ чи мобільних телефонів. Це умисні дії, спрямовані на створення психологічного тиску, які можуть включати погрози, наклепи, поширення особистих даних, інтимних фото або самозванство.

Дослідження показують, що підлітки, які зазнали кібербулінгу, в 4 рази частіше схильні до самоушкодження або суїцидальних думок, ніж інші.

Більше 45% підлітків, що зазнали кібербулінгу, відчувають безпорадність, а близько 30% – повну самотність.

Зв'язок із загальним станом здоров'я, ВООЗ та партнери наголошують, що кібератаки на медичні заклади (наприклад, лікарні) не лише ставлять під загрозу конфіденційність пацієнтів, але можуть призвести до затримок у лікуванні, створюючи пряму загрозу життю та здоров'ю.

Аналізуючи сказане вище, ми говоримо про наслідки, які потерпілі особи почали відчувати і переживати, як прямий, наочний, видимий негативний

вплив отриманої аудіо та відео інформації з екрана монітора на їхнє психічне здоров'я і, в цілому, на організм, тобто це видимі наслідки, які встановлені.

Однак, кіберзагрози можуть впливати на психіку людину та її поведінку таким чином, що особа не помічає, або не одразу помічає, шкідливий вплив на неї, а також на ті дії чи бездіяльність, які вона буде вчинювати, будучи під негативним, злочинним впливом кіберправопорушника, який може використовувати спеціальні, приховані (непомітні) канали впливу на психіку та поведінку операторів ЕОМ.

В результаті впливу загроз може бути не тільки реалізована тріада CIA, але й змінений стан операторів ЕОМ. При цьому можуть бути створені програмні завади, що «не лише дезінформують операторів, але і й змінюють їх психофізіологічний стан за рахунок потайної дії на них спеціальних оптичних і звукових сигналів»[5]. У більшості випадків, умовно кажучи – звичайно, дія загроз спрямована на напрями, що висвітлені у XVI розділі Кримінального кодексу України (ККУ) як «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»[6].

Щоб не перевантажувати цей матеріал назвами та змістом статей ККУ поставимо питання – «чи містить ККУ інформацію, яка описує покарання кіберправонарушника за злочинний вплив відтворюваної монітором інформації на психофізіологічний стан оператора ЕОМ?».

Відповідь: «Конкретно – ні. АЛЕ, побічно, для вирішення цього питання можна рекомендувати застосування низки статей ККУ».

Конкретизуємо питання: «Чи є злочином навмисний злочинний вплив зображення монітора на оператора ЕОМ»?

Відповідь: «Станом на лютий 2026 року, навмисний вплив зображення монітора на оператора ЕОМ може кваліфікуватися як злочин залежно від наслідків та способу здійснення такого впливу».

Прямої статті з таким формулюванням у Кримінальному кодексі України (ККУ) немає, проте подібні дії підпадають під наступні норми:

1.Кіберзлочини (Розділ XVI ККУ), якщо вплив здійснюється через несанкціоноване втручання в роботу комп'ютера (наприклад, хакерський злам для виведення шкідливого контенту), це порушує Статтю 361 ККУ.

2.Злочини проти життя та здоров'я:

- якщо візуальний вплив (наприклад, стробоскопічні ефекти для виклику епілептичного нападу) спричинив шкоду здоров'ю, дії можуть бути кваліфіковані за статтями про умисне нанесення тілесних ушкоджень (Ст. 121, 122, 125 ККУ);

- у разі доведення до самогубства через психологічний тиск за допомогою зображень – Стаття 120 ККУ;

---

[5] Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2019. с. 129.

[6] Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

- терористичний акт (Стаття 258 ККУ), якщо такі дії мають на меті залякування населення або вплив на прийняття рішень органами влади, вони можуть розглядатися як форма кібертероризму.

Подальший аналіз Кримінального Кодексу України може показати, що в ньому не має прямих статтей, які можливі до застосування по відношенню до кіберправопорушника, який вчинив навмисний, злочинний вплив на оператора ЕОМ, застосовуючи специфічний (прихований) сигнал чи групу різних сигналів через системи інформаційних технологій на потерпілого та його психологічний стан.

Є статті 142, 356 КК України, де перша це незаконне проведення медико-біологічних, психологічних або інших дослідів над людиною, якщо це створювало небезпеку для її життя чи здоров'я, а друга це самоправство, тобто самовільне, всупереч установленому законом порядку, вчинення будь-яких дій, правомірність яких оспорюється окремим громадянином або підприємством, установою чи організацією, якщо такими діями була заподіяна значна шкода інтересам громадянина, державним чи громадським інтересам або інтересам власника.

Що у першому, що у другому випадку із вказаними вище статтями ККУ, вони не містять згадки та можливості впливу на потерпілого за допомогою інформаційних технологій, що унеможливлює її до застосування у разі використання таких технологій на психологічний стан особи.

Окрім того, за відсутності прямої статті в ККУ за протиправні дії кіберправопорушника, які розглядаються в цій роботі, виникають питання щодо збору, фіксації належних та допустимих доказів, які повинні повно, об'єктивно та всебічно вказати на застосування кіберправопорушником злочинного впливу на оператора ОЕМ.

Ще, окрім кримінальної відповідальності, існують суворі гігієнічні вимоги до роботи з моніторами, порушення яких роботодавцем може тягнути адміністративну відповідальність.

Ретельний аналіз змісту статей ККУ 121, 122, 125, 120, 142, 258(1-6), 356 напряму не підпадає під випадки, коли оператор ЕОМ під зовнішнім оптичним впливом починає порушувати правила роботи з комп'ютерними програмними продуктами, робити помилки та порушувати роботу комп'ютерної системи. Тоді, може й не існує негативний вплив зображення на моніторі на роботу оператора ЕОМ?

Для знаходження відповіді по даному питанню, дослідимо напрямки роботи передових колективів комп'ютерних лабораторій світового рівня. При цьому, застосуємо процес спілкування з системами штучного інтелекту.

3. Перелік і зміст роботи світових комп'ютерних лабораторій, які вивчають Penetration testing

Penetration testing (тестування на проникнення) – це санкціонована, контрольована імітація кібератак на ІТ-інфраструктуру, мережі чи програми.

При здійсненні пошуку інформації виявилося, що багато комп'ютерних спеціалістів у світових лабораторіях вже доволі давно та ретельно займаються вивченням ступеню впливу акустичних та оптичних сигналів, що передані по комп'ютерних мережах і відтворені моніторами та акустичними системами на робочих місцях операторів ЕОМ.

У цьому напрямку найбільший розвиток і опис досліджень отримали психолінгвістичні онлайн-експерименти.

Методи дослідження мовленнєвої діяльності сприйняття, засвоєння та вироблення мови, вчені проводять дистанційно через інтернет за допомогою веббраузерів, спеціалізованих платформ або онлайн-форм. Вони дозволяють науковцям збирати дані про роботу мозку при обробці мови («мовні» процеси), часто вимірюючи реакцію респондентів з точністю до мілісекунд.

Про експерименти з оптичним впливом зображень на стан операторів ЕОМ в інтернеті інформація оказалася дуже скудною і обмеженою. Однак, порівняння отриманої «фірмової» інформації зі «сторонньою» інформацію про експерименти в одних і тих же лабораторіях з високим ступенем вірогідності дозволяють спеціалістам (що працюють з ІзОД) зробити висновок, що ця інформація носить закритий характер.

Існують різноманітні типи лінгвістичних та оптичних психічних онлайн-експериментів:

1. Асоціативний експеримент, – виявлення асоціацій, що сформовані попереднім досвідом (наприклад, назвати перше слово, що спадає на думку у відповідь на стимул).

2. Завдання на лексичне рішення (Lexical Decision Task), – учасник на екрані монітора бачить набір букв і має швидко визначити, чи це реальне слово, чи вигадане.

3. Оцінка прийнятності (Acceptability/Grammaticality Judgment), – респонденти оцінюють, чи є речення граматично правильним або природним.

4. Самокероване читання (Self-paced Reading) – учасник читає текст, натискаючи клавішу, щоб побачити кожне наступне слово або фразу, що дозволяє виміряти час обробки кожного елемента.

5. Називання зображень (Picture-naming Task), – учасники бачать зображення і повинні швидко його назвати.

Онлайн-експерименти стали стандартом у дослідженнях мови, особливо після 2020 року, дозволяючи збирати великі масиви даних за допомогою веббраузерів (jsPsych, Labvanced, Gorilla).

4. Провідні дослідницькі центри вивчення дистанційного впливу на психіку оператора ЕОМ

LAELabs – Psycholinguistics Lab (**University of Hawaii**), – спеціалізується на віртуальних дослідженнях того, як мова виробляється, сприймається, розуміється та засвоюється.

Psycholinguistics@York (**University of York, Великобританія**), – проводить широкий спектр поведінкових онлайн-експериментів, у тому числі з використанням методів **eye-tracking** (!) у реальному часі.

Language & Cognitive Neuroscience Lab (**University of Wisconsin-Madison**), – досліджує статистичне навчання, вплив вироблення мови на розуміння та вплив соціолінгвістичних варіацій.

Psycholinguistics Lab (**University of Strathclyde, Великобританія**), – вивчає когнітивні механізми тобто сукупність психічних процесів (сприйняття, пам'ять, мислення, увага), за допомогою яких мозок отримує, обробляє, зберігає та використовує інформацію.

University of Edinburgh (**School of Philosophy, Psychology and Language Sciences**), – дослідники (наприклад, проф. Кенні Сміт) розробляють онлайн-методи (lexical decision tasks, mouse clicks) та навчають проведенню онлайн-експериментів.

University of Cambridge (**Language Sciences**), – активно займається психолінгвістичними дослідженнями, включаючи онлайн-платформи для мовних тестів.

The ELL Psycholinguistics Lab (**University of Wisconsin-Madison**), – використовує онлайн-інструменти для перехресних лінгвістичних досліджень (наприклад, Lexical Decision Task).

Дуже показовим є те, що дані експерименти відносяться до:

1. Когнітивної психології – вивчають, як люди отримують, обробляють, зберігають та використовують інформацію.

2. Психофізіології – вивчають фізіологічні механізми психічних процесів (емоцій, станів, сприйняття).

3.Психодіагностики – якщо це спрямовано на вимірювання та зміну психічного стану.

Ці процеси разом утворюють внутрішній світ людини або її психічну діяльність.

Мультимедійні дослідження дозволяють використовувати звук, **зображення та відео для стимуляції**.

Дуже цікавою є платформа Experiment Builder, що розроблена компанією SR Research Ltd., штаб-квартира якої розташована в Канаді.

Офіси та виробничі потужності компанії знаходяться в Оттава (Канада): головний офіс компанії, Міссісога (Онтаріо, Канада): місце реєстрації та розробки програмного забезпечення, що зазвичай вказується у правилах цитування софту.

Experiment Builder – це **візуальне середовище для створення психологічних та нейрофізіологічних експериментів**, яке найчастіше використовується разом з айтрекерами серії EyeLink, що також виробляються в Канаді. Також існує хмарний інструмент з подібною назвою – Gorilla Experiment Builder, який розроблений компанією Cauldron Science у Великій Британії (Кембридж), – відкіля отримати службову інформацію дуже важко, бо вона знаходиться під зміцненим контролем .

5. Створення та застосування тестерів, що фіксуюсь оптичний вплив на оператора ЕОМ для фіксації цифрових доказів кіберправопорушення

Нагадаємо, що цифрові докази є невід'ємною частиною кримінальних проваджень сьогодення, зокрема у справах, які стосуються сучасних технологій та кіберзлочинів. Ці докази включають цифрову інформацію, залишену на таких приладах як комп'ютери, мобільні пристрої, мережеві журнали та інші ресурси, які здатні відобразити дії суб'єкта або механізми, які можуть вплинути на середовище оператора ЕОМ.

У науковій літературі цифрові докази описуються як електронна інформація, отримана та закріплена таким чином, що її можна легально представити у кримінальному процесі для підтвердження певних обставин справи[7].

Процесуальні вимоги до доказів, у тому числі електронних, формуються під впливом норм Кримінального процесуального кодексу України, які вимагають суворого забезпечення їх належності та достовірності. Саме тому технічно правильне вилучення інформації напряму впливає на можливість її використання у суді.

Правильне трактування цифрових доказів у кримінальному провадженні вимагає глибокого розуміння їх правового статусу та допустимості. У національній практиці тривають дискусії щодо допустимих меж втручання у приватне життя, порядку отримання інформації з віддалених сервісів, а також щодо можливості використання копій замість оригінальних джерел[8].

Як приклад оптичного впливу візуальних образів, з якими може зустрітися людина у житті, можна назвати лікувальний (або кримінальний…) гіпнотичний вплив на поведінку людини частини візуальних елементів такої науки як «Нейро-Лінгвістичне Програмування» (NLP), що є набором психологічних технік, які дозволяють впливати на думки і поведінку людей, змінюючи її не тільки тут та зараз, а й на майбутні моменти життя.

NLP це дистанційно-контактне програмування підсвідомості для зміни поведінки людини за допомогою мови та вербальних сигналів (в оптичному диапазоні): жестів, міміки… . Зрозуміло, що керуючі сигнали кожна людина по-своєму отримує і розуміє інформацію з каналу звуку та каналу зору. І тут очі є не тільки першим «функціональним блоком» на шляху прийому відео-інформації, але й дуже якісним індикатором зовнішнього впливу, що дозволяє контролювати і програмувати стан підсвідомості людини.

Ремарка 1. Таким чином, проміжним висновком є першим функціональним елементом, що дозволяє контролювати психологічний стан підсвідомості оператора ЕОМ, фіксуючи звичайну швидкість та напрями рухів патерн очей («очних яблук») оператора. Як було наведено раніше, для цього можуть бути застосовані:

---

[7] Електронне наукове видання «Аналітично-порівняльне правознавство». URL: http://journal-app.uzhnu.edu.ua/article/view/334687

[8] Сутність цифрових доказів і проблеми їх використання у кримінальному провадженні. URL: https://dspace.nlu.edu.ua/handle/123456789/20503

1. Стаціонарні айтрекери що розміщуються під монітором комп'ютера.

2. Айтрекери-окуляри (мобільні).

3. Веб-камери. Вони дозволяють проводити масові дистанційні дослідження, але з нижчою точністю.

В схожій науці дистанційного нейрокольороводинамічного програмування **(NCDP)** підсвідомості людини – в основу покладено наявність нейрон-фізіологічного зв'язку між впливом (причиною) навколишнього фону (наприклад, – непомітна зміна динаміки та кольорового змісту зображення на екрані комп'ютерного монітору) на підсвідомій зміні поведінки (дій) та/або стані людини.

Безліч психологічних характеристик сигналів для дистанційного програмування поведінки людей описуються по-різному. Далі ми торкнемося такої спектральної характеристиці сигналів, як довжина хвилі світла, що попадає на сітківку очей людини. Звісно, що диференціальні компоненти кольору джерела світла впливають на очі людини. Причому, на відміну від роботи Gabriel Kreiman, що спирається у своїх міркуваннях на відбите від предметів світло, а саме: «…Світло потрапляє на сітківку після того, як відбивається об'єктами довкілля…»[9], – ми звернемо увагу на інше джерело, яке на нашу думку має здібність дистанційно впливати та змінювати поведінку людини. Реально, – це групи фотонів з екранів моніторів, світлодіодних матриць, різноманітних сканерів, проекторів та й т. ін., що безпосередньо «породжуються» самим джерелом випромінювання і «відсвітлюють» предмети оточуючого середовища.

Наприклад, колір екрану монітору комп'ютера, з яким ми працюємо кожен день , звичай має більш сотні відтінків – від білого, світло-сірого до темного. І на тлі тих кольорів ми бачимо малюнки, тексти і багато чого іншого (Рис. 2). І всі ті відтінки на Рис. 2 визначені зазвичай як – «білий, світлий».

Світлова інформація досягає ока через лінзу кришталика (Рис. 3). Коли світло досягає фокальної площини, що збігається з положенням сітківки, зображення перевертається (на 180°). Сітківка є частиною центральної нервової системи: вона походить з тих же ембріональних структур, які дають початок решті мозку, і вона має гематоенцефалічний бар'єр, аналогічний такому ж як у решти мозку.

Світло проходить через безліч клітин ока і потрапляє на фоторецептори: палички та колбочки. Загалом у людини близько 10^{8} паличок та 10^{7} колбочок.

Палички дуже чутливі до світла та призначені для уловлювання фотонів в умовах низького освітлення. Нічне бачення залежить від паличок. Палички можуть захоплювати одиночний фотон видимої частини спектру, енергія якого становить лише близько 10^{-19} Дж, і передавати його енергію далі. Доказано, що люди можуть реєструвати одиночні фотони[10].

[9] Крейман Г. Біологічний та комп'ютерний зір / пер. з англ. И. Л. Люско ; під ред. Т. Б. Кіселевої. Москва : ДМК Пресс, 2022. 314 с.

[10] Там само.

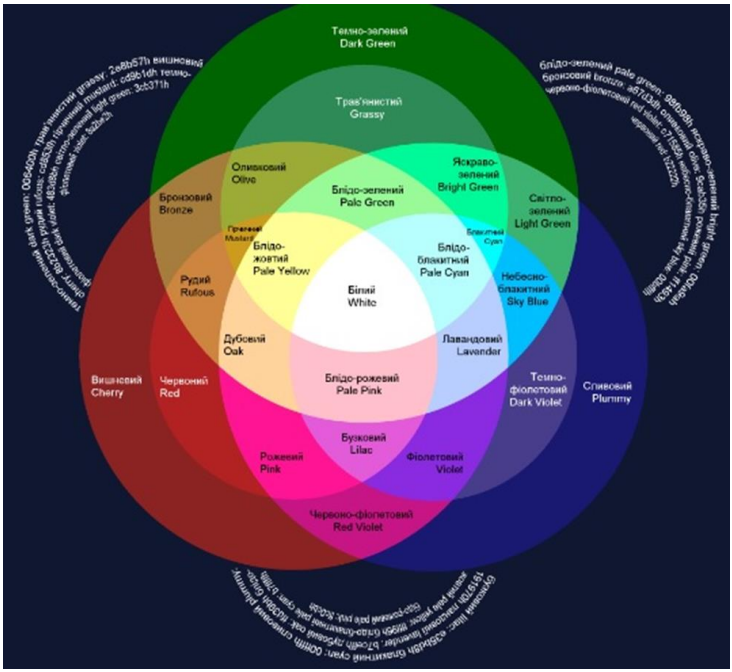


Рис. 2. Біла пляма в центрі, є інтегральним результатом реакції мозку на стимуляцію нейронів фотонами різних довжин хвиль [поширено в Інтернеті]

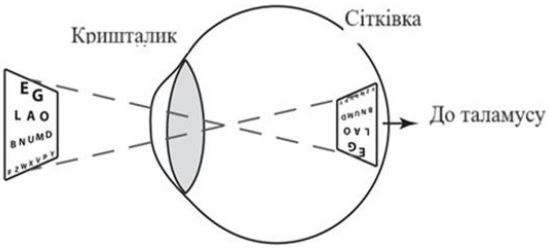


Рис. 3. Деякі функціональні елементи ока людини

У більшості людей є три типи колбочок: – довгохвильові, чутливі до довжини хвилі світла з максимумом 560 нм (жовто-зелений колір); – середньохвильові, чутливі до діапазону з максимумом 530 нм (зелений колір); – короткохвильові, чутливі до діапазону з максимумом 420 нм (фіолетовий колір). Колірний зір залежить від активності колбочок[11]».

Розуміючи схожість нейрофізіологічних зв'язків **NLP** та **NCDP** має сенс показати схожості у вигляді функціоналів, як це наведено на Рис. 4.

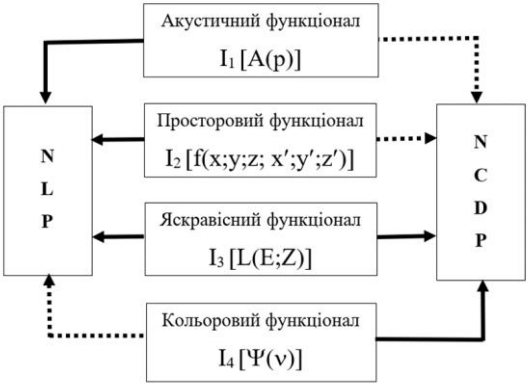


Рис. 4. Задіяність функціоналів в NLP та NCDP

Зорові нейрони тримають під контролем певну область поля зору, в якій, як доказує експеримент, вони **реагують ще на щось крім зміни візерунків**, руху предметів, та їх яскравості. Як ми розуміємо, це реакція нейронів на будь-які зміни у спектральному складі світлового потоку, що впливає на них, тобто йдеться про реакцію на динаміку змін у спектральному складі випромінювання що впливає на нейрони сітківки.

Таким чином, ретельно вивчаючи роботу Gabriel Kreiman, можна виявити, що зір людини працює не тільки на стимулюючи елементи впливу в NLP.

Зафіксовано, що нейрони головного мозку, гангліозні клітини сітківки, під час експерименту з фіксацією активності нейронів «ніби так» видають у мозок якісь сигнали, які при незнанні подразника можна класифікувати як випадкові. Ці «безпричинні» сигнали виробляються настільки часто, що їх стали ігнорувати, розмовляючи про випадкові імпульси від збудника (подразника) невідомого походження.

Іншими словами, «якщо порівняти нейрон з пороговим пристроєм, його спрацьовування не обов'язково відсутнє за відсутності зорової просторової стимуляції в межах рецептивного поля…»[12].

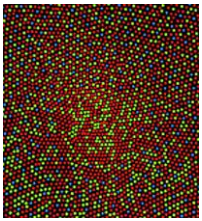
[11] Крейман Г. Біологічний та комп'ютерний зір / пер. з англ. И. Л. Люско ; під ред. Т. Б. Кіселевої. Москва : ДМК Пресс, 2022. 314 с.

[12] Там само.

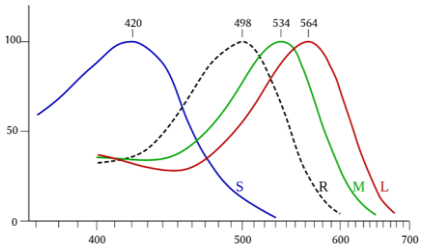
На превеликий жаль, сучасні технології дозволяють одночасно реєструвати діяльність лише кількох сотень вихідних нейронів сітківки, але й така кількість підконтрольних нейронів доказує реальну можливість здійснення **NCDP**.

6. Вплив компонентів білого кольору на психічний стан оператора ЕОМ через підсвідомість мозку

Таким чином знаючи, що, колбочки відповідальні за кольоровий зір, звернемо увагу на їх розташування на сітківці здорової людини (Рис. 5)[13].



а) Розташування в фоторецепторних клітин



б) Чутливість фоторецепторних клітин

Рис. 5. Розподіл колбочкових клітин у центральній ямці сітківки ока людини з нормальним колірним зором

Основна небезпека для людини зберігається у суміші кольорів що надають оператору ЕОМ відчуття білого екрана на тлі якого розміщують інформацію різного конфіденційного змісту – тексти, таблиці та ін. (Рис. 6).

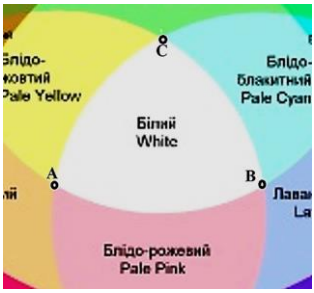


Рис. 6. «Вирізка» білої ділянки з Рис. 2

Якщо в процесі роботи правопорушник отримає можливість (а таких місць на протязі комп'ютерної мережі мінімум чотири) навмисно змінювати насиченість білої ділянки ABC, варіюючи кількість та розташування на екрані монітору

[13] Сітківка. Вікіпедія. URL: https://uk.wikipedia.org/wiki/сітківка

кольорових компонентів білого «кольору», то незалежно від бажання оператора ЕОМ та його психічного настрою, нейрони будуть постачати оператору у головний мозок інформацію, як мінімум, – о насиченості білої ділянки червоним, синім та зеленим світлом, бо в інтегральному ракурсі ця біла пляма (фон екрана) має непримітне для очей «мерехтіння». Оператор ЕОМ підсвідомо буде знаходитись під впливом комп'ютерних зображень фону екрана.

Ремарка 2. Доволі ефективні та корисні прилади застосовує в цьому напрямі фірма Optopol[14], що вивчає та лікує зір людини. Сучасний автоматичний комп`ютерний «периметрометр» використовується офтальмологом для визначення полів зору і перевірки порогової чутливості сітківки ока. Периметрія – це інструментальний метод діагностики в офтальмології, який дозволяє визначати межі полів зору і найменше їх відхилення від встановлених норм на самих ранніх стадіях, а також зафіксувати результати у вигляді діаграм, графіків та трьохвимірного зображення. Образи, що створюються на апаратурі фірми Optopol, застосовують об`єкти різного розміру та яскравості, тобто застосовується тільки просторовий і яскравісний функціонали **NCDP**.

ВИСНОВКИ

Проведене дослідження показало наступне.

1. У Кримінальному Кодексі України покарання кіберправопорушників за дії що спрямовані на негативний дистанційний вплив загроз на персонал, – оператора ЕОМ, адміністраторів та ін. – розглядаються лише побічно.
2. Прилади щодо фіксації та збору цифрових доказів такого роду кіберправопорушень знаходяться в стані розробки багатьма ведучими фірмами в системи кібербезпеки і охороняються та зберігаються на рівні ІзОД.
3. Кіберправопорушник має можливість не тільки змінювати фон в інтегральному розумінні цього процесу, але в диференціальному ракурсі має можливість створювати непомітні для зору, але-ж суттєві для підсвідомості, динамічні образи (і відео-елементи, які можуть бути корельованими з конкретними життєвими «сюжетами» оператора), що дозволяє дистанційно впливати на поведінкові реакції персоналу ЕОМ.
4. Створення тестерів для проведення тестінгу на проникнення одночасно з функціями виявлення, фіксації та збору цифрових доказів кіберправопорушень є актуальною задачею професіоналів системи кібербезпеки.

АНОТАЦІЯ

У статті досліджуються механізми прихованого дистанційного впливу на психофізіологічний стан оператора ЕОМ через оптичні та акустичні сигнали. Проаналізовано стан сучасної нормативно-правової бази України щодо кваліфікації таких дій як кіберзлочини та визначено відсутність прямих норм, які б могли описати покарання за навмисний візуальний вплив на здоров'я людини.

Розглядається концепція дистанційного нейрокольороводинамічного програмування (NDCP) підсвідомості, що базується на нейрофізіологічному

[14] Optopol Technology. URL: https://optopol.com/

зв'язку між спектральним складом випромінювання екрана та зміною поведінкових реакцій людини. Описано роль фоторецепторів сітківки у сприйнятті поодиноких фотонів та динамічних змін фону екрана, які можуть бути непомітними для свідомості, але суттєвими для підсвідомості.

Окрему роль приділено світовому досвіду проведення психолінгвістичних експериментів та використанню технологій eye-tracking для фіксації змін у стані оператора. Обґрунтовано актуальність створення спеціалізованих тестерів для виявлення та збору цифрових доказів таких правопорушень у системах кібербезпеки.

ABSTRACT

The article explores the mechanisms of covert remote influence on the psychophysiological state of a computer operator through optical and acoustic signals. The current state of Ukraine's regulatory and legal framework regarding the classification of such actions as cybercrimes is analyzed, identifying a lack of direct norms that could describe the punishment for intentional visual impact on human health.

The concept of remote Neuro-Color-Dynamic Programming (NCDP) of the subconscious is examined, based on the neurophysiological connection between the spectral composition of screen radiation and changes in human behavioral reactions. The role of retinal photoreceptors in perceiving single photons and dynamic changes in the screen background, which may be invisible to the conscious mind but significant for the subconscious, is described.

Special attention is paid to global experience in conducting psycholinguistic experiments and the use of eye-tracking technologies to record changes in the operator's state. The urgency of creating specialized testers for detecting and collecting digital evidence of such offenses within cybersecurity systems is justified.

Література

1. How much time do we spend on social media? *Mediakix*. 2016. URL: http://mediakix.com/2016/12/how-much-time-is-spent-on-social-media-lifetime/ #gs.rPNYGG8.

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII.

4. Про інформацію : Закон України від 02.10.1992 № 2657-XII.

5. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX.

6. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин : ФОП Лук'яненко В. В. ; ТПК «Орхідея», 2019. 144 с.

7. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

8. Електронне наукове видання «Аналітично-порівняльне правознавство». URL: http://journal-app.uzhnu.edu.ua/article/view/334687.

9. Сутність цифрових доказів і проблеми їх використання у кримінальному провадженні. URL: https://dspace.nlu.edu.ua/handle/123456789/20503.
10. Крейман Г. Біологічний та комп'ютерний зір / пер. з англ. И. Л. Люско ; під ред. Т. Б. Кіселевої. Москва : ДМК Пресс, 2022. 314 с..
11. Сітківка. Вікіпедія. URL: https://uk.wikipedia.org/wiki/сітківка.
12. Optopol Technology. URL: https://optopol.com/.
13. Гавриленко Є. В. NCDP – neurocolordynamic programming. Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realtà domestiche : raccolta di articoli scientifici «ΛΌΓΟΣ» con gli atti della VIII Conferenza scientifica e pratica internazionale (Bologna, 19 Dec. 2025). Bologna ; Vinnytsia, 2025. С. 138–146. DOI: 10.36074/logos-19.12.2025.025.

Information about the authors:
Gavrylenko Yeva Vladyslavivna,
Software Engineer – Bachelor's Degree of the Educational and Research Institute Computer Sciences and Artificial Intelligence of Department of Security of Information Systems, Networks & Technologies,
V.N. Karazin Kharkiv National University
6, Svobody Sq., Kharkiv, 61022, Ukraine

Sakhanchuk Andrii Dmytrovych,
Attorney in criminal law and procedure
Chairman of the Law Firm, Kyiv, Ukraine

Sakhanchuk Tetiana Ihoryvna,
Attorney at law, Kyiv, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-4

ГОЛОВНИЙ ЗАКОН ЗАХИСТУ ІНФОРМАЦІЇ

Громико І. О.

ВСТУП

Сучасна ситуація в галузі захисту інформації така, що спроби спиратися на деякі суттєві терміни, що використовуються в законах, постановах, підручниках та навчальних посібниках із захисту інформації іноді призводять до розмитості розуміння реальних процесів інформаційної діяльності. В результаті, упускаються з першого погляду «дрібні» нюанси інформаційної термінології, які надалі породжують непорозуміння серед адміністраторів та операторів ЕОМ, володарів та користувачів інформацією, що виконують свої обов'язки, знаходячись у різноманітних ланцюгах інформаційної взаємодії.

Як мінімум, такий стан розвитку інформаційних технологій створив тупикові ситуації для людей що познають основи інформаційної безпеки – працівників служб служби безпеки, студентів, та ін. Взагалі, це гальмує процес вивчення і розвитку широкого тематичного спектру діяльності носіїв інформації сучасного інформаційного простору[1].

Стан такої ситуації протягом великого тимчасового періоду (десятки років…!) переконав автора в необхідності проведення нового етапу досліджень, у ході яких було виявлено декілька суттєвих "прогалин" у інформаційної теорії взаємодії носіїв інформації. Особливо це мало відношення до забезпечення безпеки інформації в умовах різноманітних загроз. Частина цих загроз була породжена відмінностями режимів комунікабельності носіїв інформації. Саме ці питання на цей момент залишаються невивченими або невирішеними при здійсненні інформаційної діяльності.

Метою дослідження є формулювання головного закону захисту інформації на підставі аналізу інформаційної діяльності носіїв інформації в умовах впливу інформаційних загроз.

Унікальність отриманих результатів підтверджена патентами України[2,3,4,5]. Вже зараз 20.02. 2026 року в допомогу збройним силам розроблені основи реалізації способу та застосуванню приладу принципово нової військової техніки і подані заявки на отримання патентів України.

---

[1] Громико І.О. Загальна парадигма захисту інформації: проблеми захисту інформації в аспектах математичного моделювання : монографія. Харків : ХНУ ім. В.Н.Каразіна, 2014. 216 с

[2] Спосіб знешкодження вибухового пристрою : пат. Україна : МКП F42D 5/04. № 7238 ; заявл. 11.08.2006 ; опубл. : 15.06.2005, Бюл. № 5

[3] Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. № 32620 ; заявл. 26.05.2008 ; опубл. : 26.05.2008, Бюл. № 10

[4] Там само.

[5] Там само. № 114388 ; заявл. 11.08.2006 ; опубл. : 10.03.2017, Бюл. № 5.

Велика кількість доповідей на міжнародних та вітчизняних конференціях, секцій що присвячені захисту інформації.

Автор мінімізував кількість застосованих інформаційних джерел, яких в оригіналі роботи більш 80-ти, та прикладів практичного застосування досліджень, в тому числі – рекомендацій та патентів як для захисту інформації в службових кабінетах, так й для застосування в діючих підрозділах збройних сил України.

Дослідження проводилися на території кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту ХНУ ім. В.Н.Каразіна, інших факультетів та кафедр, та у дружніх наукових центрах Харкова. Особливу подяку автор висловлює колективу «Харківського регіонального науково-виробничого центру стандартизації, метрології та сертифікації», що дозволило суттєво підвищити якість науково-практичних досліджень автора у галузі інформаційної радіофізики.

В результаті багаторічних досліджень, включаючи експерименти, автором сформульований «Загальний закон захисту інформації»:

«Інформація вважається захищеною, якщо під час здійснення інформаційної діяльності обов'язково і одночасно виконуються дві головні вимоги до інформаційних ланцюгів взаємодії носіїв інформації:

1) «режимна адекватність» носіїв інформації;

2) «режимна комунікабельність» носіїв інформації» (UA).

"Information is considered protected if, during the implementation of information activities, two Key (Primary, Core and Basic) requirements for information chains of interaction of information carriers are necessarily and simultaneously fulfilled:

1) "regime adequacy" of information carriers;

2) "regime communicability" of information carriers." (ENG).

1. Інформаційна діяльність носіїв інформації

При проведенні науково-дослідницьких робіт автор використовував керівні та науково-інформаційні державні довідники, документи та рекомендації сайтів штучного інтелекту. Тому посилання на джерела в даному випадку не приведені.

1.1. Деякі визначення та термінологія

Інформація – це зафіксоване носієм, та на носії, уявлення про предмети, процеси, події, природні явища (тощо) як відображення реального світу.

Інформація завжди знаходиться з носієм та завжди має свою цінність, бо нейтральної інформації не існує.

Відомості – це будь-які дані, повідомлення, факти або інформація про осіб, події, явища, процеси чи предмети, які можуть бути зафіксовані носіями або на матеріальних носіях.

Дані (data) – це формалізоване подання фактів, чисел, понять або інструкцій, зафіксоване на носії (або в пам'яті комп'ютера), яке придатне для оброблення, передавання або інтерпретації людиною чи автоматичними системами. У комп'ютерних науках (IT): дані – це формалізоване подання

інформації, придатне для інтерпретування, пересилання чи оброблення за допомогою автоматичних засобів або людини (згідно зі стандартом ISO/IEC 2382:2015).

Об'єкт захисту – це об'єкт, який підлягає захисту від негативних дій «джерела загроз». Джерело загроз умисно або випадково здійснює чи планує напад/вплив на об'єкт захисту. В нашому ракурсі досліджень ми під «об'єктом захисту» розуміємо інформацію, інформаційні та інші процеси що застосовують при здійсненні інформаційної діяльності (або здійснюються згідно завданих програм) у ланцюгах інформаційної взаємодії носіїв інформації, які необхідно захищати відповідно до мети цифрової безпеки

Захист – це дія за значенням не допустити впливу на «об'єкт захисту» загрозам, які мають на меті запобігти порушенням прав будь-кого.

Метою захисту інформації є унеможливлення або суттєве утруднення реалізації загроз для інформації, що є власністю держави, сприяння реалізації законних інтересів та прав фізичних і юридичних осіб, державних органів здійсненню ними своїх завдань і функцій, а також загроз, реалізація яких може нанести державі, суспільству або особі політичні, економічні, моральні та інші збитки. Метою захисту інформації є забезпечення її конфіденційності, цілісності та доступності (тріада CIA: Confidentiality, Integrity, Availability). Це комплекс заходів для запобігання несанкціонованому доступу, викраденню, знищенню, модифікації або витоку даних, що мінімізує ризики та збитки для користувачів, компаній або держави.

Поняття: «володілець», «володар», «власник», або «загрози інформації», «загрози для інформації», «інформаційні загрози» та «кіберзагрози» повинні розглядатися з повним надаванням змісту та суворим відстежуванням інформаційних **причинно-наслідкових зв'язків** між авторами, власниками, володільцями, володарями та користувачами щодо наслідків інформаційної діяльності в ланцюжках взаємодії носіїв.

Загроза (англ. threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Кібератака (англ. cyber-attack) – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

1.2. Режимна адекватність носіїв інформації

На протязі багатьох років та на конкретних прикладах практика доводить, що постійно у ланцюгах інформаційної взаємодії носіїв інформації «чогось не вистачає», якихсь елементів чи додаткових дій у системах захисту інформації. У всіх державах світу фахівцями систем захисту інформації повністю не враховані деякі динамічні зовнішні чи внутрішні чинники, яким спочатку не надають істотного значення і які в реальних ситуаціях починають превалювати за значимістю над застосованими сучасними методами та засобами захисту інформації.

Внаслідок цього – загрози щодо інформації «успішно» реалізуються конкурентами, розвідувальними службами іноземних держав, терористами та ін.

Попередньо назвемо ці чинники. До таких належать:

- режимна адекватність носіїв інформації;
- комунікабельність носіїв інформації.

Режим, це передбачений правовими нормами доступ/взаємодія носіїв до інформації в процесі: створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації[6].

Адекватність – від лат. adaequatus – прирівняний, рівний.

Режимна адекватність носіїв інформації – це відповідність режимів допуску всіх носіїв інформації за їх взаємодії. Під взаємодією слід розуміти здійснення носіями будь-яких видів інформаційної діяльності.

Режим захисту інформації це система заходів, правил, запроваджуваних для досягнення мети захисту інформації.

Звернемо увагу на класифікацію інформації згідно доступу. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Таємна інформація, або «державна таємниця» – вид інформації, що охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення яких може завдати шкоди життєве важливим інтересам України і які визнані у порядку, встановленому законом, державною таємницею та підлягають охороні з боку держави[7,8].

---

[6] Про інформацію : Закон України від 2 жовтня 1992 р. № 48 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.03.2026)

[7] Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII / Верховна Рада України. URL : https ://zakon.rada.gov.ua/laws/show/ 3855-12#Text; Наказ служби безпеки України № 383 від 23.12.2020р. (Редакція станом на 09.09.2024)

[8] Наказ служби безпеки України № 383 від 23.12.2020р. (Редакція станом на 09.09.2024)

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

Службова інформація може міститися лише в документах суб'єктів владних повноважень, визначених у статті 13 Закону України «Про доступ до публічної інформації», що стосується їх діяльності. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування» (ДСК). На документах, що містять службову інформацію з:

- мобілізаційних питань, додатково проставляється відмітка "Літер "М";
- питань криптографічного захисту службової інформації, – відмітка "Літер "К";
- питань спеціальної інформації, – відмітка "СІ".

Категорії документів, на яких проставляється відмітка "Літер "К", визначаються нормативно-правовими актами Адміністрації Держспецзв'язку.

Забороняється використовувати для передачі службової інформації відкриті канали зв'язку.

Закон України «Про доступ до публічної інформації», зокрема стаття 9, окреслює коло інформації, яка може належати до категорії «службова»:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Отже, якщо інформація належить до вказаного кола, вона може отримати статус «службової».

Належати до службової така інформація може відповідно до вимог частини другої статті 6 Закону України «Про доступ до публічної інформації», тобто після застосування так званого «трискладового тесту». Так, обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Доступ до службової інформації обмежується лише за умови наявності всіх трьох вимог. При відсутності хоча б однієї з них інформація є відкритою (частина 2 статті 6 Закону України «Про доступ до публічної інформації»).

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

2. Комунікабельність як об'єднуючий універсальний термін

Збирання інформації є інформаційним аналогом її отримання особисто чи/та за допомогою технічних систем, яким відведено одну з провідних ролей у будь-яких видах інформаційної діяльності. Найбільш ємне і майже безпомилково цей інформаційний процес здійснює комп'ютерна система з елементами штучного інтелекту (***ШІ***).

Процес збору інформації супроводжується пошуком, оцінюванням, смисловим фільтруванням, приведенням у форму, зручну для подальшого використання, та іншими діями, які неможливі без здійснення **комунікацій** – початкового процесу обміну інформацією між носіями.

Повсякденне тлумачення терміну «**комунікації**» легко простежити у довідковій літературі.

У тлумачному словнику В. І. Даля (1881) слово «комунікація» тлумачилося як «шляхи, дороги, засоби зв'язку місць». Саме у цьому сенсі уродженець Полтавської області М. В. Гоголь писав: «Невський проспект є загальна комунікація Петербургу». Комунікація (від лат. communicatio – єдність, передача, з'єднання, повідомлення, пов'язане з дієсловом лат. communico – роблю спільним, повідомляю, з'єдную, похідним від лат. communis – спільний) – це процес обміну інформацією (фактами, ідеями, поглядами, емоціями тощо) між особами та системами з елементами штучного інтелекту (ШІ), спілкування за допомогою вербальних і невербальних засобів із метою передавання та одержання інформації.

Різноманітні види й способи комунікації можна поділити на три групи: усну, письмову й візуальну.

Далі ми розглянемо парадігмальне тлумачення терміну «комунікація».

Термін «комунікація» використовується багатьма суспільними, біологічними, технічними науками, і найчастіше мають на увазі елементарну схему комунікації (Рис. 1).



Рис. 1. Елементарна схема комунікації

Елементарна схема показує, що комунікація передбачає наявність щонайменше трьох учасників: носій – передавальний об'єкт (комунікант), носій (з повідомленням), носій – приймаючий об'єкт (реципієнт).

На відміну від елементарної парадігмальна схема (Рис. 2) передбачає наявність носіїв інформації, які комунікабельні настільки, що при переміщенні інформації з одного носія на інший загрози інформації не реалізуються і вона зберігає свої властивості: конфіденційність, цілісність та доступність.



Рис. 2. Парадігмальна схема комунікацій

В обох схемах ми спрощено не показує мо джерела завад (шуму та ін.).

Комунікація – це різновид інформаційної взаємодії між носіями. Для відмежування комунікації з інших інформаційних процесів покажемо її відмітні ознаки. Учасниками комунікації можуть бути:

- представники соціуму – окрема людина або група людей аж до суспільства в цілому (а також тварини – зоокомунікація);
- елементи техносфери – «технічні засоби прийому, передачі, обробки, зберігання і т. д. інформації» (далі, – ТЗПІ), а також «допоміжні технічні засоби та системи» (далі, – ДТЗС);
- програмні інформаційні продукти як об’єкти інтелектуальної діяльності, що використовуються спільно з ТЗПІ та ДТЗС.

Хтось з носіїв є джерелом, хтось – одержувачем інформації або обмін інформацією є «взаємним».

Комунікації властива доцільність чи функціональність.

Доцільність може виявлятися у кількох формах:

- переміщення носія з інформацією у геометричному просторі «з пункту А до пункту В» – у цьому полягає мета транспортної чи енергетичної комунікації;
- мета взаємодіючих носіїв полягає не тільки в обміні матеріальними предметами (конверти з листами, магнітні диски або електронні флеш-носії), а й у повідомленні один одному сенсів («смислів»), що мають особливу (смислову) природу (якісна чи смислова характеристика інформації). Носіями смислів є знаки, символи, тексти, що мають зовнішню, чуттєво сприймається форму і внутрішній умоглядний зміст. Можна дати ще одне загальне тлумачення: комунікація є опосередкована та доцільна взаємодія у просторі та в часі.

Залежно від знаходження носіїв у просторово-часовому континуумі слідує типізація комунікації, представлена на Рис. 3.

Як правило, процес переміщення інформації супроводжується узгодженням, яке включає процес приведення зібраної інформації до стандартів, розроблених для даного класу систем. Інакше без стандартизації позитивний результат процесу одержання (збору) інформації стає проблематичним.

Комунікація		
Технічна	**Соціальна**	**Логічна**
технічний, енергетичний, фізичний і т. п. типи.	смисловий, чуттєвий, психічний, технічний, енергетичний, фізичний і т.п. типи.	кодування, шифрування, кількісний, якісний і т. п. типи.

Рис. 3. Типізація комунікації

У плані інформаційної безпеки стандартизація як вид інформаційної діяльності має кінцеву мету встановлення для носіїв інформації норм, правил, характеристик та ін., які знижують ймовірність реалізації загроз для інформації шляхом забезпечення соціальної, технічної та логічної (семантичної, мовної) сумісності носіїв інформації.

Закон України показує цей процес у більш узагальненому вигляді: «Стандартизація – діяльність, що полягає в установленні положень для загального та неодноразового використання щодо наявних чи потенційних завдань і спрямована на досягнення оптимального ступеня впорядкованості у тому числі й задач інформаційної безпеки»[9].

В останні кілька років багато хто почав говорити про сумісність як інтероперабельність. Питання навіть виносилося на обговорення у міжнародних організаціях та на політичній арені. Як результат, отримано більш чітке визначення термінів в дослідженні IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens)[10].

«Інтероперабельність – це здатність інформаційних та комунікаційних технологій та бізнес-процесів, які ними підтримуються, до обміну даними та забезпечення обміну інформацією та знаннями».

1. Організаційна сумісність (соціальна, – авт.).

Сюди належить визначення бізнес-цілей, моделювання бізнес-процесів та забезпечення співпраці установ, які бажають обмінюватися інформацією (можуть мати відмінності у внутрішніх структурах та процесах).

2. Семантична сумісність (логічна, мовна).

Забезпечує зрозумілість процесу обміну інформацією для інших програм, які спочатку не були розроблені для цієї мети. Семантична сумісність дозволяє

[9] Про стандартизацію. Закон України від 5 червня 2014 року № 1315-VII Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/1315-18#Text

[10] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) [Official Journal L 144 of 30 April 2004]. https://www.ab.gov.tr/files/tarama/tarama_files/10/SC10EXP_ IDABC.pdf

об’єднати отриману інформацію з іншими інформаційними ресурсами для подальшої обробки. Як приклад семантичної сумісності браузерів показано Таблицю 1, яка не потребує додаткових пояснень сумісності[11].

Таблиця 1

Підтримка браузерами семантичних елементів

Браузер	IE	Firefox	Chrome	Safari	Opera	Safari iOS	Android
Мінімальна підтримувана версія	9	4	8	5	11.1	4	2.1

3. Технічна сумісність

Сюди входять технічні аспекти сумісності комп’ютерних систем та сервісів, такі як: відкриті інтерфейси, сервіси обміну інформацією, інтеграція даних та програмного забезпечення, подання даних, доступність та служби безпеки.

Таким чином, – комунікабельність (від пізньолат. communicabilis – сполучний, сполучений): 1) сумісність (здатність до спільної роботи (взаємодії – Авт.)) різнотипних систем передачі; 2) здатність до спілкування, товариськість.

Якщо порівняти смислове значення термінів «інтероперабельність» та «комунікабельність», то стає видно смислову ширину другого терміну, який охоплює всі три сторони терміну «сумісність». Одночасно комунікабельність узагальнено охоплює значення терміну «узгодженість» з такими його синонімами, як: узгодженість, злагодженість, струнікість; сумісність, несуперечність, контактність та ін.

Частота застосування терміну «комунікабельність» становить приблизно 30 відсотків у загальній лексиці, психології та автоматиці третину від загальної кількості застосувань. Тільки у медицині вона складає 8 відсотків від всіх термінів.

З огляду на те, що людина є носієм інформації, часто застосовують термін «сприйняття» інформації, що охоплює технічну сферу та сферу соціуму.

Сприйняття – процес перетворення відомостей у технічну систему чи живий організм із зовнішнього світу, у форму, придатну до подальшого використання. Розрізняють статичне та динамічне сприйняття

Сучасні інформаційні системи створюються, зазвичай, з урахуванням комп’ютерів і через складності мають розвинену систему сприйняття. Штучно – інтелектуальне (ШІ) сприйняття інформації представляє досить складний комплекс програмних та технічних засобів. Для розвинених систем сприйняття можна виділити кілька етапів переробки інформації, що надходить: попередня обробка для приведення вхідних даних до стандартного для даної системи виду, виділення в інформації вступників семантично і прагматично значущих інформаційних одиниць, розпізнавання об’єктів і ситуацій, корекція

[11] Браузерна сумісність семантичних елементів. [Електронний ресурс]. URL : http://professorweb.ru/my/html/html5/ level1/1_7.php

внутрішньої моделі світу (та ін.) від датчиків (сенсорів, аналізаторів), що входять до комплексу технічних засобів системи сприйняття, організується сприйняття зорового, акустичного та інших видів інформації.

Таким чином, можна стверджувати, що у певних випадках синонімами терміну «комунікабельність» є: узгодженість, сумісність, злагодженість, інтероперабельність, комунікативність та багато інших, що належать до сфер соціальних, технічних та/або логічних контактів. Застосування терміну «комунікабельність» найбільш ємне охоплює сфери сумісності інформаційних взаємодій носіїв інформації.

3. Класифікація «комунікабельності носіїв інформації»

Зрозуміло, що:

- комунікабельні носії інформації – це носії інформації які здатні до безпомилкової взаємодії:
- комунікабельність носіїв інформації – це здатність носіїв інформації брати безпомилкову участь у інформаційних процесах;
- режимна комунікабельність носіїв інформації – це здатність носіїв інформації брати безпомилкову участь (тобто з унеможливленням реалізації загроз інформації) у інформаційних процесах.

Існують і проміжні носії між носієм-джерелом і носієм-отримувачем інформації. Вони, та й весь їх інформаційний ланцюжок, так само, як і «носій-джерело та носій-отримувач», повинні відповідати вимогам комунікабельності.

Порушення комунікабельності перериває дозволені (санкціоновані) режимом доступу процеси переміщення інформації. Інформація зберігає конфіденційність, цілісність та доступність, якщо зберігається комунікабельність всього інформаційного ланцюга носіїв інформації за їх взаємодії між джерелом та отримувачем.

Аналіз понад сотні джерел інформації показав, що «комунікабельність носіїв інформації» потребує деякої систематизації та розкриття її фізичного змісту при взаємодії носіїв у процесі здійснення інформаційної діяльності.

Як було розглянуто раніше, комунікабельність носіїв інформації охоплює три середовища (сфери): соціальне, технічне та логічне. Вони своїми факторами впливають на процеси інформаційних взаємодій носіїв інформації (Рис. 5). Їх можна виділити (класифікувати) як три основні класи, що об’єднуються трьома прикордонними підкласами (зонами), які будуть наведені далі.

З середовищ впливу на комунікабельність носіїв інформації можна виділити (класифікувати) три основні класи, що об’єднуються трьома прикордонними зонами.

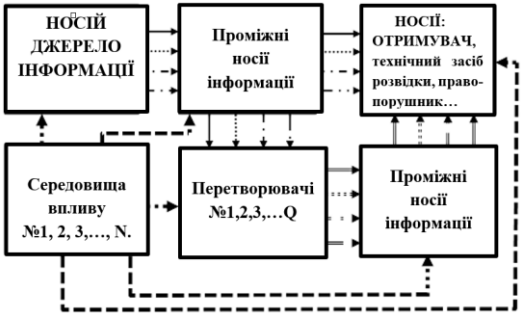


Рис. 5. Узагальнена структурна схема комунікації носіїв інформації на прикладі каналу витоку інформації

Слід зазначити, що у літературних джерелах ці поняття суттєво «перемішані». Наприклад, у сфері соціуму деякими авторами виділяється поняття «технічна комунікація» (а) на рівні професіонала – менеджера, який володіє техніками соціального «приєднання» до співрозмовника, наприклад, NLP. Також в інших джерелах «технічна комунікація» (б) трактується як набір методів, якими практикуючі фахівці користуються, щоб визначити застосовність технічних процесів, викладених у документі для виготовлення певного виду продукції. Крім цього, у визначенні «технічної комунікації» (в) закладено головну практичну мету – створити легкодоступну інформацію для аудиторії.

Класифікація та зони розмежування комунікабельностей носіїв інформації наведено на Рисунку 6.

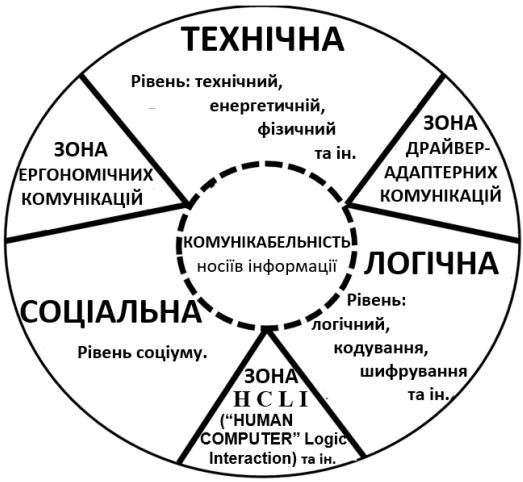


Рис. 6. Класифікація комунікабельності носіїв

А. **Соціальна комунікабельність** носіїв інформації

Подання про інформаційну сферу соціуму розглядалося ще з часів античності (Платон, Протагор), які представляли цю сферу як елемент соціального управління (Арістотель, Цицерон). Стрімкий розвиток інформаційних технологій призвів до того, що дев'ять десятих усієї інформації сьогодні циркулює в технічній «радіоелектронно- цифровій» формі та залучає до забезпечення соціальної комунікабельності фахівців у галузі технічних наук, які займаються вирішенням ергономічних питань у галузі комп'ютерної інформації.

Справа в тому, що сам процес передачі інформації по суті є соціальним через те, що в кінцевому рахунку він полягає в передачі інформації («синонімів»: змісту, відомостей, даних і т.п.) від однієї людини до іншої.

Людина (носій інформації…) є як виробником – джерелом, так і споживачем – одержувачем інформації. Тому соціальні комунікації є інформаційним процесом поширення інформації як особливої форми інформаційних відносин між людьми. У зв'язку з цим сенс та зміст інформаційної сфери соціуму необхідно розглядати у широкому соціально-технологічному контексті.

Б. **Технічна комунікабельність** носіїв інформації

Техносфера – це сфера, що містить штучні технічні споруди та пристрої, що виготовляються та використовуються людиною. Комунікації між ними та їх якість є характеристикою технічної комунікабельності носіїв інформації[12].

В. **Логічна комунікабельність** носіїв інформації

Під логічною комунікабельністю носіїв інформації розуміється область прикладної логіки інформаційно-комунікаційних пристроїв та систем як сфери застосування науки логіки; різноманітність практичного використання математико-логічних теорій, внаслідок чого логіка виконує методологічну функцію, набуває прикладного значення і відноситься до комп'ютерної логіки як базису технологій ІТ-інформаційних та ШІ.

Будь-яке порушення комунікабельності носіїв інформації істотно збільшує вірогідність реалізації негативного впливу загроз на інформацію.

ВИСНОВКИ

Підсумовуючи результати багаторічних спостережень, публікацій, зауважень, відгуків та корекцій можна зробити позитивний висновок про те, що головний закон захисту інформації дає досить точну відповідь на запитання: «У яких випадках можна вважати інформацію захищеною»[13,14,15].

---

[12] Словники ABBYY Lingvo (Uk-Uk) техносфера Explanatory (Uk-Uk) [Електронний ресурс]. URL : http://www.lingvo.ua/uk/Interpret/uk-uk/Техносфера

[13] Громико І.О. Головний закон захисту інформації. Частина друга. Collection of scientific papers «Scientia». Section 9. Information technologies and systems. DOI 10.36074/scientia-16.08.2024 – Singapore, Republic of Singapore.- August 16, 2024. p. 45-50

[14] Громико І.О. Головний закон захисту інформації. VII Міжнародна науково-практична конференція "Theoretical and empirical scientific research: concept and trends"- Section XI Information technologies and systems – DOI 10.36074/logos-16.08.2024.001 – м. Оксфорд, Сполучене Королівство. 16 серпня 2024 р. 177-188

«Інформація вважається захищеною, якщо під час здійснення інформаційної діяльності обов'язково і одночасно виконуються дві головні вимоги до інформаційних ланцюгів взаємодії носіїв інформації:

1) «режимна адекватність» носіїв інформації;

2) «режимна комунікабельність» носіїв інформації» . (UA)

"Information is considered protected if, during the implementation of information activities, two Key (Primary, Core and Basic) requirements for information chains of interaction of information carriers are necessarily and simultaneously fulfilled:

1) "regime adequacy" of information carriers;

2) "regime communicability" of information carriers." (ENG).

АНОТАЦІЯ

Базуючись змістом Законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та «Про основні засади забезпечення кібербезпеки України» та державними стандартами і нормативними документами автор спробував знайти відповідь на запитання: «Коли інформацію можна вважати захищеною?». При чому відповідь повинна була містити і статичний, і динамічний стани носіїв інформації які приймають участь в інформаційній діяльності. Перша частина «Головного закону захисту інформації» була розроблена майже 10 років тому і мала назву «Загальна парадигма захисту інформації». І тільки у теперішній час вдалося повністю дослідити реальні інформаційні сучасні процеси що дозволило сформулювати визначення «Головного закону захисту інформації» в тому вигляді, який надається в даній науковій статті. Результати опубліковані у наукових збірниках декількох Міжнародних конференцій. Зауважень, поправок та корекцій на наступний момент до автора не надійшло. На думку автора, – Головний закон захисту інформації має право на життя.

Література

1. Громико І.О. Загальна парадигма захисту інформації: проблеми захисту інформації в аспектах математичного моделювання : монографія. Харків : ХНУ ім. В.Н.Каразіна, 2014. 216 с.

2. Спосіб знешкодження вибухового пристрою : пат. Україна : МКП F42D 5/04. №7238 ; заявл. 11.08.2006 ; опубл. : 15.06.2005, Бюл. № 5.

3. Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. №32620 ; заявл. 26.05.2008 ; опубл. : 26.05.2008, Бюл. № 10.

4. Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. №107207 ; заявл. 27.11.2015 ; опубл. : 25.05.2016, Бюл. № 10.

---

[15] Громико І.О. Пірамідальна модель доступу громадянина до державної таємниці. Збірник доповідей VI міжнародної науково-практичної конференції "Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи" 29 жовтня 2025 р./ Міністерство оборони України, НУОУ. УДК: 355.451. К.: НУОУ, 2025. 237 с. Ст. 131-135.

5. Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. №114388 ; заявл. 11.08.2006 ; опубл. : 10.03.2017, Бюл. № 5.

6. Про інформацію : Закон України від 2 жовтня 1992 р. № 48 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.03.2026).

7. Про державну таємницю : Закон України від 21 січня 1994 р. №3855-XII / Верховна Рада України. URL : https ://zakon.rada.gov.ua/laws/show/ 3855-12#Text

8. Наказ служби безпеки України № 383 від 23.12.2020р. (Редакція станом на 09.09.2024)

9. Про стандартизацію. Закон України від 5 червня 2014 року № 1315-VII Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/1315-18#Text

10. Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) [Official Journal L 144 of 30 April 2004]. https://www.ab.gov.tr/files/tarama/tarama_files/10/SC10EXP_ IDABC.pdf .

11. Браузерна сумісність семантичних елементів. [Електронний ресурс]. URL : http://professorweb.ru/my/html/html5/ level1/1_7.php

12. Словники ABBYY Lingvo (Uk-Uk) техносфера Explanatory (Uk-Uk) [Електронний ресурс]. URL : http://www.lingvo.ua/uk/Interpret/uk-uk/Техносфера

13. Громико І.О. Головний закон захисту інформації. Частина друга. Collection of scientific papers «Scientia». Section 9. Information technologies and systems. DOI 10.36074/scientia-16.08.2024 – Singapore, Republic of Singapore.- August 16, 2024. p. 45-50.

14. Громико І.О. Головний закон захисту інформації. VII Міжнародна науково-практична конференція “Theoretical and empirical scientific research: concept and trends”- Section XI Information technologies and systems – DOI 10.36074/logos-16.08.2024.001 – м. Оксфорд, Сполучене Королівство. 16 серпня 2024. p. 177-188.

15. Громико І.О. Пірамідальна модель доступу громадянина до державної таємниці. Збірник доповідей VI міжнародної науково-практичної конференції “Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи” 29 жовтня 2025 р./ Міністерство оборони України, НУОУ. УДК: 355.451 – К.: НУОУ, 2025. 237 с. – Ст.131-135.

Information about the authors:
Hromyko Ihor Oleksiyovych,
Candidate of Technical Sciences, Professor ZVO
of the Educational and Research Institute Computer Sciences
and Artificial Intelligence of Department of Security
of Information Systems, Networks & Technologies,
Associate Professor,
V. N. Karazin Kharkiv National University
6, Svobody Sq., Kharkiv, 61022, Ukraine
https://orcid.org/0000-0002-7701-9557

DOI https://doi.org/10.30525/978-9934-26-686-7-5

ОСОБЛИВОСТІ ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Дзюрбель А. Д.

ВСТУП

Сучасний етап розвитку світової цивілізації характеризується тотальною трансформацією соціальних комунікацій, що зумовлена стрімким впровадженням інформаційних технологій у всі сфери людської життєдіяльності. Цей процес неминуче супроводжується якісною зміною структури злочинності: від класичних «матеріальних» правопорушень до кіберзлочинів та злочинів, де цифрові пристрої виступають знаряддям або об'єктом посягання. У цьому контексті перед криміналістичною наукою постає фундаментальне завдання – розробка теоретичних засад та практичних інструментів роботи з новим типом відображення реальності, а саме з цифровими (електронними) слідами[1].

Сучасні кримінальні правопорушення все частіше вчиняються у кіберпросторі або супроводжуються утворенням специфічних цифрових відображень, які за своєю природою суттєво відрізняються від традиційних матеріальних слідів[2]. Це ставить перед криміналістичною наукою виклик щодо переосмислення базових теоретичних положень та розробки нових методичних рекомендацій для суб'єктів досудового розслідування.

Актуальність теми зумовлена тим, що цифрові сліди сьогодні присутні майже в кожному кримінальному провадженні – від корупційних злочинів та шахрайства до воєнних злочинів та актів агресії. За оцінками Центру дослідження комп'ютерних злочинів, у 2025 році збитки від кіберзлочинності перевищать 12 трильйонів доларів США. Глобальний характер кіберризиків вимагає створення спільних дієвих міжнародних рамок для забезпечення стандартів кібербезпеки та захисту даних[3]. Також слід врахувати, що в умовах широкомасштабного вторгнення Російської Федерації в Україну цифрові докази стали основним інструментом документування звірств російських військових (відео з камер спостереження, записи з БПЛА, супутникові знімки та пости в соцмережах російських військових, тощо). У зв'язку з наведеним, перед правоохоронними органами постає питання про документування цих злочинів з врахуванням вимог національних та міжнародних правових

[1] Коломійцев С.О. Сутність та класифікація цифрових слідів кримінального правопорушення. *Вісник пенітенціарної асоціації України. 2025.* № 2 (32). С. 196-205.

[2] Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка,* № 4 (100), 2022. С. 226-236.

[3] Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL:https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

інституцій. Ключовою основою такої діяльності в умовах нашого сьогодення є цифрові технології і, зокрема цифрові докази[4].

Проте в юридичній доктрині України досі триває дискусія щодо термінологічної єдності, класифікаційних критеріїв та процесуального статусу таких об'єктів[5]. Більше того, динамічний розвиток технологій анти-криміналістики (шифрування, анонімізація, видалення даних) потребує від правоохоронних органів постійного оновлення технічного інструментарію та тактичних прийомів.

У контексті кримінального судочинства це зумовлює виникнення нових викликів перед теорією криміналістики та процесуальним правом, оскільки традиційні методи збирання та дослідження матеріальних доказів виявляються недостатніми для роботи з об'єктами нематеріальної природи. Поняття «цифровий слід» стає центральним елементом сучасної доказової бази. Це вимагає глибокого переосмислення правової природи таких слідів, удосконалення національного законодавства та гармонізації вітчизняної слідчо-судової практики з міжнародними стандартами.

Метою цієї статті є комплексний аналіз поняття, класифікації та криміналістичної характеристики цифрових слідів, дослідження проблемних аспектів їхнього використання у практичній діяльності та вивчення тенденцій сучасної судової практики для формування науково обґрунтованих пропозицій щодо вдосконалення механізмів збирання та дослідження цифрових доказів.

Питання цифрових (електронних) слідів досліджувалися багатьма вітчизняними та закордонними науковцями. Значний внесок у розвиток цифрової криміналістики зробили Г.К. Авдєєва, М.В. Капустіна, А.В. Коваленко, І.А. Колеснікова, О.І. Крицька, К.В. Латиш, В.Ю. Шепітько, І.З. Якименко та інші[6].

У працях вітчизняних науковців не досягнуто єдності в думках та поглядах у питанні визначення цифрових слідів, їх класифікації, місця та ролі у науці криміналістика та інших питаннях пов'язаних з зазначеним видом слідів. Враховуючи наведене, у статті проаналізуємо ряд проблемних та спірних питань щодо цифрових доказів та запропонуємо окремі шляхи їх вирішення.

1. Поняття, класифікація та криміналістична характеристика цифрових слідів у сучасній криміналістиці

Теоретичне осмислення сутності цифрових слідів потребує відходу від традиційної (матеріалістичної) трасологічної парадигми, де слід сприймається як фізичне відображення форми одного предмета на поверхні іншого. Саме тому, виникнення цифрових технологій змусило дослідників вийти за межі

[4] Цифрові докази війни: як технології допомагають Україні фіксувати злочини Росії. Українські правозахисники та юристи розповіли про нові методи збору доказів воєнних злочинів РФ, які витримують перевірку міжнародних судів URL: https://www.polskieradio.pl/398/7857.

[5] Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету. Серія Право.* Випуск 85: частина 4. С. 71-75.

[6] Там само.

традиційної трасології. Цифровий слід не є матеріальним об'єктом у звичному розумінні (як відбиток пальця чи сліди протектора), оскільки він існує у формі двійкового коду, записаного на фізичний носій за допомогою електромагнітних або оптичних сигналів.[7]

У науковій літературі тривалий час тривала дискусія щодо термінології. С. Хижняк пропонує використовувати термін «віртуальні сліди», розуміючи під ними будь-які зміни комп'ютерної інформації, пов'язані з подією злочину[7]. Проте інші дослідники слушно зауважують, що семантика слова «віртуальний» передбачає щось уявне або таке, що існує лише в уяві, тоді як цифрові дані є об'єктивною реальністю, яка, попри невидимість для людського ока без спеціальних пристроїв, має чітку матеріальну основу у вигляді стану напівпровідників або намагнічених ділянок диска[8]. Отже, найбільш обґрунтованим є термін «цифрові сліди», який підкреслює форму існування інформації (discrete/digital) та її нерозривний зв'язок з технологіями обробки даних[9].

Криміналістична характеристика цифрових слідів визначається їхніми специфічними властивостями, які докорінно відрізняють їх від традиційних матеріальних об'єктів. По-перше, це відсутність безпосереднього візуального сприйняття – для виявлення та фіксації цифрової інформації необхідне складне програмне та апаратне забезпечення. По-друге, це висока вразливість та нестабільність: інформація в оперативній пам'яті (RAM) зникає при відключенні живлення, а дані на накопичувачах можуть бути миттєво видалені або змінені шляхом дистанційного доступу. По-третє, цифрові сліди мають здатність до ідентичного копіювання без втрати первинних властивостей, що породжує проблему автентичності та розмежування оригіналу і копії в правовому полі.

Науковий аналіз дозволяє виділити кілька ключових підходів до визначення поняття цифрові сліди:

1. *Технічний підхід:* Цифровий слід як стан комп'ютерної системи або послідовність бітів на носії[10].

2. *Інформаційний підхід:* Як криміналістично значуща інформація про подію злочину, зафіксована в цифровій формі[11].

3. *Діяльнісний підхід:* Як відображення активності особи у віртуальному просторі (логи, транзакції, повідомлення)[12].

---

[7] Хижняк Є.С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права.* 2017. Вип.79. С. 159-166.

[8] Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний електронний журнал*. 2023. № 10. С. 472-475.

[9] Коломійцев С.О. Сутність та класифікація цифрових слідів кримінального правопорушення. *Вісник пенітенціарної асоціації України*. *2025.* № 2 (32). С. 196-205.

[10] Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304-307.

[11] Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні / І. О. Крицька // Цифрові трансформації України 2020: виклики та реалії: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу, 18 вересня 2020 р. Харків: НДІ ПЗІР НАПрН України, 2020. С. 92-97.

Враховуючи наведене, на наш погляд, найбільш адаптованим до сучасних умов є визначення запропоноване Демидовою Є.Є., згідно з яким *цифровий слід* – це дані, що залишаються у цифровому просторі в результаті використання цифрових пристроїв, технологій та інформаційних мереж, які містять відомості про обставини вчинення кримінального правопорушення[13]. Важливо також розмежовувати поняття «цифровий слід» та «джерело цифрового сліду» (наприклад, смартфон або сервер). Слід – це інформація, тоді як пристрій – це лише її матеріальний носій.

Досліджуючи поняття цифрових слідів, слід зазначити, що їм притаманні певні ключові особливості, а саме:

1. *Цифрова (бінарна) форма існування.* Інформація представлена у вигляді нулів та одиниць. Це обумовлює можливість ідеального копіювання: криміналістичний образ (image) носія є бінарно ідентичним оригіналу, що дозволяє проводити дослідження без ризику модифікації первинних даних.
2. *Волатильність (летючість).* Значна частина цифрових слідів існує лише під час роботи пристрою. Дані в оперативній пам'яті (RAM), активні мережеві з'єднання та тимчасові системні процеси зникають при вимкненні живлення. Це вимагає тактики «живого аналізу» (live forensics) перед фізичним вилученням техніки.
3. *Прихованість та залежність від засобів візуалізації.* На відміну від традиційних слідів, цифрові сліди неможливо сприйняти безпосередньо органами чуття людини. Вони потребують «перекладача» – програмно-апаратного комплексу (Cellebrite, EnCase), який декодує бінарний код у зрозумілий текст, зображення чи відео.
4. *Схильність до швидкої модифікації та знищення.* Цифрові сліди можуть бути змінені або видалені дистанційно. Функції «віддаленого стирання» у смартфонах або автоматичне очищення логів у серверах створюють ризик незворотної втрати доказів.
5. *Трансмежовість (екстериторіальність).* Механізм утворення сліду може розпочатися в одній країні (пристрій зловмисника), а завершитися в іншій (сервер провайдера), що створює складні проблеми юрисдикції та міжнародної співпраці.

Формування цифрового сліду є результатом взаємодії користувача з операційною системою або прикладним програмним забезпеченням. Будь-яка операція залишає артефакти:

- *Тимчасові мітки (Timestamps):* MAC-дати (Modified, Accessed, Created), які фіксують час будь-якої дії з файлом.
- *Лог-файли (Logs):* Системні журнали, що реєструють події (вхід у систему, підключення до Wi-Fi, встановлення програм).

---

[12] Лазебний А.М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип.1 (10) С. 226-233.

[13] Демидова Є.Є. *Цифрові сліди кримінального правопорушення: поняття та особливості. Науковий вісник Ужгородського Національного Університету. Серія Право.* Випуск 85: частина 4. С. 71-75.

- *Метадані:* Інформація «про інформацію», прихована всередині файлів (EXIF-дані фотографій з координатами GPS, авторство документів Word).

Для ефективної побудови методики виявлення та фіксації слідів критично важливою є їхня наукова класифікація. Авдєєва Г.К. та Стороженко С.В. пропонують диференціювати електронні сліди за об'єктом, що їх утворює, способом доступу та правомірністю входу до системи[14]. Гринько Л.П. вважає, що електронні сліди потрібно поділяти на ті, які містяться в мережі Інтернет та ті, що знаходяться на електронних носіях[15]. В свою чергу Колодіна А.С. та Федорова Т.С. виділяють активні та пасивні цифрові сліди, а також виокремлюють такі їх різновид як контент та метадані[16]. На наш погляд, найбільш розгорнуту систему критеріїв пропонує А. В. Коваленко, розділяючи сліди на групи за ознаками слідоутворюючого об'єкта, характеристиками самих даних та особливостями носія[17].

За ознаками носія (слідоприймаючого об'єкта) сліди поділяються на локальні та віддалені. Локальні сліди знаходяться безпосередньо в межах місця події на персональних пристроях (смартфони, ноутбуки, флеш-накопичувачі). Віддалені сліди можуть перебувати як у межах національної юрисдикції (сервери вітчизняних провайдерів), так і поза її межами (хмарні сервіси Google, Apple, Microsoft, сервери месенджерів Telegram або WhatsApp). Цей поділ безпосередньо впливає на тактику слідчої дії: якщо для вилучення локальних слідів достатньо проведення огляду або обшуку, то робота з віддаленими слідами вимагає застосування процедур тимчасового доступу до речей і документів або використання механізмів Будапештської конвенції про кіберзлочинність[18].

Додатково слід виокремити класифікацію за способом сприйняття та форматуванням даних. Цифрові сліди існують у формі текстових документів, графічних зображень, відео- та звукозаписів, лог-файлів (журналів реєстрації подій), метаданих (EXIF-дані фотографій, історія редагування документів) та баз даних. Метадані часто мають вищу криміналістичну цінність, ніж сам зміст файлу, оскільки вони фіксують час створення, координати GPS та ідентифікатори пристрою, що дозволяє встановити об'єктивну картину події незалежно від показань підозрюваного.

Особливу категорію складають сліди, що перебувають у захищеному стані. Розвиток технологій шифрування (наприклад, File-Based Encryption в Android

[14] Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття і види. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2017. № 1(77). С. 168-175.

[15] Гринько Л.П. «Слідова картина» шахрайств, вчинених через мережу Інтернет. *Полтавський правовий часопис*. 2022. № 3. С. 16-27.

[16] Колодіна А.С., Федотова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський правовий часопис*. Випуск 1. С. 176-180.

[17] Коваленко А.В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Випуск 161. С. 202-214.

[18] Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

або Data Protection в iOS) призводить до того, що вилучений носій без знання ключа або пароля перетворюється на «нечитабельну» сукупність даних[19]. Це актуалізує проблему правомірності вилучення паролів та біометричних даних під час слідчих дій, а також необхідність залучення фахівців, здатних використовувати спеціалізовані методи обходу засобів захисту (brute-force, розшифрування за допомогою апаратних ключів)[18]. Розуміння цієї класифікаційної структури є обов'язковою умовою для забезпечення допустимості доказів, оскільки неправильне визначення типу сліду призводить до вибору невідповідної процедури його фіксації.

Незважаючи на стрімкий розвиток технологій, Кримінальний процесуальний кодекс України станом на 2025–2026 роки не містить окремої норми, яка б прямо визначала поняття «електронний доказ» або «цифровий слід». Стаття 84 КПК України (Далі КПК) встановлює вичерпний перелік процесуальних джерел доказів: показання, речові докази, документи та висновки експертів. У цій структурі електронна інформація традиційно відноситься до категорії документів. КПК оперує поняттям «документи», до яких відносить і комп'ютерні дані (ст. 99). Відповідно до зазначеної статті КПК, до документів належать матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації, у тому числі електронні[20].

Таке нормативне регулювання породжує низку проблем у правозастосовчій діяльності. По-перше, електронна інформація за своїми властивостями часто ближча до речових доказів, оскільки вона є слідовим відображенням злочинної діяльності в пам'яті пристрою, а не просто засобом фіксації думок чи фактів, як класичний документ. По-друге, відсутність чіткої диференціації ускладнює процес збирання та перевірки таких доказів. На відміну від цивільного, господарського та адміністративного судочинства, де статус електронних доказів закріплений в окремих статтях ще з 2017 року, кримінальний процес залишається надмірно консервативним[21].

Підсумовуючи наведене, ми повністю поділяємо точку зору наукової спільноти щодо внесення змін до КПК України, зокрема до статей 84 та 99, для виокремлення електронних доказів як самостійного виду. Це зумовлено специфікою їх природи: вони існують лише в цифровій формі, потребують спеціального обладнання для зчитування та професійного аналізу, а також мають надзвичайну вразливість до маніпуляцій.

---

[19] Курман О.В. Особливості та проблеми виявлення й фіксації цифрових слідів під час огляду мобільних засобів зв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство».* Випуск № 04, 2025, частина 3. С. 238-242.

[20] Науково-практичний коментар Кримінального процесуального кодексу України – науково-методична робота. Станом на 14 квітня 2024 року / За заг. ред. Стратонова В.М. Київ: Видавничий дім «Професіонал», 2024. 1208 с.; Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[21] Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : Закон України від 3 жовт. 2017 р. No 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147-19.

2. Процесуальний порядок отримання та міжнародні стандарти ідентифікації та збереження електронних доказів

У сучасній юридичній науці триває дискусія щодо співвідношення термінів «електронні докази» та «цифрові докази». Хоча стаття 99 КПК України використовує термін «електронні документи» та їхні дублікати, практика та доктрина дедалі частіше схиляються до ширшого поняття – цифрових доказів. Правова природа таких доказів визначається як будь-яка інформація, створена, передана, отримана або збережена в електронній формі, яка має значення для кримінального провадження[22].

Ключовою особливістю цифрових доказів є їхня бінарна форма існування, що робить їх невидимими для людського ока без спеціального інтерфейсу. Це створює ситуацію, коли доказом є не сам фізичний носій (флеш-драйв чи сервер), а саме логічна послідовність даних, зафіксована на ньому.

Відмінність цифрових доказів від традиційних полягає в тому, що вони є надзвичайно крихкими. Якщо для пошкодження паперового документа потрібен фізичний вплив, то для зміни цифрового файлу достатньо відкрити його без використання спеціальних засобів блокування запису (write-blockers), що автоматично змінює метадані (час останнього доступу). Саме тому процесуальний порядок їх збирання має бути значно суворішим, ніж для матеріальних об’єктів.

Згідно з чинним законодавством України, збирання цифрових доказів здійснюється шляхом проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій (НСРД) та через запити до володільців інформації. Основним інструментарієм є огляд, обшук та тимчасовий доступ.

Огляд комп’ютерних даних. Стаття 237 КПК регламентує проведення огляду, який у контексті цифровізації найчастіше стосується інформації з відкритих джерел (вебсайтів, соцмереж) або вмісту гаджетів. Процедура огляду вимагає відображення інформації в протоколі у формі, придатній для сприйняття: через скриншоти, відеозапис процесу навігації по сайту або виготовлення паперових копій[23]. Важливо, що при огляді даних із мережі Інтернет слідчі мають дотримуватися стандартів Протоколу Берклі, щоб забезпечити допустимість матеріалів у міжнародних інстанціях, що особливо актуально при документування воєнних злочинів[24].

Слід також відмітити, що процедура огляду комп’ютерних даних (ч. 2 ст. 237 КПК) потребує особливої уваги. Слідчий має право проводити огляд не лише

---

[22] Петрик В.В. Використання електронних доказів у кримінальних провадженнях: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського Національного Університету.* 2025. Серія Право. Випуск 87: частина 4. С. 119-123.

[23] Маркіна А.В. Способи збирання стороною обвинувачення електронних доказів у кримінальних провадженнях щодо воєнних злочинів. *Право.ua.* 2025 № 4. С. 104-112.

[24] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

фізичних носіїв, а й безпосередньо інформації. При цьому, згідно з позицією Верховного Суду та науковими рекомендаціями, вилучення електронної інформації має бути зафіксоване в протоколі, а носій – визнаний речовим доказом[25]. Проте існує колізія: чи можна вилучати інформацію шляхом копіювання без вилучення самого пристрою? Сучасна практика схиляється до того, що копіювання (imaging) є допустимим засобом фіксації, якщо воно здійснюється за участю спеціаліста та з використанням засобів, що гарантують ідентичність копії та оригіналу[26]. Це дозволяє не паралізувати роботу підприємств вилученням серверів, одночасно забезпечуючи інтереси слідства.

Тимчасовий доступ та виїмка. Механізм тимчасового доступу до речей і документів (ст. 159 КПК) є критично важливим для отримання даних від провайдерів. Проте закон встановлює обмеження: якщо доступ надається до електронних інформаційних систем, він здійснюється виключно шляхом зняття копії інформації без вилучення самих систем (комп'ютерів, серверів), якщо інше не вказано в ухвалі[27]. Це положення спрямоване на захист інтересів бізнесу та забезпечення безперервності роботи критичної інфраструктури.

Обшук та вилучення носіїв. Обшук (ст. 234 КПК) застосовується у випадках, коли є підстави вважати, що цифрова техніка містить сліди злочину і власник не надасть їх добровільно. Головною проблемою під час обшуку є вилучення всієї техніки замість копіювання конкретних файлів. Судова практика поступово схиляється до того, що вилучення фізичних носіїв є виправданим лише у разі потреби проведення комплексної комп'ютерно-технічної експертизи або коли є ризик видалення даних за допомогою віддаленого доступу[28].

Негласні слідчі (розшукові) дії. НСРД (ст. 263, 264 КПК) проводяться за ухвалою слідчого судді виключно щодо тяжких та особливо тяжких злочинів. Отримання електронних доказів під час НСРД вимагає специфічного підходу до фіксації «цифрового сліду», який включає не лише сам файл, а й умови його створення та передачі. Проблема отримання доказів за ст. 263 КПК полягає в тому, що сучасні оператори зв'язку використовують складні протоколи передачі даних. Процедура передбачає доступ до каналів зв'язку в режимі реального часу. Судова практика Верховного Суду 2024 року вказує, що інформація про спеціальні технічні засоби, які використовуються для такої НСРД, є державною таємницею, і її нерозголошення в суді є обґрунтованим[29].

---

[25] Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Трибуна молодого вченого.* 2021. № 6. С. 273-278.

[26] Кохановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2019. № 1(31). С. 13-19.

[27] Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 336-339.

[28] Маркіна А.В. Способи збирання стороною обвинувачення електронних доказів у кримінальних провадженнях щодо воєнних злочинів. *Право.ua.* 2025 № 4. С. 104-112.

[29] Телизіна Я. Оцінка доказів, отриманих в результаті проведення НСРД: частина 2. URL:https://advokatpost.com/pro-otsinku-dokaziv-otrymanykh-u-rezultati-provedennia-nsrd-prokuror-iana-talyzina.

Основною проблемою при знятті інформації з електронних інформаційних систем (ст.264 КПК) є доступ до зашифрованих даних месенджерів (Telegram, WhatsApp)[30]. Оскільки інформація зазвичай захищена наскрізним шифруванням, перехоплення трафіку (ст. 263) часто є малоефективним. Натомість НСРД за ст. 264 КПК дозволяє отримати доступ безпосередньо до пристрою або серверної частини системи. Проблеми виникають при використанні віддаленого доступу до хмарних сховищ (Google Drive, iCloud). Юридична невизначеність щодо юрисдикції даних, які фізично знаходяться на серверах у США або ЄС, створює перешкоди для легітимізації таких доказів в українських судах[31].

Суттєвим недоліком в роботі з цифровими слідами загалом є те, що КПК не містить детальних інструкцій щодо того, як саме технічно їх фіксувати, щоб вони не втратили допустимості. Це призводить до того, що слідчі часто обмежуються скріншотами, які без належного засвідчення метаданих легко піддаються сумніву в суді[32].

Проблема «фейків» та легкості маніпулювання цифровими даними вимагає від правоохоронців використання спеціальних криптографічних засобів під час оформлення доказів. Ключовим поняттям тут є хешування – створення унікального цифрового «відбитка» файлу за допомогою алгоритмів.

У протоколі слідчої дії обов'язково мають бути зазначені хеш-суми всіх скопійованих файлів. Це дозволяє в суді через будь-який проміжок часу перевірити, чи не вносилися зміни у доказ. Якщо хеш-сума файлу в суді не збігається з тією, що вказана в протоколі, доказ вважається недостовірним. Верховний Суд у своїх постановах (наприклад, від 29 березня 2021 року у справі № 554/5090/16-к) підкреслює, що допустимість електронного документа залежить від можливості перевірки його цілісності та автентичності[33].

Ланцюг збереження доказів (Chain of Custody) у вітчизняній практиці. Забезпечення цілісності електронного доказу від моменту його виявлення до подання суду є ключовим завданням процесуального порядку. У міжнародній практиці та стандартах цифрової криміналістики це реалізується через «ланцюг збереження» (chain of custody)[34].

Ланцюг збереження – це документально зафіксований шлях доказу, що включає:

1. Ідентифікацію джерела (URL, фізичний пристрій, IMEI, MAC-адреса).

---

[30] Кірчев В.О. Новітні засоби доказування пропозиції, обіцянки або надання неправомірної вигоди службовій особі. *Європейський правничий часопис.* 2025. Випуск 6,7. С. 216-223.

[31] Петрик В.В. Використання електронних доказів у кримінальних провадженнях: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського Національного Університету.* 2025. Серія Право. Випуск 87: частина 4. С. 119-123.

[32] Колісник О.В., Король С.С. Електронні докази:критерії їх оцінки. *Юридичний науковий електронний журнал.* 2024. № 4. С. 158-160.

[33] Постанова від 29.03.2021 № 554/5090/16-к Верховний Суд. Касаційний кримінальний суд. URL:https://verdictum.ligazakon.net/document/96074938.

[34] Погорецький М.А. Використання даних ENCROCHAT у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий журнал.* 2025. Випуск № 8. С. 223-229.

2. Фіксацію стану в момент виявлення через розрахунок хеш-суми (MD5, SHA-1, SHA-256). Хеш-сума є «цифровим відбитком» файла; будь-яка зміна навіть одного біта в даних змінить це значення

3. Опис інструментів збирання (назва та версія програмного забезпечення, наприклад, FTK Imager, EnCase)[35].

4. Документування кожної передачі доказу між особами (слідчий – експерт – суд) із зазначенням часу та способу транспортування (сейф-пакет, зашифрований канал) [36].

В українському процесуальному законодавстві термін «chain of custody» прямо не вживається, хоча його елементи присутні у вимогах до протоколювання слідчих дій (ст. 104 КПК). Проте на практиці суди все частіше звертають увагу на цей стандарт. Відсутність у протоколі огляду інформації про хеш-суму вилученого файла або про використання пристроїв блокування запису (write-blockers) дає підстави захисту висувати версію про можливість штучного створення або модифікації доказів правоохоронцями.

Іншими словами, концепція ланцюжка зберігання передбачає хронологічне документування всіх етапів життя доказу: від моменту виявлення на місці події до представлення в суді. Це включає фіксацію:

- Хто мав доступ до доказу?
- Коли і де він зберігався?
- Які інструменти використовувалися для аналізу?
- Чи забезпечено захист від зовнішнього (електромагнітного) впливу.

Будь-яка прогалина в цьому ланцюжку (наприклад, якщо жорсткий диск зберігався в незапечатаному вигляді в кабінеті слідчого) є підставою для визнання доказу недопустимим, оскільки створюється «обґрунтований сумнів» щодо його незмінності[37].

Процесуальне дослідження цифрової інформації здебільшого реалізується через залучення експертів. Комп'ютерно-технічна експертиза (КТЕ) проводиться відповідно до Інструкції Мін'юсту № 53/5 та має на меті відповіді на питання про наявність певних файлів, відновлення видаленої переписки, виявлення слідів злому або стороннього втручання[38].

Метадані (дані про дані) часто є більш важливими, ніж основний контент. Наприклад, файл фотографії містить метадані EXIF, де вказано модель

[35] Погорецький М.А. Криптовалюта як об'єкт, предмет та засіб вчинення злочину: проблеми виявлення, документування і доказування в досудовому та судовому провадженнях. *Держава і регіони. Серія:Право.* 2025. № 3(88). С. 70-90.

[36] Погорецький М.А. Використання даних ENCROCHAT у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий журнал.* 2025. Випуск № 8. С. 223-229.

[37] Стефанів Н. Суддя ВС проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1751385.

[38] Наказ Міністерства юстиції України № 53/5 від 08.10.1998 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень». URL: https://https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

телефону, точний час зйомки та GPS-координати. Експертиза дозволяє встановити, чи був файл створений саме на тому пристрої, який вилучено у підозрюваного. Проте слід враховувати, що багато месенджерів (Viber, Telegram) при пересиланні файлів автоматично стирають метадані, що вимагає використання складніших методів відновлення з пам'яті самого пристрою[39].

Сучасні розслідування оперують терабайтами даних. У таких умовах ручний аналіз неможливий. Новітні тенденції в криміналістиці передбачають використання ШІ для автоматичного пошуку аномалій, ідентифікації об'єктів на тисячах годин відеозаписів та встановлення зв'язків між фігурантами через аналіз «великих даних» (Big Data)[40]. Впровадження таких інструментів потребує створення відповідної нормативної бази, щоб результати роботи алгоритмів могли бути визнані допустимими доказами.

Злочинність у цифрову епоху не визнає державних кордонів. Часто жертва знаходиться у Львові, злочинець – в Берліні, а дані зберігаються на сервері в Каліфорнії. Це робить міжнародне співробітництво життєво необхідним.

Будапештська конвенція та Другий додатковий протокол. На міжнародному рівні основним документом, що визначає стандарти роботи з цифровими даними, є Конвенція про кіберзлочинність (Будапештська конвенція). Вона встановлює обов'язок держав-учасниць запровадити механізми термінового збереження комп'ютерних даних (стаття 16) та часткового розкриття даних про рух інформації (стаття 17)[41]. Це критично важливо для випадків, коли дані можуть бути видалені провайдером автоматично або за запитом користувача. Конвенція передбачає оперативне забезпечення збереженості даних, які можуть бути змінені або втрачені в процесі розслідування. В Україні ці положення частково імплементовані через процедуру тимчасового доступу до речей і документів, проте механізм «термінового збереження» (data preservation order) без судового рішення на короткий строк (до 90 днів за Конвенцією) все ще потребує вдосконалення в національному законодавстві.

Також важливим кроком стало прийняття Другого додаткового протоколу (2022), який запровадив механізми прямої взаємодії правоохоронців із сервіс-провайдерами (Google, Meta) без традиційних і повільних запитів про міжнародну правову допомогу[42]. Це дозволяє в екстрених випадках (наприклад, загроза життю) отримати дані протягом годин, а не місяців.

---

[39] Карпець Ю.В. Цифрові докази та комп»ютерно-технічні експертизи у кримінальних провадженнях про військові злочини. *Юридичний науковий електронний журнал.* 2025. № 11. С. 226-230.

[40] Орещук В. Докази, отримані за допомогою штучного інтелекту, та їх використання в суді. URL:https:// www.hsa.org.ua/blog/dokazi-otrimani-za-dopomogoiu-stucnogo-intelektu-ta-yix-vikoristannia-v-sudi.

[41] Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

[42] ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.

*Новий Регламент ЄС e-Evidence (2023).*Європейський Союз запровадив революційні зміни, прийнявши Регламент (EU) 2023/1543[43]. Основні нововведення включають:

- *European Production Order (EPOC):* Наказ, що зобов'язує провайдера надати дані протягом 10 днів (або 8 годин у термінових випадках) безпосередньо органу іншої країни ЄС.
- *European Preservation Order (EPOC-PR):* Наказ про негайне заморожування даних, щоб вони не були видалені до моменту отримання основного запиту.

Цей Регламент ігнорує територіальний принцип: провайдер зобов'язаний надати дані, навіть якщо вони зберігаються за межами ЄС, якщо компанія пропонує послуги на європейському ринку. За невиконання передбачено штрафи до 2% від світового обороту компанії.

Технічна процедура фіксації має базуватися на принципах, викладених у міжнародному стандарті ISO/IEC 27037:2012 «Настанови щодо ідентифікації, збирання, отримання та збереження електронних доказів», який в Україні діє як ДСТУ EN ISO/IEC 27037:2022[44]. Стандарт визначає чотири ключові процеси, виконання яких гарантує надійність доказів. А саме: ідентифікацію, збирання, здобуття та збереження.

Фундаментальним принципом за ISO/IEC 27037 є мінімізація оброблення первісних цифрових пристроїв. Будь-які дії, що призводять до зміни стану пристрою (наприклад, увімкнення смартфона для перегляду повідомлень без спеціального обладнання), повинні бути детально описані та обґрунтовані в протоколі. Якщо слідчий самостійно оглядає телефон, він фактично змінює метадані файлів (час останнього доступу), що може бути використано захистом для тверджень про фальсифікацію. Тому стандарт вимагає документування кожного кроку, щоб незалежний експерт міг відтворити дії слідчого та прийти до того ж результату.

Важливою є роль суб'єктів виявлення та вилучення. Крім слідчих, до процесу залучаються інспектори-криміналісти, фахівці Департаменту кіберполіції та експерти Експертної служби МВС. Стандартизація їхньої діяльності через впровадження ДСТУ ISO/IEC 27037 дозволяє уніфікувати вимоги до їхньої кваліфікації та методів роботи, що є критичним для забезпечення допустимості результатів їхньої праці у судовому засіданні.

[43] The E-Evidence Regulation (eER) entered into force on 18 August 2023. After a three-year transition period, it will become binding from 18 August 2026. The Regulation regulates direct cross-border access to electronic evidence by law enforcement authorities of the Member States. URL:https:// www.bfdi.bund.de/EN/Fachthemen/Inhalte/Polizei-Strafjustiz/E-Evidence.html

[44] ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

3. Техніко-криміналістичне та тактичне забезпечення вилучення цифрової інформації

Технічне забезпечення фіксації цифрових слідів пройшло еволюцію від простого копіювання файлів до використання складних програмно-апаратних комплексів (ПАК), що працюють на рівні мікросхем та прошивок. Провідним інструментом у світовій та вітчизняній практиці є комплекс UFED (Universal Forensic Extraction Device), який дозволяє здійснювати фізичне та логічне вилучення даних з тисяч моделей мобільних пристроїв. Функціонал таких комплексів включає можливість обходу блокувань екрана, вилучення видалених повідомлень з месенджерів (Viber, Telegram, WhatsApp), відновлення історії браузерів та геолокаційних даних[45].

Однак ефективність ПАК постійно обмежується вдосконаленням систем безпеки виробниками смартфонів. Вихід нових версій iOS та Android з посиленим шифруванням та протоколами Secure Enclave створює ситуації, коли навіть найсучасніше обладнання не може «пробити» захист[46]. У таких випадках тактика слідчої дії повинна трансформуватися від технічного зламу до використання тактичних прийомів, наприклад, проведення огляду пристрою, поки він знаходиться в розблокованому стані безпосередньо під час затримання («live forensics»)[47].

Для забезпечення незмінності даних під час підключення носія до комп'ютера слідчого обов'язковим є використання блокуваторів запису (Forensic Write Blockers). Ці пристрої на апаратному рівні блокують будь-які команди запису, що надходять від операційної системи до накопичувача, дозволяючи лише читання даних.

Тактичні особливості проведення слідчих дій (огляду, обшуку) за наявності цифрових слідів вимагають суворої послідовності дій. На підготовчому етапі слідчий повинен передбачити наявність засобів ізоляції пристроїв від мережі (клітки Фарадея або авіарежим), щоб запобігти дистанційному видаленню даних (Remote Wipe)[48]. На робочому етапі огляду місця події фіксація повинна відбуватися за принципом «від найбільш летких даних до найменш летких»[49]. Це означає, що спочатку фіксується вміст оперативної пам'яті (RAM) та відкриті вікна програм, і лише після цього пристрій може бути вимкнений для вилучення.

---

[45] Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень , учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Випуск 3(9). С. 111-118.

[46] Курман О.В. Особливості та проблеми виявлення й фіксації цифрових слідів під час огляду мобільних засобів зв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство». Випуск № 04,* 2025, частина 3. С. 238-242.

[47] Караман К.В. Вилучення цифрових слідів під час реалізації ухвали на отримання тимчасового доступу до відомостей, що становлять охоронювану законом таємницю. *Вісник кримінологічної асоціації України* № 36(3). С. 257-267.

[48] Там само.

[49] Коваленко А.В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Випуск 161. С. 202-214.

Процес фіксації у протоколі має бути максимально деталізованим. Недостатньо просто вказати «вилучено мобільний телефон». Необхідно зафіксувати:

1. Точну модель та серійний номер (IMEI) пристрою.
2. Стан пристрою на момент виявлення (увімкнений/вимкнений, підключений до мережі).
3. Наявність та тип засобів блокування (пароль, графічний ключ, FaceID).
4. Метод вилучення (фізичне вилучення пристрою або копіювання інформації на місці).
5. Алгоритм та значення хеш-суми для кожного вилученого масиву даних або фізичного образу носія.

Хеш-сума (hash value) є математичним результатом обробки даних, який є унікальним для кожного набору інформації. Порівняння хеш-сум, розрахованих слідчим під час вилучення та експертом під час дослідження, є головним доказом того, що інформація не була підроблена. Будь-яка зміна хоча б одного біта інформації призведе до повної зміни значення хеш-суми, що робить цей інструмент надійним запобіжником проти маніпуляцій.

Особливим тактичним прийомом є використання Big Data та OSINT (Open Source Intelligence) під час проведення НСРД. Фіксація даних з відкритих джерел (соціальні мережі, форуми) потребує негайної фіксації шляхом створення знімків екрана (скріншотів) та збереження копій вебсторінок, оскільки автори можуть видалити публікації після усвідомлення уваги правоохоронних органів[50]. При цьому важливо фіксувати не лише візуальне відображення, а й HTTP-заголовки та вихідний код сторінки, що дозволяє верифікувати джерело походження інформації[51].

Слід також зазначити, що в умовах триваючої війни з російським агресором цифрові сліди фактично стали ключовим інструментом фіксації їх звірств.

Тут критично важливою є верифікація за допомогою геолокації та аналізу метаданих, щоб довести, що відео було знято саме в Бучі та саме у березні 2022 року. Для цього українські органи активно співпрацюють з Міжнародним кримінальним судом (МКС) та використовують стандарти Протоколу Берклі, які вимагають збереження «цифрового негатива» – первинного файлу без жодних модифікацій[52].

---

[50] Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень , учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Випуск 3(9). С. 111-118.

[51] Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*. 2025. Випуск 91: частина 4. С. 251-259.

[52] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник./ неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/ wp-content/uploads/ 2022/03/Berkeley-ProtocolUkrainian.pdf

4. Типові помилки та проблеми фіксації цифрових слідів у судовій практиці: шляхи вдосконалення

Аналіз судово-слідчої практики свідчить про те, що цифрові сліди часто стають об'єктом жорсткої критики з боку захисту, що призводить до визнання їх недопустимими доказами. Основним каменем спотикання є недотримання встановленої законом процесуальної форми та технічних регламентів[53]. Типові помилки слідчих можна згрупувати за кількома напрямами.

Перша група помилок стосується порушення порядку вилучення. Часто слідчі вилучають комп'ютерну техніку без отримання спеціального дозволу слідчого судді, передбаченого ст. 234-236 КПК, або вилучають «все підряд» без обґрунтування зв'язку пристроїв з предметом доказування[54]. Суди, керуючись доктриною «плодів отруєного дерева», визнають такі докази недопустимими, навіть якщо на них міститься пряме підтвердження вини[55].

Друга група – це технічні помилки при фіксації. Відсутність у протоколі відомостей про розрахунок хеш-сум є однією з найпоширеніших проблем[56]. Без хеш-суми неможливо довести, що файл, який досліджує експерт через два місяці після обшуку, є тим самим файлом, що був знайдений у підозрюваного. Також критичною помилкою є огляд пристрою без залучення спеціаліста, що призводить до випадкової зміни системних файлів або дати доступу, що стає підставою для сумнівів у цілісності даних.

Третя група – помилки у забезпеченні ланцюга зберігання (Chain of Custody). Якщо у матеріалах справи відсутня інформація про те, як доказ транспортувався, де зберігався (наприклад, відсутність сейф-пакетів або їх пошкодження), суд не може бути впевнений, що до носія не мали доступу сторонні особи[57].

Сучасна судова практика Верховного Суду демонструє поступове формування стандартів оцінки електронних доказів. У постанові ККС ВС від 7 грудня 2023 року у справі № 420/15422/22 було акцентовано увагу на тому, що електронне листування є належним доказом, якщо можна встановити його

---

[53] Юр»єв Д.С., Мірошніченко А.О., Забудський О.П. Електронні докази в кримінальному провадженні: практика застосування. *UNIVERSUM*/ 2026. № 28. С. 101-104.

[54] Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Трибуна молодого вченого.* 2021. № 6. С. 273-278.

[55] Використання цифрової інформації в розслідуванні кримінальних правопо рушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. 104 с. DOI: https://doi.org/10.31359/978-966-998-460-9. Techniques and standards for Preservation of Data.

[56] Techniques and standards for Preservation of Data. Digital Forensics 2023-2024. Topic 4. С. 27-38. URL:https://www.uomustansiriyah.edu.iq/media/lectures/6/6_2024_05_10!06_53_48_AM.pdf

[57] Юр»єв Д.С., Мірошніченко А.О., Забудський О.П. Електронні докази в кримінальному провадженні: практика застосування. *UNIVERSUM*/ 2026. № 28. С. 101-104.

походження та автентичність[58]. Суди починають приймати скріншоти месенджерів як докази, але лише за умови, що вони підкріплені оглядом самого пристрою або даними від провайдера. Проте залишається проблема автентичності: у справах про кібершахрайство зловмисники часто використовують спуфінг (підміну номера або імені), що вимагає від суду глибшого аналізу технічних логів, а не лише візуального змісту повідомлень[59].

Для подолання цих проблем та гармонізації українського законодавства з міжнародними стандартами пропонуються такі кроки:

1. Законодавче закріплення поняття «електронний доказ» та «цифровий слід» у КПК України, а також встановлення чіткої процедури їх копіювання як альтернативи вилученню техніки.
2. Розробка та впровадження обов'язкових методичних рекомендацій для слідчих, заснованих на ДСТУ ISO/IEC 27037, щодо порядку ідентифікації та збереження цифрових даних.
3. Створення єдиної цифрової системи обліку речових доказів (e-Evidence), яка б автоматично фіксувала кожен етап «ланцюга зберігання» та інтегрувала значення хеш-сум у електронний протокол.
4. Підвищення рівня кваліфікації слідчих та суддів через спеціалізовані курси з цифрової криміналістики, оскільки нерозуміння різниці між файлом та носієм або між логічним та фізичним образом призводить до судових помилок.

Окремим викликом є використання результатів штучного інтелекту (ШІ) у доказуванні. Вже зафіксовані випадки спроб використання ChatGPT для обґрунтування юридичних позицій[60]. У майбутньому ШІ може використовуватися для аналізу гігабайтів лог-файлів, проте фіксація результатів такого аналізу потребуватиме нових законодавчих визначень та процесуальних гарантій.

ВИСНОВКИ

Фіксація цифрових слідів у сучасному кримінальному процесі є критично важливим етапом, від успішності якого залежить можливість розкриття переважної більшості злочинів. Цифрова трансформація вимагає від криміналістики відмови від застарілих підходів на користь динамічних методів, що базуються на міжнародних стандартах та передових технологіях. Дослідження показало, що цифровий слід є складним інформаційним об'єктом, який характеризується невидимістю, легкістю модифікації та транскордонністю, що обумовлює специфіку його правового режиму.

---

[58] Постанова ККС ВС від 7 грудня 2023 року у справі № 420/15422/22. URL: https://iplex.com.ua/doc.php?regnum=115484427; Судді ВС обговорили судову практику щодо електронних доказів і захист права на приватність при роботі з доказами в умовах застосування штучного інтелекту. URL:https://supreme.court.gov.ua/supreme/pokaznikidiyalnosti/navch_suddiv_praciv__aparativ_2021.

[59] Кохановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2019. № 1(31). С. 13-19.

[60] Огляд судової практики Верховного Суду щодо використання технології штучного інтелекту в судовому процесі (актуальна судова практика станом на 22.07.2025). URL:https://court.gov.ua/storage/portal/sud5023/Scintelekt.pdf.

Основними гарантіями допустимості цифрових доказів є суворе дотримання «ланцюга зберігання», використання апаратних засобів блокування запису та обов'язкова верифікація даних через хеш-функції. Імплементація стандартів ISO/IEC 27037 у вітчизняну практику дозволить мінімізувати суб'єктивний фактор та забезпечити належну якість збирання доказів. Водночас технічний прогрес у сфері шифрування та захисту даних вимагає постійного оновлення парку програмно-апаратних комплексів (як-от UFED) та посилення взаємодії між слідчими органами та підрозділами кіберполіції.

Подальше вдосконалення процесуального законодавства має йти шляхом деталізації процедур роботи з електронною інформацією, впровадження інституту термінового збереження даних та легалізації цифрових методів фіксації (копіювання образу диска). Лише комплексна синергія правових норм, технічних інструментів та фахової компетентності учасників кримінального провадження дозволить ефективно протидіяти викликам злочинності у цифрову епоху.

АНОТАЦІЯ

У статті проведено комплексне дослідження теоретичних та прикладних аспектів функціонування цифрових слідів у сучасній криміналістиці. Визначено понятійно-категоріальний апарат, проаналізовано співвідношення термінів «цифровий слід», «електронний доказ» та «віртуальне відображення». Особливу увагу приділено криміналістичній характеристиці таких слідів, їхнім специфічним властивостям, таким як волатильність, реплікованість та трансмежовість. На основі аналізу останніх досягнень техніко-криміналістичного забезпечення розкрито методику виявлення, фіксації та вилучення цифрової інформації з використанням спеціалізованих апаратно-програмних комплексів. Окремий розділ присвячено аналізу актуальних проблем практичної діяльності, зокрема подоланню шифрування та роботі з хмарними сховищами. Проаналізовано сучасну судову практику Верховного Суду України (2023–2025 рр.) щодо допустимості скріншотів, месенджерів та електронного листування як доказів у кримінальному провадженні. Сформульовано рекомендації щодо вдосконалення процесуального законодавства та імплементації міжнародних стандартів ISO/IEC 27037.

Ключові слова: цифрові сліди, цифрова криміналістика, електронні докази, криміналістична характеристика, судова практика, ланцюжок збереження доказів, Cellebrite UFED, хмарні технології, кіберзлочинність.

Література

1. Коломійцев С.О. Сутність та класифікація цифрових слідів кримінального правопорушення. *Вісник пенітенціарної асоціації України. 2025. №2 (32).* С. 196-205.

2. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, № 4 (100), 2022.* С. 226-236.

3. Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний

університет імені Юрія Федьковича. 27.02.2025. URL:https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist.

4. Цифрові докази війни: як технології допомагають Україні фіксувати злочини Росії. Українські правозахисники та юристи розповіли про нові методи збору доказів воєнних злочинів РФ, які витримують перевірку міжнародних судів URL: https://www.polskieradio.pl/398/7857.

5. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету. Серія Право. Випуск 85: частина 4.* С.71-75.

6. Хижняк Є.С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права.* 2017. Вип.79. С.159-166.

7. Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний електронний журнал. 2023. №10.* С.472-475.

8. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право. 2019. №5.* С. 304-307.

9. Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні / І. О. Крицька // Цифрові трансформації України 2020: виклики та реалії: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу, 18 вересня 2020 р. – Харків: НДІ ПЗІР НАПрН України, 2020. – С. 92-97.

10. Лазебний А.М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10) С.226-233.

11. Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття і види. *Вісник Луганського державного університету внутрішніх справ імені Е.О.Дідоренка.* 2017. №1(77). С.168-175.

12. Гринько Л.П. «Слідова картина» шахрайств, вчинених через мережу Інтернет. *Полтавський правовий часопис.* 2022. №3. С.16-27.

13. Колодіна А.С., Федотова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський правовий часопис.* Випуск 1. С.176-180.

14. Коваленко А.В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності. 2023. Випуск 161*. С.202-214.

15. Курман О.В. Особливості та проблеми виявлення й фіксації цифрових слідів під час огляду мобільних засобів зв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство». Випуск №04, 2025, частина 3.* С.238-242.

16. Науково-практичний коментар Кримінального процесуального кодексу України – науково-методична робота. Станом на 14 квітня 2024 року / За заг. ред. Стратонова В.М. – Київ: Видавничий дім «Професіонал», 2024. – 1208 с.; Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-VI. URL: https://zakon.rada.gov.ua/laws/ show/4651-17#Text.

17. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного

судочинства України та інших законодавчих актів : Закон України від 3 жовт. 2017 р. No 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147-19.

18. Петрик В.В. Використання електронних доказів у кримінальних провадженнях: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського Національного Університету. 2025. Серія Право. Випуск 87: частина 4.* С.119-123.

19. Маркіна А.В. Способи збирання стороною обвинувачення електронних доказів у кримінальних провадженнях щодо воєнних злочинів. *Право.ua. 2025 №4.* С.104-112.

20. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf.

21. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Трибуна молодого вченого. 2021. №6.* С.273-278.

22. Кохановський В.Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник. 2019. №1(31).* С.13-19.

23. Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал. 2021. №8.* С.336-339.

24. Телизіна Я. Оцінка доказів, отриманих в результаті проведення НСРД: частина 2. URL:https://advokatpost.com/pro-otsinku-dokaziv-otrymanykh-u-rezultati-provedennia-nsrd-prokuror-iana-talyzina.

25. Кірчев В.О. Новітні засоби доказування пропозиції, обіцянки або надання неправомірної вигоди службовій особі. *Європейський правничий часопис. 2025. Випуск 6,7.* С.216-223.

26. Колісник О.В., Король С.С. Електронні докази:критерії їх оцінки. *Юридичний науковий електронний журнал. 2024. №4*. С.158-160.

27. Постанова від 29.03.2021 № 554/5090/16-к ВС. Касаційний кримінальний суд. URL:https://verdictum.ligazakon.net/document/96074938.

28. Погорецький М.А. Використання даних ENCROCHAT у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий журнал. 2025. Випуск №8.* С.223-229.

29. Погорецький М.А. Криптовалюта як об’єкт, предмет та засіб вчинення злочину: проблеми виявлення, документування і доказування в досудовому та судовому провадженнях. *Держава і регіони. Серія:Право.* 2025. №3(88). С. 70-90.

30. Стефанів Н. Суддя ВС проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1751385.

31. Наказ Міністерства юстиції України №53/5 від 08.10.1998 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень». URL:https://https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

32. Карпець Ю.В. Цифрові докази та комп»ютерно-технічні експертизи у кримінальних провадженнях про військові злочини. *Юридичний науковий електронний журнал. 2025. №11.* С.226-230.

33. Орещук В. Докази, отримані за допомогою штучного інтелекту, та їх використання в суді. URL:https:// www.hsa.org.ua/blog/dokazi-otrimani-za-dopomogoiu-stucnogo-intelektu-ta-yix-vikoristannia-v-sudi.

34. ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL:https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.

35. The E-Evidence Regulation (eER) entered into force on 18 August 2023. After a three-year transition period, it will become binding from 18 August 2026. The Regulation regulates direct cross-border access to electronic evidence by law enforcement authorities of the Member States. URL: https:// www.bfdi.bund.de/EN/Fachthemen/Inhalte/Polizei-Strafjustiz/E-Evidence.html.

36. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf.

37. Климчук М.П., Кунтій А.І. Виявлення та вилучення слідів кримінальних правопорушень , учинених із використанням засобів стільникового зв'язку. *Соціально-правові студії.* 2020. Випуск 3(9). С.111-118.

38. Караман К.В. Вилучення цифрових слідів під час реалізації ухвали на отримання тимчасового доступу до відомостей, що становлять охоронювану законом таємницю. *Вісник кримінологічної асоціації України №36(3).* С. 257-267.

39. Гловюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету.* 2025. Випуск 91: частина 4. С. 251-259.

40. Юр»єв Д.С., Мірошніченко А.О., Забудський О.П. Електронні докази в кримінальному провадженні: практика застосування. *UNIVERSUM/* 2026. № 28. С.101-104.

41. Використання цифрової інформації в розслідуванні кримінальних правопо рушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. 104 с. DOI:

https://doi.org/10.31359/978-966-998-460-9. Techniques and standards for Preservation of Data.

42. Techniques and standards for Preservation of Data. Digital Forensics 2023-2024.Topic4. С. 27-38. URL: https://www.uomustansiriyah.edu.iq/media/lectures/6/6_2024_05_10!06_53_48_AM.pdf.

43. Постанова ККС ВС від 7 грудня 2023 року у справі № 420/15422/22. URL: https://iplex.com.ua/doc.php?regnum=115484427; Судді ВС обговорили судову практику щодо електронних доказів і захист права на приватність при роботі з доказами в умовах застосування штучного інтелекту. URL: https://supreme.court.gov.ua/supreme/pokazniki-diyalnosti/navch-_suddiv_praciv__aparativ_2021.

44. Огляд судової практики ВС щодо використання технології штучного інтелекту в судовому процесі (актуальна судова практика станом на 22.07.2025).URL:https://court.gov.ua/storage/portal/sud5023/Scintelekt.pdf.

Information about the author:
Dzyurbel Andriy Dariiovych,
Candidate of Legal Sciences,
Senior lecturer of the Department of Criminal Law and Procedure
West Ukrainian National University
11, Lvivska St., 11, Ternopil, 46009, Ukraine
https://orcid.org/0009-0000-1778-8699

DOI https://doi.org/10.30525/978-9934-26-686-7-6

АНАЛІЗ кІБЕРЗЛОЧИННОСТІ У ЗОНАХ ЗБРОЙНИХ КОНФЛІКТІВ (НА ОСНОВІ ДОСВІДУ УКРАЇНИ): ФАКТОРИ ВІКТИМІЗАЦІЇ ТА СТРАТЕГІЇ ПРЕВЕНЦІЇ

Думчиков М. О., Янішевська К. Д., Мурач Д. В.

ВСТУП

З часу ухвалення Конвенції про кіберзлочинність у 2001 році[1] чітко сформувалося усвідомлення зростання загроз для суспільства з боку осіб, які використовують інформаційні технології зі злочинною метою. Ця тенденція закономірно еволюціонує у кібертероризм та кібервійну, що супроводжується відповідним оновленням методів ведення гібридної війни. Досвід застосування кіберзброї під час конфлікту між Росією та Грузією у 2008 році слугує прикладом цієї тенденції[2]. Більше того, висловлюються думки, що підвищення стійкості країн до кіберзагроз може бути досягнуто шляхом освітніх заходів[3], впровадження інноваційних технологій[4] та інших засобів.

Попри це, наразі спостерігається брак досліджень щодо впливу війни на кіберзлочинність у межах країни, які б розглядали це явище відокремлено від інструментального характеру кіберзлочинності як одного з проявів гібридної війни. Такі дослідження забезпечили б підґрунтя для оцінки характеристик цього впливу та, на основі отриманих результатів, розробки специфічної стратегії протидії кіберзлочинності у воєнний час.

Відповідно метою цього дослідження є вивчення потенційного взаємозв'язку між станом війни та рівнем кіберзлочинності в країні задля визначення теоретичної пояснювальної моделі, здатної сприяти формуванню конкретних стратегій для покращення ситуації у сфері кіберзлочинності.

[1] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 09.02.2026).

[2] Galushkin A. A. Education in the Field of National Information Security in the Russian Federation and Abroad. *Journal of Computer Science*. 2015. Т. 11, № 10. С. 988–994. URL: https://doi.org/10.3844/jcssp.2015.988.994.

[3] Filshtinskiy S. Cybercrime, cyberweapons, cyber wars: is there too much of it in the air*? Communications of the ACM*. Vol. 56, № 6. 2023. Pp. 28–30. DOI: https://doi.org/10.1145/2461256.2461266.

[4] Maher D. Can artificial intelligence help in the war on cybercrime?. *Computer Fraud & Security*. 2017. Vol. 2017, no. 8. P. 7–9. URL: https://doi.org/10.1016/s1361-3723(17)30069-6.

1. Онто- та патогенез кіберзлочинності в національному праві України

Окреслення онтогенезу явища в рамках феноменологічного підходу[5], як правило, передбачає 4 кроки: брекетинг (ідентифікація та тимчасове відкладення будь-яких заздалегідь сформованих вірувань та думок, пов'язаних з феноменом дослідження), Intuiting (калькуляція консенсуальних ознак феномену), аналіз (кодування, де проводиться категоризація та усвідомлення значущих смислів феномену), дескрипція (визначення шляхом дефініції)[6]. Позаконтекстуальна (номінальна)[7] форма зображення таких дескрипцій ієрархічно налічує 3 ступені повноти: екстенсіональний, інтенсіональний та змістовний (аналітичний). Найбільш достатнім з епістемологічної точки зору є змістовний ступінь визначення[8]. Однак попри те, що можна сформулювати ще більш точні визначення, це не дасть нам приблизного уявлення про те, чим може бути культивоване поняття для закону[9]. Певний акт може вважатися частиною правової мови не відповідно до певної форми або лексикону, що використовується, але головним чином за позамовними обставинами в контексті, де він виконується[10]. Відповідно надалі продукована дефініція адаптується під конкретний контекст (вимір), що в нашому випадку являє собою вимір права, де отримає нову сутнісну ознаку у вигляді юридичнодетермінованих функцій (функціональний контекстуалізм)[11]. Юридичний (правовий) контекст має власні аутентичні критерії селективного абстрагування множини об'єктів, що до нього входять. Враховуючи те, що мова йде про формальне закріплення явища в правовому вимірі шляхом дефініцій, згадана множина обмежується формальними та неформальними джерелами права. Їх атомічні твердження (норми права та їх положення/частини) виступають в якості засновків юридичного аргументу[12] в межах якого буде проходити правове моделювання дефініції кіберзлочину. З урахуванням достатності висунутої MacColl аргументації, логічний апарат

[5] Brandenburg N. Phenomenology of Law. In: Sellers, M., Kirste, S. (eds). *Encyclopedia of the Philosophy of Law and Social Philosophy*. Springer, Dordrecht. 2023. DOI: https://doi.org/10.1007/978-94-007-6730-0_74-2.

[6] Greening N. Phenomenological Research Methodology. *Scientific Research Journal*. 2019. Vol. VII, no. V. URL: https://doi.org/10.31364/scirj/v7.i5.2019.p0519656.

[7] Naik V., Metallinou A., Goel R. Context Aware Conversational Understanding for Intelligent Agents With a Screen. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2018. Vol. 32, no. 1. URL: https://doi.org/10.1609/aaai.v32i1.11952.

[8] Gupta A., Mackereth S. "Definitions". *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.). URL: https://plato.stanford.edu/archives/fall2023/entries/definitions.

[9] Fincham D. How Law Defines Art (November 7, 2014). *John Marshall Review of Intellectual Property Law*, 2015, Available at SSRN: https://ssrn.com/abstract=2520594.

[10] Glogar O. The Concept of Legal Language: What Makes Legal Language 'Legal'?. *J Semiot Law*, № 3**6**. Pp. 1081–1107. 2023. DOI: https://doi.org/10.1007/s11196-023-10010-5.

[11] Barbir L., Goldstein A. The History of Functional Contextualism. 2016. DOI: 10.13140/RG.2.2.23324.08329.

[12] Рабінович П. М., Дудаш Т. І. Аргументи у правовій аргументації: деякі загальнотеоретичні аспекти. *Вісник Національної академії правових наук України.* 2022. Т. 29. № 3. С. 47–68. DOI: 10.31359/1993-0909-2022-29-3-47.

у цьому разі буде опиратися на базові положення логіки предикатів першого порядку (пропозиційній логіці)[13]. За таких обставин формальними критеріями для висунення джерел права будуть виступати їх легальність[14] та легітимність[15] на території України. Легальність визначається як відповідність Конституції України (ст. 8 Конституції), що додатково передбачає створення та надання юридичної сили акту в передбачених підпорядкованими Конституції НПА процедурам[16]. Легітимність (або правомірність) має проявом суспільне визнання наділення юридичної сили певному акту та відповідність мети акту фундаментальним принципах державотворення у виді верховенства закону, верховенства права тощо. Масив актів обмежується в ієрархічні зв'язки з урахуванням визнаних в Україні міжнародно-правового звичаїв (pacta sunt servanda) та принципів (принцип дружнього ставлення до міжнародного права) та ряду інших базових положень доктрин «дружнього ставлення до міжнародного права» або «координації». Як наслідок, інтеграція міжнародного права в чинну національну систему відбувається шляхом імплементації, яка передбачає ратифікацію міжнародних договорів, згода на які надана Верховною Радою України. При цьому, ратифікація Україною Угоди про асоціацію з ЄС від 27.06.2014 року закріпила курс євроінтеграції[17], що передбачає виконання Україною низки зобов'язань, головним чином похідних від Копенгагенських критеріїв. За таких обставин, і з урахуванням наявності кондиціональних (обов'язкових) умов для асоціації міжнародних угод, якщо в процесі євроінтеграції виникає колізійність між нормами міжнародних договорів, ратифікованих Верховною Радою України, й нормами національного законодавства, пріоритетному застосуванню підлягають норми міжнародних договорів[18]. Таке становище відповідає доктрині радикального монізму з приматом міжнародного права (вихідним з природи Спільнот або «Monism results from Communities nature»), згідно базових положень якої норми міжнародного права де-факто та де-юре домінують над національними[19], що обумовлює ієрархічну домінацію норм міжнародного права над національними,

---

[13] Chevalier J.-M. Some Arguments for Propositional Logic: Maccoll as a Philosopher. *Philosophia Scientiæ*, № 15-1(1). 2011. Pp. 129-147. DOI: https://doi.org/10.4000/philosophiascientiae.368.

[14] Wang S. Varieties of authoritarian legality. *Asia Pacific Law Review*. 2024. P. 1–18. DOI: https://doi.org/10.1080/10192557.2024.2323803.

[15] Toward a multidimensional model of legitimacy: Validation of the Traffic Rules Perceived Legitimacy scale. / F. Varet et al. *Psychology, Public Policy, and Law*. 2024. DOI: https://doi.org/10.1037/law0000416.

[16] Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

[17] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода Україна від 27.06.2014 : станом на 14 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.

[18] Про міжнародні договори України : Закон України від 29.06.2004 № 1906-IV : станом на 15 берез. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1906-15#Text.

[19] Ciongaru E. The monistic and the dualistic theory in European law. *Acta Universitatis George Bacovia*. Juridica, 1, № 1. 2012. Pp. 212-231. URL: http://www.ugb.ro/Juridica/Issue1EN/10_Teoria_monista_si_ dualista_in_dreptul_europeanCiongaruEN.pdf.

звужуючи при цьому нормативний базис для засновків до пріоритетних (ратифікованих) джерел міжнародного права. Виходячи з положень статті 3 Закону України «Про основні засади забезпечення кібербезпеки України»[20] серед міжнародних договорів правову основу забезпечення кібербезпеки України, в тому числі розуміння теоретико-правового концепту «кіберзлочину» (ст. 1), становить Конвенція про кіберзлочинність від 23.11.2001 року та Протоколи до неї[21], логіко-семантичний аналіз положень яких дає підстави до наступних висновків: за способом встановлення значення Конвенція та похідні до неї акти містять розділене екстенсіональне (денотативне) визначення терміну «кіберзлочин». Екстентами (проявами) виступають окремі види кіберзлочинів та їх кваліфікації, що мають відповідники (аналоги або еквіваленти) в чинному кримінальному законодавстві України (Таблиця 1).

Таблиця 1

Кіберзлочини Конвенції про кіберзлочинність та їх українські відповідники

Заголовок Конвенції про кіберзлочинність	Стаття в Конвенції про кіберзлочинність	Відповідник в чинному Кримінальному кодексі України
Правопорушення проти конфіденційності	Ст. 2 – Незаконний доступ	Ст. 361 КК України; Ст. 361-1 КК України; Ст. 361-2 КК України
	Ст. 3 – Нелегальне перехоплення	Ч. 2 ст. 362 КК України
	Ст. 4 – Втручання у дані	Ч. 1 ст. 362 КК України
	Ст. 5 – Втручання у систему	Ст. 361 КК України
	Ст. 6 – Зловживання пристроями	Ст. 363 КК України; Ст. 363-1 КК України
Правопорушення, пов'язані з комп'ютерами	Ст. 7 – Підробка, пов'язана з комп'ютерами	Ч. 1 ст. 362 КК України
	Ст. 8 – Шахрайство, пов'язане з комп'ютерами	Ч. 4 ст. 190 КК України; ст. 200 КК України
Правопорушення, пов'язані зі змістом	Ст. 9 – Правопорушення, пов'язані з дитячою порнографією	Ч. 1-2 ст. 156-1 КК України; Ст. 301-1 КК України
Правопорушення, пов'язані з порушенням авторських та суміжних прав	Ст. 10 – Правопорушення, пов'язані з порушенням авторських та суміжних прав	Ст. 176 КК України

Джерело: створено автором

[20] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

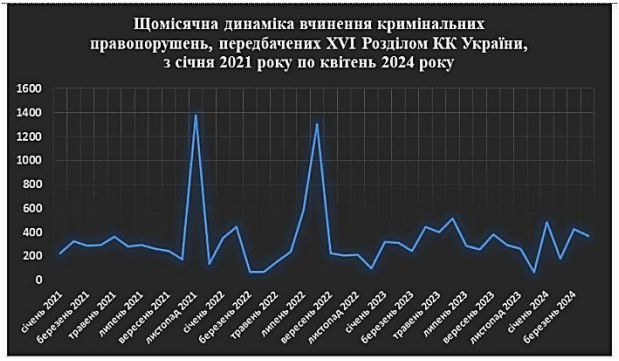
[21] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (укр/рос) : Протокол Ради Європи від 28.01.2003 : станом на 21 лип. 2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.

Концепт кіберзлочину в українській локалізації асоціюється в окремому XVI Розділі «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України, з додатковими уточненнями в інших розділах. Уточнення становлять собою автономні правопорушення в межах категоризації розділів, об'єктивна сторона кваліфікацій яких піддається редукції до тих дій та діянь, що передбачені в Розділі XVI. Наприклад, Ч. 4 ст. 190 КК України є класичним шахрайством (родовий об'єкт шахрайства – власність), що «вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки»[22].

З урахуванням цього щоб визначити рівень, тенденції та закономірності кіберзлочинності на території України необхідно провести статистичне дослідження, основними джерелами якого є офіційні дані (зведені звіти про злочинність), дослідження жертв (національні опитування жертв злочину) та аналіз самоповідомлення. Так, згідно даних Офісу Генерального прокурора України[23], щомісячна динаміка вчинення кримінальних правопорушень, передбачених Розділом XVI КК України, починаючи з січня 2021 року по квітень 2024 року, має 2 точки екстремуму N-max у межах, що підпадають на періоди кінця 2021 року, початку 2022 року (Графік 1).

Графік 1

Щомісячна динаміка вчинення кримінальних правопорушень, передбачених XVI Розділом КК України, з січня 2021 року по квітень 2024 року



Джерело: створено автором

[22] Науково-практичний коментар до статті 190 Кримінального кодексу України: науково-практичний коментар від 01.01.2009 року. LIGA 360. URL: https://ips.ligazakon.net/document/KK004696 (дата звернення: 01.01.2026).

[23] Статистика кримінальної протиправності. Офіс Генерального прокурора України. URL: https://erdr-map.gp.gov.ua/csp/map/index.html#/map (дата звернення: 12.09.2025).

Середньомісячне значення зафіксованих правопорушень за роками становить: 2020 року – 208.17; 2021 року – 359.17; 2022 року – 334.25; 2023 року – 320.08; 2024 року (січень-квітень) – 372.25 інциденти, що вказує на підйом рівня кіберзлочинності починаючи з кінця 2021 року, невеликий спад в 2022/23 рр., та зростання на початку 2024 року.

Більш ґрунтовний аналіз даних потребує завчасного розкриття методологічних прогалин, що можуть вплинути на об'єктивність результатів інтерпретації інформації щодо стану кіберзлочинності. Так, постійні методологічні зрушення побудови якісних статистичних досліджень злочинів ускладнені плутаниною засобів та цілей[24]. Академічні дослідники покладаються на неї, щоб досліджувати причини злочинів, а також його просторові, часові та демографічні особливості. Статистика з правоохоронних органів (наприклад, поліція, в'язниці, суди) використовується для оцінки ефективності, ефективності та справедливості цих установ[25]. Відповідно наших цілей статистика повинна вказувати на об'єктивні процеси, протікаючі в суспільстві, а відтак методологічно повинна мати стандартизований під таку ціль дизайн, що буде враховувати різні «розмиваючі» фактори[26]. Серед таких виділяються: етичні перепони, питання конфіденційності, доступ до первинних або одиничних записів даних, політичні та соціальні зміни в суспільстві[27], особливості досліджуваного виду злочину тощо.

У нашому випадку ми оперуємо офіційними даними суду, правоохоронних органів та інституцій. Статистика правоохоронних органів та інституцій формується з даних, що внесені до Єдиного реєстру досудових розслідувань, передумовою чого є подання заяви, повідомлення про вчинене кримінальне правопорушення або самостійне виявлення слідчим, прокурором з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення. Одним із наслідків завершення досудового розслідування є початок судового провадження, в межах якого відповідальною особою апарату суду вносяться рішення суду до Єдиного державного реєстру судових рішень, що є джерелом судової статистики. Виходячи з цього, визначальними можуть вважатися ті фактори, що будуть перешкоджати реалізації вказаного механізму на будь-якій його стадії. Досліджуваний хронологічний діапазон включає в себе періоди, що мають прямі наслідки для вказаного механізму побудови статистики, а саме: з 22.02.2022 року рф вчинила повномасштабне вторгнення на територію України, що потягнуло за собою в тому числі окупацію значної частини території держави. Вказані території мають спеціальний правовий статус та зафіксовані в Переліку територіальних громад, які розташовані

[24] Fox C., Mackay S., Hope T. The Independent Review of Crime Statistics. *Safer Communities*. 2006. Vol. 5, no. 4. P. 4–12. DOI: https://doi.org/10.1108/17578043200600028.

[25] Warr M., Kirk D. S. Data Bases and Statistical Systems: Crime and Delinquency. *International Encyclopedia of the Social & Behavioral Sciences*. 2015. P. 717–719. DOI: https://doi.org/10.1016/b978-0-08-097086-8.41068-8.

[26] Makkai T. Statistical Systems: Crime. *International Encyclopedia of the Social & Behavioral Sciences*. 2001. P. 15053–15056. DOI: https://doi.org/10.1016/b0-08-043076-7/00011-5.

[27] Maguire M. Criminal Statistics and The Construction of Crime. *The Oxford Handbook of Criminology*. 2012. P. 206–244. DOI: https://doi.org/10.1093/he/9780199590278.003.0008.

в районі проведення воєнних (бойових) дій або які перебувають в тимчасовій окупації, оточенні (блокуванні)[28] та оновленому Переліку територій, на яких ведуться (велися) бойові дії або тимчасово окупованих Російською Федерацією від 22.12.2022 року[29]. При цьому, під час режиму тимчасової окупації, згідно Закону України «Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України», діяльність судових та правоохоронних органів припиняється, і, у разі необхідності такі органи проходять процедуру дислокації та релокації[30]. Так, оновлений Перелік судів, територіальну підсудність яких було змінено у зв'язку з неможливістю здійснювати правосуддя під час воєнного стану станом на 30.10.2023 року включає 201 суд з 10 областей України[31]. Паралельно до цього, за словами Заступника Генерального прокурора Ігоря Мустеца: «На сьогодні у нас відсутня єдина практика розгляду клопотань прокурорів про відновлення внаслідок окупації окремих територій втрачених матеріалів кримінальних проваджень»[32]. Також, починаючи з 24.02.2022 року як тимчасово окупованих, так і на підконтрольних територіях внаслідок збройної агресії рф спостерігалися значні періоди відсутності електропостачання, і, як наслідок зв'язку, що унеможливлює навіть дистанційне повідомлення про кіберзлочин через Систему подачі електронних звернень громадян.

Збройна агресія стимулювала міграційні процеси: починаючи з лютого 2022 року в Україні почалася стрімка хвиля еміграції, і, станом на 21.06.2023 року кількість громадян України, що мігрували закордон, становить 8 177 638 осіб[33]. Вказані фактори прямо впливають як на результати звітної діяльності державних органів, так і на їх інтерпретацію з боку академічної спільноти.

---

[28] Про затвердження Переліку територіальних громад, що розташовані в районі проведення воєнних (бойових) дій або які перебувають в тимчасовій окупації, оточенні (блокуванні) станом на 25 квітня 2022 року : Наказ М-ва з питань реінтеграції тимчасово окуп. територій України від 25.04.2022 № 75 : станом на 27 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/z0453-22#Text (дата звернення: 09.02.2026).

[29] Про затвердження Переліку територій, на яких ведуться (велися) бойові дії або тимчасово окупованих Російською Федерацією : Наказ М-ва з питань реінтеграції тимчасово окуп. територій України від 22.12.2022 № 309 : станом на 20 берез. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/z1668-22#Text (дата звернення: 09.02.2026).

[30] Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України : Закон України від 15.04.2014 № 1207-VII : станом на 19 трав. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1207-18#Text (дата звернення: 09.02.2026).

[31] Перелік судів, територіальну підсудність яких було змінено у зв'язку з неможливістю здійснювати правосуддя під час воєнного стану. *Верховний Суд.* URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/rozporyadjennya/Zagalna_tablica_sudiv_30_10_2023.pdf (дата звернення: 10.05.2024).

[32] В Офісі Генпрокурора обговорили налагодження роботи правоохоронних органів та судових інстанцій, переміщених з тимчасово окупованих територій держави. *Офіс Генерального прокурора.* 2023. URL: https://www.gp.gov.ua/ua/posts/v-ofisi-genprokurora-obgovorili-robotu-pravooxoronnix-organiv-ta-sudovix-instancii-peremishhenix-z-timcasovo-okupovanix-teritorii-derzavi.

[33] Ukrinform. За кордоном перебувають майже 9 мільйонів українців – демограф. *Укрінформ – актуальні новини України та світу.* URL: https://www.ukrinform.ua/rubric-society/3790729-za-kordonom-perebuvaut-majze-9-miljoniv-ukrainciv-demograf.html.

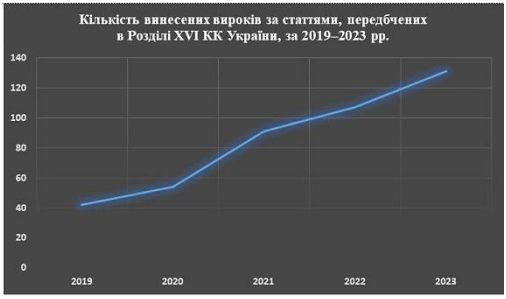
Конкретно ж на результати метричних калькуляцій будуть впливати не всі з перелічених факторів. Мається на увазі, не всі з ним мають значення при роботі з вже наявними даними. Відтак існує сенс акцентувати увагу на тих показниках, які використовують у метричних обчисленнях злочинності, таких як кількість населення у формулі коефіцієнта інтенсивності злочинності.

Відтак, з урахуванням кількості населення в Україні у вказаний період, а саме: 2020 року – 41, 588,4 тис осіб; 2021 року – 41 167,3 тис осіб; 2022 року – 35, 0 млн осіб; 2023 року – 33,2 млн осіб; 2024 року – 33,2 млн осіб [34] [35] [36], маємо наступні показники коефіцієнту інтенсивності злочинності, передбаченої в XVI Розділі КК України, на 10 000 населення: 2020 рік – 0.60; 2021 рік – 1.04; 2022 рік – 1.15; 2023 рік – 1.16; 2024 рік (січень-квітень) – 1.35 випадка. Оперовані статистичні показники містять проміжки, що не вписуються в середньорічний темп приросту, – період починаючи від кінця 2021/початку 2022 року. Паралельно цьому, з 2022 року тримається стала тенденція до збільшення кількості злочинів (темпи приросту), передбачених Розділом XVI КК України, з урахуванням на 10 000 населення.

Виявлені тенденції чітко прослідковуються в даних процесуальних рішень, висунутих за вказаний період часу: у Єдиному реєстрі судових рішень[37] наявна наступна інформація про видані у формі вироку судові рішення по статтям, передбачених за Розділом XVI КК України (Графік 2).

Графік 2

Кількість винесених вироків за статтями, передбчених в Розділі XVI КК України, за 2019–2023 рр.



Джерело: створено автором

[34] Чисельність та склад населення. Держстат. URL: https://stat.gov.ua/uk/datasets/chyselnist-ta-sklad-naselennya.

[35] МВФ оцінив кількість населення України та дав прогноз на найближчі роки. *РБК-Украина*. URL: https://www.rbc.ua/rus/news/mvf-otsiniv-kilkist-naselennya-ukrayini-ta-1713333704.html (дата звернення: 09.02.2026).

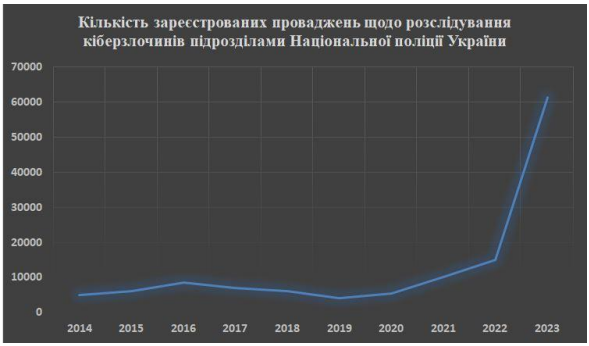
[36] WORLD ECONOMIC OUTLOOK 2024: APR Steady but Slow: Resilience amid Divergence. 2024. 202 p. URL: https://www.imf.org/-/media/files/publications/weo/2024/april/english/text.pdf.

[37] Єдиний реєстр судових рішень. URL: https://reyestr.court.gov.ua/ (дата звернення: 01.01.2025).

Згідно звітних даних Національної поліції України, що оперують унормованим (складеним) концептом кіберзлочинів, за 2014[38], 2015, 2016[39], 2017[40], 2018[41], 2019[42], 2020[43], 2021[44], 2022[45], 2023[46] роки кількість зареєстрованих проваджень щодо розслідування кіберзлочинів підрозділами Національної поліції України підтверджує виявлені в суміжних даних закономірності (Графік 3).

Графік 3

Кількість зареєстрованих проваджень щодо розслідування кіберзлочинів підрозділами Національної поліції України



Джерело: створено автором

[38] Економічна правда. Легкі гроші: Україна перетворюється на Мекку для кіберзлочинців. *Економічна правда*. URL: https://epravda.com.ua/publications/2016/03/28/587004/ (дата звернення: 09.02.2026).

[39] Річний звіт Національної поліції України за 2016 рік. Національна поліція України. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvit_2016.pdf.

[40] Економічна правда. Голова Кіберполіції: "Ваш син у поліції" приносить шахраям на "зоні" мільйон гривень на добу. *Економічна правда*. URL: https://www.epravda.com.ua/publications/2018/01/15/633003/ (дата звернення: 09.02.2026).

[41] Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік. 19 с. URL: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf.

[42] Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. 12 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf.

[43] Звіт Національної поліції України про результати роботи у 2020 році. 14 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf.

[44] Звіт Національної поліції України про результати роботи у 2021 році. 18 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/Zvit_NPU_2021_.pdf.

[45] Звіт Національної поліції України про результати роботи у 2022 році. 14 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf.

[46] Звіт Національної поліції України про результати роботи у 2023 році. 12 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2023/zvit_NPU_2023.pdf.

Аналіз показує, що середній щорічний темп приросту кіберзлочинів за період з 2014 по 2023 роки становить приблизно 53.48%. Для того, щоб визначити (підтвердити) анонормальні проміжки, необхідно порівняти середні щорічні темпи приросту за всі можливі періоди з 2014 по 2023 роки. Так, за період 2014-2015 рр. приріст становив 25.52%; 2014-2016 рр. – 33.31%; 2014-2017 рр. – 16.32%; 2014-2018 рр. – 8.67%; 2014-2019 рр. – 1.54%; 2014-2020 рр. – 4.44%; 2014-2021 рр. – 17.83%; 2014-2022 рр. – 21.82%; 2014-2023 рр. – 53.48%. Ці розрахунки показують, що середній щорічний приріст кіберзлочинів значно коливався протягом аналізованого періоду. Приріст у 2022 році (48.72%) був значно вищим за середній приріст за періоди 2014-2021 (17.83%) і 2014-2020 (4.44%). Однак, найбільш значний приріст спостерігається у 2023 році, що робить середній щорічний приріст за весь період (2014-2023) найбільшим – 53.48%, що в свою чергу підтверджує тезу про аномальне зростання кіберзлочинності починаючи з 2022 року. Більше того, збитки, завдані кіберзлочинами за 2022/23 досягають аналогічного рівня аномальних значень (99,8 та 308,7 млн грн) та не вписуються в жодні прогнозовані показники[47].

Паралельно до цього, національні органи у сфері кібербезпеки, такі як Державна служба спеціального зв'язку та захисту інформації України, диференціюють кіберзлочини та кіберінциденти. Останні являють собою подію або сукупність несприятливих подій ненавмисного характеру або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці інформаційної інфраструктури, створюють імовірність порушення штатного режиму її функціонування, а також ставлять під загрозу захищеність інформаційних ресурсів[48]. Однак як видно з аналізу вказано поняття, об'єктивна сторона що кіберзлочину що кіберінциденту в контексті національного права України однаково охоплюються поняттям «кіберзлочину», що міститься в Конвенції про кіберзлочинність, з відмінністю в тмоу, що в останніх жертвою є держава. Так, кіберінциденти охоплюють широкий спектр дій, направлений на порушення функціонування систем інформаційного захисту, та визначені в окрему Переліку категорій кіберінцидентів, розроблений на основі Переліку категорій кіберінцидентів, що включає наступні категорії: образливий контент, шкідливий код, збір інформації, спроби вторгнення та власне вторгнення, а також порушення доступності, безпека інформаційного наповнення, шахрайство та вразливі системи та інші[49]. За даними Держспецзв'язку саме починаючи з 2022 року почалося стрімке зростання кількості кіберінцидентів на рівні

[47] Звіт Національної поліції України про результати роботи у 2023 році. С. 9-11. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2023/zvit_NPU_2023.pdf.

[48] Про затвердження Інструкції з оцінювання на відповідність міжнародним стандартам оверсайту суб'єктів, які виконують функції центрального депозитарію цінних паперів, центрального контрагента, торгового репозиторію та системи розрахунків у цінних паперах в Україні : Постанова Нац. банку України від 05.04.2024 № 38. URL: https://zakon.rada.gov.ua/laws/show/v0038500-24#Text (дата звернення: 09.02.2026).

[49] Reference Incident Classification Taxonomy Task Force Status and Way Forward. 2018. URL: https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-1%20Good%20practice%20guide%20on%20how%20to%20improve%20CSIRT%20capabilities.pdf.

у 2,8 рази більше ніж у 2021 році[50], а у 2023 році кількість зареєстрованих в Україні кіберінцидентів зросла ще на 62,5% у порівнянні з 2022 роком (всього 1105 кіберінцидентів)[51].

Експертні установи пов'язують таку ситуацію з війною: повідомляється, що російське вторгнення в Україну масово позначилася на кіберзагрозах. З початком війни кібератаки російського походження на електронні адреси європейських та американських компаній збільшилися у 8 разів[52]. 97% організацій помітили зростання кіберзагроз з початку російсько-української війни в 2022 році, що демонструє глибокий вплив геополітичних напруг на кібербезпеку[53]. Масовані кібератаки проти державних структур України та бізнесу посилились з початку агресії рф[54]. Кібератаки є звичним проявом аргесії під час введення гібридної війни і на правлення на підрив стабільності інституцій супротивника. При цьому, гіпотеза війни як індукуючого фактору дозволяє також пояснити зростання кіберзлочинності в кінці 2021 року: паралельно з масовими повідомленнями в інформаційному просторі України в другій половині 2021 року про наміри початку воєнної агресії за боку зс рф[55], дані Google Trends з теми «війна» та окремі запроси «війна», «война», «war» на території України показують приріст веб-пошукових запросів та публікацій на вказану тематику саме в ці проміжки[56].

Перелічені обставини вказують на наявність надвисокого ступеня кореляційного зв'язку між фактом початку повномасштабного вторгнення рф на територію України і аномальним зростанням кіберзлочинності, навіть незважаючи на такі обставини, як велика міграція населення, криза, періоди блекауту, окупація, зменшення чисельності компетентних правоохоронних органів на тимчасово окупованих територіях та інших, що в сукупності повинні давати діаметрально протилежний ефект. Подібне зумовлює наступне припущення: війна обумовлює приріст кіберзлочинності. Однак не зрозуміло яким чином, адже враховуючи демаркацію кіберіндицдентів від кіберзлочинів при побудові статистики, стає очевидним, що аномальне зростання не пов'язане з

[50] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022 рік. 10 с. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf.

[51] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023 рік. 12 с. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a.

[52] The Latest Cyber Crime Statistics (updated October 2025) | AAG IT Support. *AAG IT Services*. URL: https://aag-it.com/the-latest-cyber-crime-statistics/.

[53] How cybersecurity boosts enterprise reinvention to drive business resilience: State of Cybersecurity Resilience 2023. 39 p. URL: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf.

[54] Інформаційне повідомлення. Комітет з питань цифрової трансформації інформує про кібератаки, роботу мобільних операторів та інформаційну безпеку. *Офіційний портал Верховної Ради України*. URL: https://www.rada.gov.ua/print/221400.html (дата звернення: 09.02.2026).

[55] Михайлов Д. Путін прийняв рішення про початок повномасштабної війни проти України на початку 2021 року – ЗМІ. *Суспільне новини*. 2023. URL: https://suspilne.media/456759-putin-prijnav-risenna-pro-pocatok-povnomasstabnoi-vijni-proti-ukraini-na-pocatku-2021-roku-zmi/.

[56] Google Trends. *Google corp*. URL: https://trends.google.com.ua/trends/.

агресією в рамках гібридної війни[57], що вказує на інший вплив війни як фактора збільшення кіберзлочинності.

2. Війна як фактор віктимізації кіберзлочинності

У соціологічних дослідженнях статистичні моделі можуть бути використані для аналізу причинності явищ (казуація), передбачення майбутніх результатів (предикція та прогнозування) та опису поточного стану суспільства або групи осіб (дескрипція). Кожна з цих пізнавальних функцій є важливою для розуміння соціальних явищ і процесів, однак найбільш значимою областю дослідження є казуація (причинність або причинно-наслідкові зв'язки) і вона ж є найбільш проблемною для інтерпретації[58]. Це, в тому числі, обумовлює обмеженість усіх статистичних моделей, хоча і не принижує їх цінність для науки, особливо в питаннях постановки кореляційних зв'язків сильно проявлених явищ, що спостерігаються в серйозних зрушеннях статистичних показників.

Загалом же предикторами зрушень поліцейської статистики можуть бути: (1) методологічні зміни правил збирання, оброблення та оформлення отриманих даних; (2) емпіричні сутнісні зміни досліджуваного об'єкта; (3) компіляція в певному відношенні обох варіантів одночасно. Методологія збирання інформації про кіберзлочинність визначена в правових актах уповноважених правоохоронних органів, проявлена у відповідності до визначених форм. Так, порядок формування Єдиного реєстру досудових розслідувань наряду з формами звітності органів Національної поліції України не змінювалися за досліджуваний період, що виключає перший та третій варіанти одночасно. Аналогічна ситуація з судовою статистикою: форма звітності про діяльність місцевих, апеляційних та судів касаційної інстанції, паралельно з правилами формування Єдиного реєстру судових рішень та ведення Автоматизованої системи документообігу суду за досліджуваний період пройшли оновлення, що не мали якісного впливу на результативність суду, а тим паче на показники злочинності. Відповідно предиктором аномальних змін є видозміна об'єкта дослідження, а саме злочинності.

Сам же феномен злочинності, його природа в елементах причин, наслідків, закономірностей та внутрішніх законів динаміки й розвитку в сукупності та окремо виступають в якості предмету досліджень низки академічних дисциплін, таких як антропологія[59], біологія[60], психіатрія[61], психологія[62],

[57] Simons G., Danyk Y., Maliarchuk T. Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace & Security*. 2020. Vol. 32, no. 3. P. 337–342. DOI: https://doi.org/10.1080/14781158.2020.1732899.

[58] Pearl J. Causal inference in statistics: An overview. *Statistics Surveys*. 2009. Vol. 3. P. 96–146. URL: https://doi.org/10.1214/09-ss057.

[59] Schneider J., Schneider P. The Anthropology of Crime and Criminalization. *Annual Review of Anthropology*. 2008. Vol. 37, no. 1. P. 351–373. DOI: https://doi.org/10.1146/annurev.anthro.36.081406.094316.

[60] Ling S., Umbach R., Raine A. Biological explanations of criminal behavior. *Psychology, Crime & Law*. 2019. Vol. 25, no. 6. P. 626–640. DOI: https://doi.org/10.1080/1068316x.2019.1572753.

соціологія[63], юриспруденція[64], економіка[65] та багатьох інших. Кросдисциплінарні[66], інтердисциплінарні[67], мультидисциплінарні[68] та трансдисциплінарні[69] зв'язки з теоретичними концептами різних об'єктів науки, що визнаються в якості детермінантів девіантної поведінки, в межах монодисциплінарності зосереджуються в кримінології. Кримінологія, в свою чергу, традиційно не враховувала «повний життєвий шлях» суб'єкта при спробах пояснити антисоціальну та злочинну поведінку. У результаті чого було пропущено важливі відомості про кримінальні траєкторії та передумови для антисоціальності та злочинності[70]. Надаючи теоретичні концепти злочинності, кримінологи намагаються дати відповідь на питання: чому виникає подібна поведінка, і як з цього розуміння можна їй запобігти. Це відбувається за допомогою таких властивостей теорій, що називаються науковими чеснотами (theoretical virtues)[71]. До стандартних теоретичних чеснот належать: перевірюваність, емпірична точність, простота, уніфікація, несуперечливість, когерентність та плідність[72]. Ортодоксальні цілі та суспільні очікування від вчених-кримінологів та кримінології як наукової дисципліни обумовлюють переважаюче становище саме, витікаючого з казуації прогностичного

---

[61] Sathyanarayana Rao T. Psychiatrist and the science of criminology: Sociological, psychological and psychiatric analysis of the dark side. *Indian Journal of Psychiatry*. 2007. Vol. 49, no. 1. P. 3. DOI: https://doi.org/10.4103/0019-5545.31511.

[62] Bartol C., Bartol A. *Criminal behavior: A psychological approach* (12th edition.). 2021. Boston: Pearson.

[63] Shahid A. Sociological theories of crime. 2022. DOI: 10.13140/RG.2.2.17683.66081.

[64] Waite J. The Legal Approach to Crime and Correction, 23 *Law and Contemporary Problems* 594-610 (Fall 1958). URl: https://scholarship.law.duke.edu/lcp/vol23/iss4/3.

[65] Becker G. Crime and Punishment: An Economic Approach. *The Journal of Political Economy*. № 176. P. 176–177. 1968. URL: https://masonlec.org/site/rte_uploads/files/JEP/Readings/Butler%20Economic%20Analysis%20for%20Lawyers%203rd%20ed/CH%20VII%20Crime.pdf.

[66] Skrzypiec G. Adolescents' Intentions to Engage in Criminal Activity: A Cross-Disciplinary Approach Linking Theories From Social Psychology and Criminology. *Journal of Forensic Psychology Research and Practice*. 2017. Vol. 17, no. 5. P. 305–337. DOI: https://doi.org/10.1080/24732850.2017.1374720.

[67] Walsh A, Criminology: An Interdisciplinary Approach. *Faculty & Staff Authored Books*. 2007. URL: https://scholarworks.boisestate.edu/fac_books/93.

[68] Taylor S. Crime and Criminality. Routledge, 2015. DOI: https://doi.org/10.4324/9781315713298.

[69] Yanishevska K., Kosiachenko K., Kamyshanskyi O., Neviadovskyi V., Telizhenko L. Transdisciplinary theory of the nature of crime as an expression of a symbiotic complex approach. *Revista Amazonia Investiga*, № *12*(66). 2023. Pp. 188–197. DOI: https://doi.org/10.34069/AI/2023.66.06.18.

[70] Farrington D. P. Introduction to Integrated Developmental and Life-Course Theories of Offending. *Integrated developmental and life-course theories of offending*. 2017. P. 1–15. URL: https://doi.org/10.4324/9780203788431-1.

[71] Schindler S. Theoretical virtues: do scientists think what philosophers think they ought to think?. *Philosophy of Science*. 2022. P. 1–31. DOI: https://doi.org/10.1017/psa.2021.40.

[72] Schindler S. Theoretical Virtues in Science. 2020. DOI: 10.1093/obo/9780195396577-0409.

потенціалу (функції) теоретичного концепту злочинності, адже саме він надає превентивний інструментарій.

Так, наразі існує низка різноманітних теорій злочинності: загальна теорія злочинності розглядає низький рівень індивідуального самоконтролю як ключовий детермінант кримінальної поведінки[73]; критична теорія злочинності інтерпретує правопорушення як реакцію на наявну в суспільстві нерівність у розподілі влади та матеріальних благ[74]; теорія розвитку або життєвого шляху, що пов'язує виникнення злочинності із взаємодією процесів індивідуального розвитку та несприятливих факторів зовнішнього середовища[75]; теорія соціального навчання, згідно з якою протиправна поведінка засвоюється через взаємодію із соціальним оточенням[76]; теорія раціонального вибору, яка передбачає, що перед вчиненням злочину індивід зважує потенційні ризики й вигоди[77]; загальна теорія вибору, де суб'єкт обирає вчинити злочин, розглядаючи перед собою можливості, відважуючи користь проти покарання і вирішуючи, чи йти далі чи ні[78]; Класичні теорії згідно яких люди раціональні, мають свободу волі і відповідальні за свої дії, а також скоєні злочини[79]; Теорія конфліктів як форма критичної теорії, що ґрунтується на працях Карла Маркса та Макса Вебера, і наголошує на нерівностях у суспільстві, таких як матеріальні блага, влада, клас, і як ці нерівності впливають на життєвий досвід та шанси особистостей, створюючи конфлікти між та всередині соціальних груп[80]; теорія особистісних рис, згідно якої у людей є певні риси, які можуть призвести до того, чи вони здатні вчинити злочин, коли їх тягне у певному напрямку або коли вони перебувають у стані стресу[81]; теорії напруги (стресу) стверджують, що деякі напруги або стресори збільшують ймовірність насильства. Ці стреси збентежують осіб, створюючи тиск для коригувальних

[73] Gottfredson M. R., Hirschi T. *A general theory of crime.* Stanford University Press. 1990. URL: https://psycnet.apa.org/record/1990-97753-000.

[74] Cullen F. T., Wilcox P. Encyclopedia of Criminological Theory. SAGE Publications, Incorporated, 2010. DOI: http://dx.doi.org/10.4135/9781412959193.n208.

[75] Moffitt T. E. Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review, № 100*(4). 1993. Pp. 674–701. DOI: https://doi.org/10.1037/0033-295X.100.4.674.

[76] Social Learning and Deviant Behavior: A Specific Test of a General Theory / R. L. Akers et al. *American Sociological Review*. 1979. Vol. 44, no. 4. P. 636. DOI: https://doi.org/10.2307/2094592.

[77] Scott M. The Reasoning Criminal / ed. by D. B. Cornish, R. V. Clarke. Routledge, 2017. DOI: https://doi.org/10.4324/9781315134482.

[78] Glasser W. *Choice theory: A new psychology of personal freedom.* HarperPerennial. 1999. URL: https://psycnet.apa.org/record/1999-02074-000.

[79] Early and Classical Criminological Theories. *SAGE Publications*. 2020. 26 p. URL: https://www.sagepub.com/sites/default/files/upm-assets/97953_book_item_97953.pdf.

[80] Schneewind K. A. Socialization and Education: Theoretical Perspectives. *International Encyclopedia of the Social & Behavioral Sciences*. 2015. P. 861–865. URL: https://doi.org/10.1016/b978-0-08-097086-8.92071-3.

[81] Mann R. D. A review of the relationships between personality and performance in small groups. *Psychological Bulletin,* № 56(4). Pp. 241–270. 1959. DOI: https://doi.org/10.1037/h0044587.

дій[82]; теорія соціальної дезорганізації визначає, що злочин відбувається в спільнотах, де руйнується соціальні норми та можливості, наприклад, у великих міських спільнотах з низьким рівнем доходів[83]; позитивістська школа виходить із того, що злочинна поведінка є наслідком дії об'єктивних факторів, які не залежать від волі індивіда. У межах цього підходу розрізняють індивідуальний та соціологічний напрями, причому біологічні теорії позитивізму часто характеризуються як такі, що мають псевдонаукове підґрунтя[84]. І хоча всі ці концепти намагаються пояснити в різних аспектах один і той же феномен, проте в них є спільні елементи, що відкривають можливість для систематизації. Так, за підходами теорії злочинності класифікують на біологічні та соціологічні[85]. Кожна як окремо взята теорія так і їх умовні категорії мають свої переваги та недоліки в тих чи інших питаннях у порівнянні з іншими[86], і при цьому жоден з підходів в межах класичної кримінології, як було зазначено вище, наразі не може пояснити весь масив випадків, що постають перед спеціалістами з питань злочинності[87], і, відповідно надати точний інструментарій для прогнозування злочинності. Великий потенціал наразі вбачається в синергетичному (емерджентному «emergence») підході, що поєднує центральні положення вказаних течій в межах однієї двохфакторної моделі психодевіації, що на сьогодні представлена в епігенетичних дослідженнях[88]. Теоретичне підгрунтя епігенетики тримається на постулатах, що (1) протиправна (злочинна) поведінка асоційована з девіантною або руйнівною (disruptive behaviour (DB)) (aggression, opposition-defiance, rule breaking, and stealing-vandalism)[89]), остання

[82] Agnew R. S. Strain theory and violent behavior. In D. J. Flannery, A. T. Vazsonyi, & I. D. Waldman (Eds.), *The Cambridge handbook of violent behavior and aggression*. Pp. 519–529. 2007. Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511816840.027.

[83] Wong C. Clifford R. Shaw and Henry D. McKay, The Social Disorganization Theory. *CSISS Classics*. *UC Santa Barbara: Center for Spatially Integrated Social Science*. 2002. URL: https://escholarship.org/uc/item/47j411pr.

[84] Positivist Criminology | Overview & Theory. URL: https://study.com/academy/lesson/positivist-criminology-definition-theory.html#:~:text=The%20positivist%20theory%20in%20criminology%20states%20that%20individuals%20commit%20crimes,positivism%20is%20based%20on%20pseudoscience.

[85] Theories and causes of crime. University of Glasgow. 9 p. URL: https://www.sccjr.ac.uk/wp-content/uploads/2016/02/SCCJR-Causes-of-Crime.pdf.

[86] Kavish N., Boutwell B. The unified crime theory and the social correlates of crime and violence: problems and solutions. *Journal of Criminal Psychology*. 2018. Vol. 8, no. 4. P. 287–301. URL: https://doi.org/10.1108/jcp-06-2018-0028.

[87] Ilan J. Dorine W. Biological theories of crime versus psychological theories of crime – Comparison and evaluation of their contributions to our understanding of crime and/or criminal justice. 2017. 23 p. DOI: 10.13140/RG.2.2.14740.14726.

[88] From 1957 to Nowadays: A Brief History of Epigenetics / P. Peixoto et al. *International Journal of Molecular Sciences*. 2020. Vol. 21, no. 20. DOI: https://doi.org/10.3390/ijms21207571.

[89] Tremblay R. E. Developmental origins of disruptive behaviour problems: the 'original sin' hypothesis, epigenetics and their consequences for prevention. *Journal of Child Psychology and Psychiatry*. 2010. Vol. 51, no. 4. P. 341–367. DOI: https://doi.org/10.1111/j.1469-7610.2010.02211.x.

в свою чергу з патологічною в контексті середовища (географічний детермінізм[90]), зокрема виділяється критерій «агресивності» (імпульсивності) як один із метричних чинників, що піддаються впливу; (2) злочин є поведінковим наслідком індукованої змінами навколишнього середовища експресії та/або метиляції генів: молекулярно-генетичні дослідження на тваринах і людях виявили численні гени, залучені до дофамінергічної, серотонінергічної та адреналіно-норадреналінської нейротрансмісії, які тісно пов'язані з насильницькими правопорушеннями, зовнішньою поведінкою та нижчим «гальмівним» контролем[91]. Найбільш дослідженими нас сьогоні є гени моноамінoксидази А (MAOA)[92], рецепторів допаміну (DRD2, DRD3, DRD4 тощо)[93] і гени транспортера серотоніну (5-HTT або SLC6A4)[94]. Показано, що генетично залежні процеси нейророзвитку впливають на здатність поступово контролювати агресивну поведінку[95], при цьому, середовище та детермінований ним суб'єктивний досвід індивіда відіграють колосальну роль у формуванні патернів поведінки в довгостроковій перспективі певним чином впливаючи на вказані нейробіологічні мозкові системи[96]. І хоча наразі немає точного концепту універсального деваінтноіндукуючого досвіду (або умов), проте проспективні лонгітюдні дослідження надали більшість доказів, які пов'язують певні фактори ризику з пізнішими правопорушеннями чи кримінальними правопорушеннями та фактично виявили численні предиктори такої поведінки. Так, до прикладу, негаразди, пережиті під час пренатального життя, дитинства та підліткового віку, заважають нормальним процесам проліферації та диференціації клітин, що призводить до змін нейронних ланцюгів, які були пов'язані з агресивною поведінкою та зовнішнім спектром

[90] Hong S. Environmental and Geographic Determinism: Jared Diamond and His Ideas. In: Wiarda, H.J. (eds) Grand Theories and Ideologies in the Social Sciences. Palgrave Macmillan, New York. 2010. DOI: https://doi.org/10.1057/9780230112612_9

[91] Tremblay R. E., Vitaro F., Côté S. M. Developmental Origins of Chronic Physical Aggression: A Bio-Psycho-Social Model for the Next Generation of Preventive Interventions. *Annual review of psychology*, № 69. Pp. 383–407. 2018. DOI: https://doi.org/10.1146/annurev-psych-010416-044030.

[92] Gene expression analysis of MAOA and the clock gene ARNTL in individuals with bipolar disorder compared to healthy controls / S. Bengesser et al. *The World Journal of Biological Psychiatry*. 2021. P. 1–19. DOI: https://doi.org/10.1080/15622975.2021.1973816.

[93] Anxiety, aggression, reward sensitivity, and forebrain dopamine receptor expression in a laboratory rat model of early-life disadvantage / J. S. Lonstein et al. *Developmental Psychobiology*. 2023. Vol. 65, no. 7. DOI: https://doi.org/10.1002/dev.22421.

[94] Genes and Aggressive Behavior: Epigenetic Mechanisms Underlying Individual Susceptibility to Aversive Environments / S. Palumbo et al. *Frontiers in Behavioral Neuroscience*. 2018. Vol. 12. DOI: https://doi.org/10.3389/fnbeh.2018.00117.

[95] Genetic and Environmental Influences on the Developmental Course of Attention-Deficit/Hyperactivity Disorder Symptoms From Childhood to Adolescence / J.-B. Pingault et al. *JAMA Psychiatry*. 2015. Vol. 72, no. 7. P. 651. DOI: https://doi.org/10.1001/jamapsychiatry.2015.0469.

[96] Iofrida C., Palumbo S., Pellegrini S. Molecular genetics and antisocial behavior: Where do we stand?. *Experimental Biology and Medicine*. 2014. Vol. 239, no. 11. P. 1514–1523. DOI: https://doi.org/10.1177/1535370214529508.

розладів (наприклад, проблеми з контролем поведінки[97]). Спільною рисою усіх таких досвідів та умов є їхня стрессовість для особи[98]. Екстремальні стресогенні умови асоціюються з «життям в гарячих точках», під час збройних конлфіктів/окупації зокрема. Згідно з представленною Р. Лешем та Д. Вайсбурдом моделлю, воно пов'язане з профілем ДНК, суміжним із насильством, відповідно взаємодіє з механізмами розвитку мозку, що, у свою чергу, може призвести до збільшення показника агресивності, що є предиктором злочинності[99]. Однак наслідки хронічного неконтрольованого стресу для психіки людини в цілому залежать від наявних у неї генетичних, фізіологічних та психічних передумов, що формують схильності до певних станів: розглядаючи цю тезу в категоріях A Theory Of Crime Resistance And Susceptibility, де резистентність та сприятливість є функціями чинників, які впливають на сприйняття та інтерпретацію криміногенних подій та умов, емоційну реакцію на них та поведінкові нахили, які вони спонукають[100], можна стверджувати, що в залежності від закладених схильностей наслідки криміногенних подій можуть мати або криміногенний вплив на агресора (зменшуючи резистентність) або віктимізуючий вплив на жертву (впливаючи на її сприятливість). В обох випадках в довгостроковій перспективі це буде мати якісний стимулюючий вплив на фактичну ситуацію зі злочинністю, але менш очевидним та конктретним буде вплив на показники поліцейської статистики, якраз таки через методолоічні та інші проблеми, що зумовлюють неспроможність її відображати картину стану злочинності в суспільстві повно. Відтак, згадуючи такі специфічні ознаки, передбачених в поліцейській статистиці кіберзлочинів, як їх відчужений (дистанційний), переважно анонімний характер, успіх в реалізації злочинного наміру з боку кіберзлочинця цілком буде залежати від його здатності ввести в оману людину шляхом маніпуляції інформацією в мережі, що виступає в якості інструменту вчинення злочину. Враховуючи, що за вказаний період у звітах Національної поліції України відсутні будь-які згадки про новітні методи та способи вчинення кіберзлочинності, причина росту в більшій мірі зводиться до зміни здатності критичного протистояння злочинному наміру з боку потенціальної жертви, тобто до її віктимності. Показниками віктимності в цьому разі виступають розуміння характеру та значення (1) інформації в мережі, тобто можливість її ідентифікації як злочинної; (2) власних дій та їх наслідків щодо цієї інформації, а також спроможність давати супротив протиправному впливу. Додатково, вказані особливості кіберзлочинів на практиці обмежують визначений

[97] Genes and Aggressive Behavior: Epigenetic Mechanisms Underlying Individual Susceptibility to Aversive Environments / S. Palumbo et al. *Frontiers in Behavioral Neuroscience*. 2018. Vol. 12. DOI: https://doi.org/10.3389/fnbeh.2018.00117.

[98] Dee G., Ryznar R., Dee C. Epigenetic Changes Associated with Different Types of Stressors and Suicide. *Cells, № 12*(9). 2023. DOI: https://doi.org/10.3390/cells12091258.

[99] Leshem R., Weisburd D. Epigenetics and Hot Spots of Crime: Rethinking the Relationship Between Genetics and Criminal Behavior. *Journal of Contemporary Criminal Justice*. 2019. Vol. 35, no. 2. P. 186–204. DOI: https://doi.org/10.1177/1043986219828924.

[100] Agnew R. A Theory Of Crime Resistance And Susceptibility. *Criminology*. 2016. Vol. 54, no. 2. P. 181–211. DOI: https://doi.org/10.1111/1745-9125.12104.

статею 214 КПК України[101] перелік підстав для внесення відомостей про кримінальне правопорушення до ЄРДР, що є першоумовою формування поліцейської статистики в нашому випадку, виключно до повідомлення про факт вчинення такого злочину жертвою. Відтак зрушення статистики будуть пов'язані в більшій мірі саме з віктимізуючими процесами, адже саме від здатності особи ідентифікувати злочинний вплив наряду з розвинутою ассертивністю, залежить чи буде вона вчиняти опір взагалі. Ключовою психічною характеристикою у такому разі буде здатність до критичної оцінки (критичного мислення) навколишньої реальності наряду зі тією ж самою ассертивністю, загальним психологічним тонусом та суміжними характеристиками психіки, що детермінують як малу ймовірність реалізації злочинного наміру.

Отже, стан війни асоціюється з умовами надвисокого хронічного неконтрольованого стресу, що індукує експресію/метиляцію наборів генів, пов'язаних з певними психічними захворюваннями та/або дефіцитними станами, спільним симптомом яких є дегенрація когнітивних здібностей людини, що, в свою чергу, проявляється зниженням здатності до критичного мислення, що є прямим предиктором збільшення вірогідності стати жертвою кіберправопорушення (фактор віктимізації). Враховуючи, що наповненість поліцейської статистики кіберзлочинів залежить від кількості повідомлень про інциденти завершених кіберзлочинів, а успіх реалізації злочинного наміру кіберзлочинця, в свою чергу, за умови сталості методів залежить від сприятливості особи до кіберзлочину, то створення віктимізуючих умов в суспільстві може відображатися в аномальних зрушеннях поліцейської статистики кіберзлочинності.

Подібна гіпотеза вписується в концепт епігенетики та має підтвердження в межах аналогічних ситуацій. Зниження критичного мислення можна розглядати як симптом індукованого проживанням під час війни, як правило, стрес-асоційованим та тавма-асоційованим розладом включно з тривожністю, депресією, посттравматичним стресовим розладом, гострим стресовим розладом, психозом тощо[102], або загостренням вже наявної патології[103]. Афективні переживання в межах травматичного досвіду життя в гарячих точках можуть мати деструктивний характер та культивувати наслідки 2 типів (1) психоедукація: монотравма (гостра стресова реакція, розлади адаптації), мультитравма (ПТСР); та (2) стабілізація: секвенційна травма (фобії, депресія, соматоформні розлади залежності як коморбідні розлади), травма розвитку

[101] Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 1 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 09.02.2026).

[102] Carpiniello B. The Mental Health Costs of Armed Conflicts–A Review of Systematic Reviews Conducted on Refugees, Asylum-Seekers and People Living in War Zones. *International Journal of Environmental Research and Public Health*. 2023. Vol. 20, no. 4. P. 2840. DOI: https://doi.org/10.3390/ijerph20042840.

[103] Hassan G, Ventevogel P, Jefee-Bahloul H, Barkil-Oteo A, Kirmayer LJ. Mental health and psychosocial wellbeing of Syrians affected by armed conflict. *Epidemiology and Psychiatric Sciences*. 2016, № 25(2). Pp. 129-141.DOI: 10.1017/S2045796016000044.

(дисоціативні розлади, комплексний ПТСР)[104]. Усі з перелічених станів, незалежно від того чи були вони набутими внаслідок війни чи мали загострення через індукований нею стрес, виступають в ролі віктимізуючих факторів кіберзлочинності, та, скоріше за все, класичної злочинності в тому числі.

3. Стратегії превенції кіберзлочинності під час війни (на основі досвіду України)

Через ескалацію конфлікту наразі неможливо надати точні показники захворюванності на психічні розлади серед населення України, однак очевидним є факт, що такі показники знаходяться на своєму історичну піку. Прогнози та оцінки поширеності психічних розладів серед населення України містять доволі страшні цифри: за оцінками МОЗ України психологічної підтримки потребуватимуть до 15,7 млн українців, із них майже 3–4 млн – - медикаментозного лікування[105]; з дослідження 9 795 респондентів лише 11% назвали свій психічний стан стабільним[106]; експертні оцінки вказують, що 40–50% населення потребуватимуть психологічної допомоги[107], при чому прогнозована потреба в допомозі на первинній ланці медицини – 27 млн звернень[108]; ВООЗ також прогнозує, що до 2025 року 50% українців можуть зіткнутися з проблемами у сфері ментального здоров'я[109]. Такі індуковані війною психодефіцитні стани можуть мати різне походження: внаслідок міграції[110], перебування в зоні та поза зоною (в безпечному регіоні,

[104] Childhood traumas: an outline and overview. *American Journal of Psychiatry*. 1991. Vol. 148, no. 1. P. 10–20. DOI: https://doi.org/10.1176/ajp.148.1.10.

[105] Вплив війни на психічне здоров'я – колосальний, – Віктор Ляшко. *Міністерство охорони здоров'я України*. 2022. URL: https://www.kmu.gov.ua/news/vpliv-vijni-na-psihichne-zdorovya-kolosalnij-viktor-lyashko (дата звернення: 09.02.2026).

[106] Психічне здоров'я в умовах війни: як громадські організації підтримувані ПРООН надають психологічну допомогу українцям. United Nations Development Programme. URL: https://www.undp.org/uk/ukraine/news/psykhichne-zdorovya-v-umovakh-viyny-yak-hromadski-orhanizatsiyi-pidtrymuvani-proon-nadayut-psykholohichnu-dopomohu-ukrayintsyam.

[107] Зеленська про програму ментального здоров'я: Виявилося, що «сильні не ходять до психологів». *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-society/3703135-zelenska-pro-programu-mentalnogo-zdorova-viavilosa-so-silni-ne-hodat-do-psihologiv.html (дата звернення: 09.02.2026).

[108] У межах Всеукраїнської програми ментального здоров'я визначили пріоритетні проєкти. *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-society/3695613-u-mezah-vseukrainskoi-programi-mentalnogo-zdorova-viznacili-prioritetni-proekti.html (дата звернення: 09.02.2026).

[109] Маємо переплавити жахливий досвід на посттравматичне зростання – перша леді на Міжвідомчій координаційній раді з питань охорони психічного здоров'я – Офіційне інтернет-представництво Президента України. *Офіційне інтернет-представництво Президента України*. URL: https://www.president.gov.ua/news/mayemo-pereplaviti-zhahlivij-dosvid-na-posttravmatichne-zros-80849 (дата звернення: 09.02.2026).

[110] Mental health of migrants with pre-migration exposure to armed conflict: a systematic review and meta-analysis / C. Mesa-Vieira et al. *The Lancet Public Health*. 2022. Vol. 7, no. 5. P. e469-e481. DOI: https://doi.org/10.1016/s2468-2667(22)00061-5.

але в одній країні[111]) конфлікту[112], досвіду катування, жорстокого поводження або інших травматичних подій[113]; безпосереднього досвіду бойових дій[114], і, навіть, зв'язку з воєнізованими формуваннями[115], однак усі вони призводять до збільшення сприятливості (віктимності) до кіберзлочинів за рахунок пригнічення когнітивних функцій як спільного симптому. Вірогідність виникнення або загострення вже наявного розладу залежить від готовності особи та її психіки до умов, в яких вона перебуває: якщо рівень адаптації та стрессостійкості відповідає викликам навколишнього середовища або нівелює їх, то ризик розвитку розладу зменшується. Відповідно стратегія превенції кіберзлочинності в умовах збройного конфлікту повинна фокусуватися на профілактиці та роботі з подібними захворюваннями серед населення, а, враховуючи стрімкий ріст та прогнозовану тотальну розповсюдженість, – це має бути одним із напрямків політики держави. В умовах надзвичайних ситуацій люди зазнають різного впливу та потребують різних видів допомоги. Ключовим елементом організації охорони психічного здоров'я та психосоціальної підтримки є створення багаторівневої системи взаємодоповнювальних послуг, що задовольняє потреби різних груп населення. Така система має складатися з 4 рівнів [116][117]:

Рівень 1: Соціальні аспекти базових послуг та безпеки (базові послуги, що надаються шляхом утвердження почуття безпеки, захисту гідності та дотримання прав людини).

В Україні на сьогодні, згідно Звіту за формою F42 МОЗ України, станом на 2023 рік, нараховується всього 5 психоневрологічних диспансерів та

[111] Psychological well-being of Ukrainian students three months after the emerge of full-scale war / I. Pinchuk et al. *Psychiatria Polska*. 2024. Vol. 58, no. 1. P. 121–151. DOI: https://doi.org/10.12740/pp/177073..

[112] Prevalence of depression and posttraumatic stress disorder in adult civilian survivors of war who stay in war-afflicted regions. A systematic review and meta-analysis of epidemiological studies / N. Morina et al. *Journal of Affective Disorders*. 2018. Vol. 239. P. 328–338. DOI: https://doi.org/10.1016/j.jad.2018.07.027.

[113] Association of Torture and Other Potentially Traumatic Events With Mental Health Outcomes Among Populations Exposed to Mass Conflict and Displacement / Z. Steel et al. *JAMA*. 2009. Vol. 302, no. 5. P. 537. DOI: https://doi.org/10.1001/jama.2009.1132.

[114] Depression in Gulf War veterans: a systematic review and meta-analysis / J. D. Blore et al. *Psychological Medicine*. 2015. Vol. 45, no. 8. P. 1565–1580. URL: https://doi.org/10.1017/s0033291714001913.

[115] Freeman J. A. The mental, reproductive, and physical health impacts of female children's association with armed forces and groups. *Child Abuse & Neglect*. 2020. Vol. 107. P. 104626. DOI: https://doi.org/10.1016/j.chiabu.2020.104626.

[116] Zabłocka-Żytka L., Lavdas M. The stress of war. Recommendations for the protection of mental health and wellbeing for both Ukrainian refugees as well as Poles supporting them. *Psychiatria Polska*. 2023. Vol. 57, no. 4. P. 729–746. URL: https://doi.org/10.12740/pp/156157.

[117] Inter-Agency Standing Committee (IASC) (2007). IASC Guidelines on Mental Health and Psychosocial Support in Emergency Settings. Geneva: IASC. 189 p. URL: https://interagencystandingcommittee.org/sites/default/files/migrated/2020-11/IASC%20Guidelines%20on%20Mental%20Health%20and%20Psychosocial%20Support%20in%20Emergency%20Settings%20%28English%29.pdf.

42 психоневрологічні лікарні[118], а на початок 2022 року на 100 тисяч осіб в Україні припадало 9 лікарів, які надають психіатричну допомогу в закладах охорони здоров'я[119], що явно недостатньо для охоплення всього масиву прогнозованих випадків. Відповідно до цього та з урахуванням наслідків післявоєнної демобілізації ветеранів, постає потреба в розширенні системи медичних закладів психоневрологічної підтримки населення. Поруч з цим важливим видається вектор протидії психологічним операціям в межах гібридної війни: в Україні наразі немає системи органів протидії дезінформації. Є низка органів, до відання яких віднесено «протидію дезінформації» або «забезпечення інформаційної безпеки держави» (органи Національної поліції України, Служба безпеки України, органи Ради національної безпеки і оборони України тощо), однак ці обов'язки, по-перше, є занадто широкими (потреба в конкретизації), а по-друге, дублюються, при чому, без регламентації взаємодії або співпраці вказаних органів в цьому напрямку, а тим паче детальної регламентації не отримало питання визначення ролі громадського сектору в цьому напрямку, що в сукупності обґрунтовує сталу потребу в створенні Концепції адміністративно-правової протидії дезінформації в України.

Рівень 2: Зміцнення підтримки на рівні громади та сім'ї (інтервенції, що спираються на соціальні зв'язки; простори, дружні до дитини; традиційні форми підтримки в громаді).

Можливо покращити психічне здоров'я постраждалого населення за допомогою втручань, які формально не вважаються психотерапевтичними за своєю природою[120], до таких можемо віднести стабілізаційні заходи, направлені на покращення загального рівня життя населення. У чинному правовому контексті перелік таких заходів обмежується збільшенням фінансової, гуманітарної та психо-соціальної підтримки категорій осіб з числа тих, хто опинився в складних життєвих обставинах. Чинники, що можуть зумовити складні життєві обставини: похилий вік; часткова або повна втрата рухової активності, пам'яті; невиліковні хвороби, хвороби, що потребують тривалого лікування; психічні та поведінкові розлади, у тому числі внаслідок вживання психоактивних речовин; інвалідність; бездомність; безробіття; малозабезпеченість особи; поведінкові розлади у дітей через розлучення батьків; ухилення батьками або особами, які їх замінюють, від виконання своїх обов'язків із виховання дитини; втрата соціальних зв'язків, у тому числі під час перебування в місцях позбавлення волі; жорстоке поводження з дитиною; насильство за ознакою статі; домашнє насильство; потрапляння в ситуацію торгівлі людьми; шкода, завдана пожежею, стихійним лихом, катастрофою, бойовими діями, терористичним актом, збройним конфліктом, тимчасовою

[118] Форма № 47. Звіт про мережу та діяльність медичних закладів. Міністерство охорони здоров'я України. 2023. URL: http://medstat.gov.ua/im/upload/F47_R0_2023.xls.

[119] 10 цікавих фактів про психологів та психологію – Київська обласна військова адміністрація. *Київська обласна військова адміністрація*. URL: https://koda.gov.ua/10-czikavyh-faktiv-pro-psyhologiv-ta-psyhologiyu/ (дата звернення: 09.02.2026).

[120] Miller K. E., Rasmussen A. The mental health of civilians displaced by armed conflict: an ecological model of refugee distress. *Epidemiology and psychiatric sciences*, № *26*(2). 2017. Pp. 129–138. DOI: https://doi.org/10.1017/S2045796016000172.

окупацією тощо[121]. Також, важливими будуть дії, направлені на забезпечення стабільності кричної інфраструктури та інфраструктури життєзабезпечення.

На квазітерапевтичному рівні можна поєднувати терапевтичні практики з нетерапевтичними шляхом застосування технологій, асоційованих з буденним масовим використанням. Так, привабливим видається використання сучасних технологій у у вигляді телемедицини для дистанційної консультації, мобільних додатків для самомоніторингу та інших інновацій[122]. Головним завданням квазітерапевтичних заходів буде створення сприятливого психічному здоров'ю інформаційного простору. Вплив на масову свідомість буде відбуватися за допомогою трансляції відповідного інформаційного повідомлення, згенерованого у відповідності до базових положень та принципів доказових підходів. Зокрема пропонуємо наступний концепт методології генерації таких повідомлень в межах КПТ та АСТ: за допомогою соціологічних досліджень та методу статистики зібрати дані про найбільш часті тригерні когнітивні упередження серед населення та, із застосуванням метафоричних образів в межах АСТ, генерувати найбільш переконливі раціональні контраргументи та надалі транслювати їх в інформаційному потоці. Сутність образу можна моделювати шляхом аналізу універсальних для культурного середовища українців контенту.

Рівень 3: Сфокусована (індивідуальна) неспеціалізована підтримка (базова допомога у сфері психічного здоров'я, яку надають медичні працівники первинної ланки; базова емоційна та психосоціальна підтримка з боку працівників громади).

Подібна профілактика включає в себе підтримку належного рівня життєстійкості шляхом формування конструктивної стресдолаючої поведінки (адаптації) в людей різних категорій. Така поведінка розглядається як один з проявів життєздатності людини, оскільки подолання труднощів не тільки зберігає життєздатність, але й актуалізує її, апробує і вкорінює[123]. Дане визначення включає певні стилі – проблемноорієнтований копінг, емоційно-орієнтований копінг, уникнення, що виконують певну роль у подоланні людиною важких життєвих ситуацій[124]. Робота повинна вестися шляхом навчання людей базових навичкам життєстійкості, однак, з міркувань точності пропонуємо обрати понятійно-категоріальний апарат в межах конкретного психотерапевтичного підходу. Найбільш перспективним для таких цілей на сьогодні вбачається підхід,

---

[121] Про соціальні послуги : Закон України від 17.01.2019 № 2671-VIII : станом на 7 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2671-19#Text (дата звернення: 09.02.2026).

[122] Regarding the implementation of foreign psychotherapeutic approaches in the mental health protection system of the population of Ukraine in conditions of war / N. O. Nekrasova et al. *Psychiatry Neurology and Medical Psychology*. 2024. No. 23. P. 84–95. DOI: https://doi.org/10.26565/2312-5675-2024-23-10.

[123] Khamis V. Coping with war trauma and psychological distress among school-age Palestinian children. *American Journal of Orthopsychiatry*. 2015. Vol. 85, no. 1. P. 72–79. URL: https://doi.org/10.1037/ort0000039.

[124] Sörensen S., Hirsch J. K., Lyness J. M. Optimism and Planning for Future Care Needs among Older Adults. *GeroPsych*. 2014. Vol. 27, no. 1. P. 5–22. URL: https://doi.org/10.1024/1662-9647/a000099.

запропонований С. Хайесом та іншими[125], що іменується Терапія прийняття та відповідальності. Основними компонентами Терапії прийняття та відповідальності (АСТ) є деконструкція «порядку денного контролю», когнітивне роз'єднання, готовність, Я-як-контекст, цінності та узяття зобов'язань. АСТ належить до традиції когнітивно-поведінкової терапії (КПТ), хоча й має суттєві відмінності від традиційної моделі. Основна мета АСТ полягає у полегшенні людських страждань через допомогу клієнтам у веденні повноцінного (вітального) життя, що ґрунтується на цінностях, в тому числі життя під час війни. Цей вид терапції є трансдіагностичною моделлю втручань, яка може вирішувати ряд психосоціальних та пов'язаних з поведінкою проблем, з якими стикаються ветерани, шляхом націлювання на ключові загальні фактори, зокрема, на уникнення. Завдяки встановленій ефективності в лікуванні депресії, тривоги та болю, АСТ було ефективно впроваджено як серед цивільних осіб, так і ветеранів[126]. З цієї точки зору, потенційним значущим ефектом інтервенцій АСТ буде адаптація до проживання в зоні бойових дій/окупації або просто в країні під час війни шляхом націлювання на розвиток навичок Гексафлексу та подальше прийняття та залучення до значущої (ціннісної) життєвої діяльності. Додатково, Інтервенції, що застосовуються у груповому форматі, такі як Терапія прийняття та відповідальності (АСТ) і Тренінг стійкості (Resilience Strength Training), були визначені як потенційно ефективні для роботи з моральною (психологічною) травмою[127].

Рівень 4: Спеціалізовані послуги (фахова допомога у сфері психічного здоров'я, яку надають спеціалісти: психіатри, клінічні психологи, психотерапевти).

Оскільки країнам із низьким і середнім рівнем доходів не вистачає достатнього фінансування та кваліфікованих фахівців, щоб забезпечити психологічне лікування на основі доказів для такої великої кількості постраждалих людей, необхідні альтернативні та масштабовані стратегії з використанням наявних ресурсів у первинній медичній допомозі та громадах[128]. Вбачаємо в альтернативі стабілізацію чинної системи шляхом точкового подолання найбільш гострих проблем. До таких відносимо застарілість протоколів лікування, застосування препаратів з недоведеною

[125] Hayes S.C., Pierson H. Acceptance and Commitment Therapy. In: Freeman, A., Felgoise, S.H., Nezu, C.M., Nezu, A.M., Reinecke, M.A. (eds) Encyclopedia of Cognitive Behavior Therapy. Springer, Boston, MA. 2005. DOI: https://doi.org/10.1007/0-306-48581-8_1/

[126] Development and evaluation of an 1-day Acceptance and Commitment Therapy workshop for Veterans with comorbid chronic pain, TBI, and psychological distress: Outcomes from a pilot study / L. Dindo et al. *Contemporary Clinical Trials*. 2020. Vol. 90. DOI: https://doi.org/10.1016/j.cct.2020.105954.

[127] Denov M. Encountering children and child soldiers during military deployments: the impact and implications for moral injury. *European Journal of Psychotraumatology*. 2022. Vol. 13, no. 2. DOI: https://doi.org/10.1080/20008066.2022.2104007.

[128] Global burden of post-traumatic stress disorder and major depression in countries affected by war between 1989 and 2019: a systematic review and meta-analysis / T. H. Hoppen et al. *BMJ Global Health*. 2021. Vol. 6, no. 7. DOI: https://doi.org/10.1136/bmjgh-2021-006303.

ефективністю, діагностика «неіснуючих» хвороб тощо. Вбачається необхідним врегулювати питання призначення дієтичних добавок, гомеопатії та інших видів препаратів з недоведеною ефективністю пацієнтам з гострими станами шляхом (1) обмеження або повної заборони обігу таких препаратів на території України способом прямої імплементації стандартів FDA, WHO, NICE та інших авторитетних інституцій у сферу правового регулювання стандартів випуску та обігу лікарських засобів в Україні; (2) введення кримінальної відповідальності за призначення лікарем «завідомо недієвого препарату або способу лікування» замість цивільно-правової. Подолання практики недієвих методів та способів лікування додатково потребує оновлення стандартів та протоколів лікування у відповідності до найсучасніших наукових напрацювань та досліджень шляхом прив'язки їх на законодавчому рівні до стандартів та протоколів міжнародних спеціалізованих організацій наряду зі згаданими FDA, WHO та іншими. Визнання приписів або рецептів з завідомо недієвими препаратами та/або неіснуючих діагнозів нікчемними, а подальші юридично значущі дії з ними, на кшталт отримання лікарняного, – незаконними. На додаток, окремої уваги потребує питання зменшення стигматизації психічних захворювань шляхом збільшення обізнаності населення в цій сфері. Окрім проведення просвітницької кампанії з розвінчення стигм, стереотипів та міфів навколо психічного здоров'я та методів його корекції, цей крок передбачає обмеження підсилюючих недовіру населення до доказової медицини проявів її антиподу у вигляді нетрадиційної медицини: наразі в Україні чинні Порядок видачі та анулювання спеціального дозволу на зайняття народною медициною (цілительством)[129] та Порядок видачі атестаційно-експертного висновку, що підтверджує наявність в особи цілительських здібностей[130], також Національний класифікатор України «Класифікатор професій» включає в себе ворожок, хіромантів та цілителів[131], до яких за статистикою щороку звертається понад п'ять мільйонів людей[132]. Враховуючи тотальну неефективність засобів нетрадиційної медицини при будь-яких станах, наряду з прогресуючими без належного та вчасного лікування хворобами, які у разі відсутності адекватної лінії лікування потенційно можуть призвести до смерті особи, наявність

[129] Про затвердження Порядку видачі та анулювання спеціального дозволу на зайняття народною медициною (цілительством) : Постанова Каб. Міністрів України від 03.12.2012 № 1145 : станом на 10 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1145-2012-п#Text.

[130] Про порядок видачі атестаційно-експертного висновку, що підтверджує наявність в особи цілительських здібностей : Наказ МОЗ України від 23.09.2013 № 822 : станом на 8 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/z1943-13#Text.

[131] Національний класифікатор України "Класифікатор професій". *Міністерство економіки, довкілля та сільського господарства України*. URL: https://www.me.gov.ua/Profession/List?lang=uk-UA&id=d4162ef8-2771-4ac5-99ef-1d4b6f5336af&tag=KlasifikatorProfesii-Poshuk (дата звернення: 09.02.2026).

[132] Радиш Я. Ф., Євтушенко В.В. Українська народна медицина як національний феномен: генеза та перспективи розвитку (до проблеми державного управління у сфері народної медицини і цілительства). *Інвестиції: практика та досвід*. 2015. № 12. С. 63–71. URL: http://www.investplan.com.ua/pdf/12_2015/16.pdf.

легального статусу подібних «сфер медицини» є фактом геноциду, що потребує належного рівня реагування у вигляді повної заборони та криміналізації.

ВИСНОВКИ

Аналіз поліцейської та судової статистики вказує на високу кореляцію між початком повномасштабного вторгнення Росії в Україну та аномальним зростанням інтенсивності кіберзлочинності в цьому регіоні. Критичний аналіз методології поліцейської статистики дозволив виокремити три можливі причини таких зрушень: зміни об'єкта дослідження, зміни методології збору даних або поєднання обох варіантів у різних пропорціях. За результатами вивчення всіх трьох варіантів встановлено, що це аномальне зростання безпосередньо пов'язане зі змінами об'єкта дослідження, що стосуються суб'єктного складу кіберзлочинності.

Враховуючи, що національне законодавство України диференціює та розмежовує поняття «кіберзлочин» і «кіберінцидент» (де останній є актом агресії в ході гібридної війни), таке аномальне зростання є не прямим проявом війни, а радше її наслідком. З огляду на унікальні характеристики кіберзлочинів порівняно з «класичними злочинами», а також відсутність даних про зміни в тактиці вчинення кіберзлочинів, коло порушених суб'єктів звужується до потенційних жертв, тоді як вплив війни набуває віктимізуючого характеру.

Використовуючи теоретичну базу епігенетики, запропоновано пояснювальну модель, згідно з якою стан війни асоціюється з умовами надзвичайно високого хронічного неконтрольованого стресу, що індукує експресію/метилювання наборів генів, пов'язаних із певними психічними розладами та/або дефіцитарними станами, спільним симптомом яких є деградація когнітивних здібностей людини. Це проявляється у зниженні навичок критичного мислення, що є прямим предиктором підвищеної ймовірності стати жертвою кіберзлочину. Відповідно до цієї моделі запропоновано специфічну чотирирівневу стратегію протидії кіберзлочинності, спрямовану на її профілактику шляхом покращення загального психічного благополуччя населення через усунення концептуальних прогалин у сфері підтримки психічного здоров'я в Україні.

АНОТАЦІЯ

Дослідження присвячене здійсненню комплексного міждисциплінарного аналізу кореляційного взаємозв'язку між станом війни та динамікою інтенсивності кіберзлочинності в межах однієї країни, що базується на емпіричному досвіді України періоду 2014–2024 років. Автори застосовують методологічний апарат, що поєднує юридичну герменевтику, компаративістський підхід та методи статистики, зокрема регресійний і факторний аналізи поліцейської та судової статистики . У роботі виявлено та обґрунтовано аномальне зростання показників кіберзлочинності, яке розпочалося наприкінці 2021 року та набуло пікових значень після повномасштабного вторгнення російської федерації. Шляхом розмежування понять «кіберзлочин» та «кіберінцидент» у національному законодавстві доведено, що цей сплеск є

не прямим проявом кібервійни, а наслідком глибоких змін у структурі віктимізації населення.

Центральним елементом наукової новизни є розробка унікальної пояснювальної моделі онто- та патогенезу кіберзлочинності крізь призму епігенетичної теорії. Дослідження аргументує, що умови екстремального хронічного неконтрольованого стресу, спричиненого війною, індукують експресію або метиляцію генів, асоційованих із психодефіцитними станами та ментальними розладами. Спільним симптомом таких змін визначено дегенерацію когнітивних здібностей і зниження критичного мислення, що виступає безпосереднім предиктором підвищеної вразливості особи до маніпулятивного впливу кіберзлочинців.

На основі отриманих результатів авторами запропоновано багаторівневу стратегію превенції кіберзлочинності. Ця стратегія передбачає імплементацію комплексу заходів: від створення безпечного інформаційного простору та квазітерапевтичної протидії дезінформації до навчання населення навичкам життєстійкості з використанням інструментарію Терапії прийняття та відповідальності (ACT). Особливу увагу приділено реформуванню системи спеціалізованої допомоги, що включає необхідність криміналізації призначення лікарями препаратів з недоведеною ефективністю та повну заборону нетрадиційної медицини (цілительства, гомеопатії) як факторів, що перешкоджають своєчасному лікуванню психотравм та посилюють віктимність щодо кіберправопорушень суспільства в умовах воєнного часу.

Література

1. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 09.02.2026).
2. Galushkin A. A. Education in the Field of National Information Security in the Russian Federation and Abroad. *Journal of Computer Science*. 2015. Т. 11, № 10. С. 988–994. URL: https://doi.org/10.3844/jcssp.2015.988.994.
3. Filshtinskiy S. Cybercrime, cyberweapons, cyber wars: is there too much of it in the air*? Communications of the ACM*. Vol. 56, № 6. 2023. Pp. 28–30. DOI: https://doi.org/10.1145/2461256.2461266.
4. Maher D. Can artificial intelligence help in the war on cybercrime?. *Computer Fraud & Security*. 2017. Vol. 2017, no. 8. P. 7–9. URL: https://doi.org/10.1016/s1361-3723(17)30069-6.
5. Brandenburg N. Phenomenology of Law. In: Sellers, M., Kirste, S. (eds). *Encyclopedia of the Philosophy of Law and Social Philosophy*. Springer, Dordrecht. 2023. DOI: https://doi.org/10.1007/978-94-007-6730-0_74-2.
6. Greening N. Phenomenological Research Methodology. *Scientific Research Journal*. 2019. Vol. VII, no. V. URL: https://doi.org/10.31364/scirj/v7.i5.2019.p0519656.
7. Naik V., Metallinou A., Goel R. Context Aware Conversational Understanding for Intelligent Agents With a Screen. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2018. Vol. 32, no. 1. URL: https://doi.org/10.1609/aaai.v32i1.11952.

8. Gupta A., Mackereth S. "Definitions". *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.). URL: https://plato.stanford.edu/archives/fall2023/entries/definitions.

9. Fincham D. How Law Defines Art (November 7, 2014). *John Marshall Review of Intellectual Property Law*, 2015, Available at SSRN: https://ssrn.com/abstract=2520594.

10. Glogar O. The Concept of Legal Language: What Makes Legal Language 'Legal'?. *J Semiot Law*, № 3**6**. Pp. 1081–1107. 2023. DOI: https://doi.org/10.1007/s11196-023-10010-5.

11. Barbir L., Goldstein A. The History of Functional Contextualism. 2016. DOI: 10.13140/RG.2.2.23324.08329.

12. Рабінович П. М., Дудаш Т. І. Аргументи у правовій аргументації: деякі загальнотеоретичні аспекти. Вісник Національної академії правових наук України. 2022. Т. 29. №3. С. 47–68. DOI: 10.31359/1993-0909-2022-29-3-47.

13. Chevalier J.-M. Some Arguments for Propositional Logic: Maccoll as a Philosopher. *Philosophia Scientiæ*, № 15-1(1). 2011. Pp. 129-147. DOI: https://doi.org/10.4000/philosophiascientiae.368.

14. Wang S. Varieties of authoritarian legality. *Asia Pacific Law Review*. 2024. P. 1–18. DOI: https://doi.org/10.1080/10192557.2024.2323803.

15. Toward a multidimensional model of legitimacy: Validation of the Traffic Rules Perceived Legitimacy scale. / F. Varet et al. *Psychology, Public Policy, and Law*. 2024. DOI: https://doi.org/10.1037/law0000416.

16. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

17. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода Україна від 27.06.2014 : станом на 14 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.

18. Про міжнародні договори України : Закон України від 29.06.2004 № 1906-IV : станом на 15 берез. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1906-15#Text.

19. Ciongaru E. The monistic and the dualistic theory in European law. *Acta Universitatis George Bacovia*. Juridica, 1, № 1. 2012. Pp. 212-231. URL: http://www.ugb.ro/Juridica/Issue1EN/10_Teoria_monista_si_dualista_in_dreptul_europeanCiongaruEN.pdf.

20. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

21. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (укр/рос) : Протокол Ради Європи від 28.01.2003 : станом на 21 лип. 2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.

22. Науково-практичний коментар до статті 190 Кримінального кодексу України: науково-практичний коментар від 01.01.2009 року. LIGA 360. URL: https://ips.ligazakon.net/document/KK004696 (дата звернення: 01.01.2026).

23. Статистика кримінальної протиправності. Офіс Генерального прокурора України. URL: https://erdr-map.gp.gov.ua/csp/map/index.html#/map (дата звернення: 12.09.2025).

24. Fox C., Mackay S., Hope T. The Independent Review of Crime Statistics. *Safer Communities*. 2006. Vol. 5, no. 4. P. 4–12. DOI: https://doi.org/10.1108/17578043200600028.

25. Warr M., Kirk D. S. Data Bases and Statistical Systems: Crime and Delinquency. *International Encyclopedia of the Social & Behavioral Sciences*. 2015. P. 717–719. DOI: https://doi.org/10.1016/b978-0-08-097086-8.41068-8.

26. Makkai T. Statistical Systems: Crime. *International Encyclopedia of the Social & Behavioral Sciences*. 2001. P. 15053–15056. DOI: https://doi.org/10.1016/b0-08-043076-7/00011-5.

27. Maguire M. Criminal Statistics and The Construction of Crime. *The Oxford Handbook of Criminology*. 2012. P. 206–244. DOI: https://doi.org/10.1093/he/9780199590278.003.0008.

28. Про затвердження Переліку територіальних громад, що розташовані в районі проведення воєнних (бойових) дій або які перебувають в тимчасовій окупації, оточенні (блокуванні) станом на 25 квітня 2022 року : Наказ М-ва з питань реінтеграції тимчасово окуп. територій України від 25.04.2022 № 75 : станом на 27 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/z0453-22#Text (дата звернення: 09.02.2026).

29. Про затвердження Переліку територій, на яких ведуться (велися) бойові дії або тимчасово окупованих Російською Федерацією : Наказ М-ва з питань реінтеграції тимчасово окуп. територій України від 22.12.2022 № 309 : станом на 20 берез. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/z1668-22#Text (дата звернення: 09.02.2026).

30. Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України : Закон України від 15.04.2014 № 1207-VII : станом на 19 трав. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1207-18#Text (дата звернення: 09.02.2026).

31. Перелік судів, територіальну підсудність яких було змінено у зв'язку з неможливістю здійснювати правосуддя під час воєнного стану. *Верховний Суд.* URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/rozporyadjennya/Zagalna_tablica_sudiv_30_10_2023.pdf (дата звернення: 10.05.2024).

32. В Офісі Генпрокурора обговорили налагодження роботи правоохоронних органів та судових інстанцій, переміщених з тимчасово окупованих територій держави. *Офіс Генерального прокурора.* 2023. URL: https://www.gp.gov.ua/ua/posts/v-ofisi-genprokurora-obgovorili-robotu-pravooxoronnix-organiv-ta-sudovix-instancii-peremishhenix-z-timcasovo-okupovanix-teritorii-derzavi.

33. Ukrinform. За кордоном перебувають майже 9 мільйонів українців – демограф. *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-society/3790729-za-kordonom-perebuvaut-majze-9-miljoniv-ukrainciv-demograf.html.

34. Чисельність та склад населення. Держстат. URL: https://stat.gov.ua/uk/datasets/chyselnist-ta-sklad-naselennya.

35. МВФ оцінив кількість населення України та дав прогноз на найближчі роки. *РБК-Украина*. URL: https://www.rbc.ua/rus/news/mvf-otsiniv-kilkist-naselennya-ukrayini-ta-1713333704.html (дата звернення: 09.02.2026).

36. WORLD ECONOMIC OUTLOOK 2024: APR Steady but Slow: Resilience amid Divergence. 2024. 202 p. URL: https://www.imf.org/-/media/files/publications/weo/2024/april/english/text.pdf.

37. Єдиний реєстр судових рішень. URL: https://reyestr.court.gov.ua/ (дата звернення: 01.01.2025).

38. Економічна правда. Легкі гроші: Україна перетворюється на Мекку для кіберзлочинців. *Економічна правда*. URL: https://epravda.com.ua/publications/2016/03/28/587004/ (дата звернення: 09.02.2026).

39. Річний звіт Національної поліції України за 2016 рік. Національна поліція України. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvit_2016.pdf.

40. Економічна правда. Голова Кіберполіції: "Ваш син у поліції" приносить шахраям на "зоні" мільйон гривень на добу. *Економічна правда*. URL: https://www.epravda.com.ua/publications/2018/01/15/633003/ (дата звернення: 09.02.2026).

41. Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік. 19 с. URL: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf.

42. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. 12 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf.

43. Звіт Національної поліції України про результати роботи у 2020 році. 14 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf.

44. Звіт Національної поліції України про результати роботи у 2021 році. 18 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/Zvit_NPU_2021_.pdf.

45. Звіт Національної поліції України про результати роботи у 2022 році. 14 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf.

46. Звіт Національної поліції України про результати роботи у 2023 році. 12 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2023/zvit_NPU_2023.pdf.

47. Звіт Національної поліції України про результати роботи у 2023 році. С. 9-11. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2023/zvit_NPU_2023.pdf.

48. Про затвердження Інструкції з оцінювання на відповідність міжнародним стандартам оверсайту суб'єктів, які виконують функції центрального депозитарію цінних паперів, центрального контрагента, торгового репозиторію та системи розрахунків у цінних паперах в Україні : Постанова Нац. банку України від 05.04.2024 № 38. URL: https://zakon.rada.gov.ua/laws/show/v0038500-24#Text (дата звернення: 09.02.2026).

49. Reference Incident Classification Taxonomy Task Force Status and Way Forward. 2018. URL: https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-1%20Good%20practice%20guide%20on%20how%20to%20improve%20CSIRT%20capabilities.pdf.

50. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022 рік. 10 с. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf.

51. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023 рік. 12 с. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a.

52. The Latest Cyber Crime Statistics (updated October 2025) | AAG IT Support. *AAG IT Services*. URL: https://aag-it.com/the-latest-cyber-crime-statistics/.

53. How cybersecurity boosts enterprise reinvention to drive business resilience: State of Cybersecurity Resilience 2023. 39 p. URL: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf.

54. Інформаційне повідомлення. Комітет з питань цифрової трансформації інформує про кібератаки, роботу мобільних операторів та інформаційну безпеку. *Офіційний портал Верховної Ради України*. URL: https://www.rada.gov.ua/print/221400.html (дата звернення: 09.02.2026).

55. Михайлов Д. Путін прийняв рішення про початок повномасштабної війни проти України на початку 2021 року – ЗМІ. *Суспільне новини*. 2023. URL: https://suspilne.media/456759-putin-prijnav-risenna-pro-pocatok-povnomasstabnoi-vijni-proti-ukraini-na-pocatku-2021-roku-zmi/.

56. Google Trends. *Google corp*. URL: https://trends.google.com.ua/trends/.

57. Simons G., Danyk Y., Maliarchuk T. Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace & Security*. 2020. Vol. 32, no. 3. P. 337–342. DOI: https://doi.org/10.1080/14781158.2020.1732899.

58. Pearl J. Causal inference in statistics: An overview. *Statistics Surveys*. 2009. Vol. 3. P. 96–146. URL: https://doi.org/10.1214/09-ss057.

59. Schneider J., Schneider P. The Anthropology of Crime and Criminalization. *Annual Review of Anthropology*. 2008. Vol. 37, no. 1. P. 351–373. DOI: https://doi.org/10.1146/annurev.anthro.36.081406.094316.

60. Ling S., Umbach R., Raine A. Biological explanations of criminal behavior. *Psychology, Crime & Law*. 2019. Vol. 25, no. 6. P. 626–640. DOI: https://doi.org/10.1080/1068316x.2019.1572753.

61. Sathyanarayana Rao T. Psychiatrist and the science of criminology: Sociological, psychological and psychiatric analysis of the dark side. *Indian Journal of Psychiatry*. 2007. Vol. 49, no. 1. P. 3. DOI: https://doi.org/10.4103/0019-5545.31511.

62. Bartol C., Bartol A. *Criminal behavior: A psychological approach* (12th edition.). 2021. Boston: Pearson.

63. Shahid A. Sociological theories of crime. 2022. DOI: 10.13140/RG.2.2.17683.66081.

64. Waite J. The Legal Approach to Crime and Correction, 23 *Law and Contemporary Problems* 594-610 (Fall 1958). URl: https://scholarship.law.duke.edu/lcp/vol23/iss4/3.

65. Becker G. Crime and Punishment: An Economic Approach. *The Journal of Political Economy*. № 176. P. 176–177. 1968. URL: https://masonlec.org/site/rte_uploads/files/JEP/Readings/Butler%20Economic%20Analysis%20for%20Lawyers%203rd%20ed/CH%20VII%20Crime.pdf

66. Skrzypiec G. Adolescents' Intentions to Engage in Criminal Activity: A Cross-Disciplinary Approach Linking Theories From Social Psychology and Criminology. *Journal of Forensic Psychology Research and Practice*. 2017. Vol. 17, no. 5. P. 305–337. DOI: https://doi.org/10.1080/24732850.2017.1374720.

67. Walsh A, Criminology: An Interdisciplinary Approach. *Faculty & Staff Authored Books*. 2007. URL: https://scholarworks.boisestate.edu/fac_books/93.

68. Taylor S. Crime and Criminality. Routledge, 2015. DOI: https://doi.org/10.4324/9781315713298.

69. Yanishevska K., Kosiachenko K., Kamyshanskyi O., Neviadovskyi V., Telizhenko L. Transdisciplinary theory of the nature of crime as an expression of a symbiotic complex approach. *Revista Amazonia Investiga*, № *12*(66). 2023. Pp. 188–197. DOI: https://doi.org/10.34069/AI/2023.66.06.18.

70. Farrington D. P. Introduction to Integrated Developmental and Life-Course Theories of Offending. *Integrated developmental and life-course theories of offending*. 2017. P. 1–15. URL: https://doi.org/10.4324/9780203788431-1.

71. Schindler S. Theoretical virtues: do scientists think what philosophers think they ought to think?. *Philosophy of Science*. 2022. P. 1–31. DOI: https://doi.org/10.1017/psa.2021.40.

72. Schindler S. Theoretical Virtues in Science. 2020. DOI: 10.1093/obo/9780195396577-0409.

73. Gottfredson M. R., Hirschi T. *A general theory of crime*. Stanford University Press. 1990. URL: https://psycnet.apa.org/record/1990-97753-000.

74. Cullen F. T., Wilcox P. Encyclopedia of Criminological Theory. SAGE Publications, Incorporated, 2010. DOI: http://dx.doi.org/10.4135/9781412959193.n208.

75. Moffitt T. E. Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review*, *№ 100*(4). 1993. Pp. 674–701. DOI: https://doi.org/10.1037/0033-295X.100.4.674.

76. Social Learning and Deviant Behavior: A Specific Test of a General Theory / R. L. Akers et al. *American Sociological Review*. 1979. Vol. 44, no. 4. P. 636. DOI: https://doi.org/10.2307/2094592.

77. Scott M. The Reasoning Criminal / ed. by D. B. Cornish, R. V. Clarke. Routledge, 2017. DOI: https://doi.org/10.4324/9781315134482.

78. Glasser W. *Choice theory: A new psychology of personal freedom.* HarperPerennial. 1999. URL: https://psycnet.apa.org/record/1999-02074-000.

79. Early and Classical Criminological Theories. *SAGE Publications*. 2020. 26 p. URL: https://www.sagepub.com/sites/default/files/upm-assets/97953_book_item_97953.pdf.

80. Schneewind K. A. Socialization and Education: Theoretical Perspectives. *International Encyclopedia of the Social & Behavioral Sciences*. 2015. P. 861–865. URL: https://doi.org/10.1016/b978-0-08-097086-8.92071-3.

81. Mann R. D. A review of the relationships between personality and performance in small groups. *Psychological Bulletin, № 56*(4). Pp. 241–270. 1959. DOI: https://doi.org/10.1037/h0044587.

82. Agnew R. S. Strain theory and violent behavior. In D. J. Flannery, A. T. Vazsonyi, & I. D. Waldman (Eds.), *The Cambridge handbook of violent behavior and aggression*. Pp. 519–529. 2007. Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511816840.027.

83. Wong C. Clifford R. Shaw and Henry D. McKay, The Social Disorganization Theory. *CSISS Classics*. *UC Santa Barbara: Center for Spatially Integrated Social Science*. 2002. URL: https://escholarship.org/uc/item/47j411pr.

84. Positivist Criminology | Overview & Theory. URL: https://study.com/academy/lesson/positivist-criminology-definition-theory.html#:~:text=The%20positivist%20theory%20in%20criminology%20states%20that%20individuals%20commit%20crimes,positivism%20is%20based%20on%20pseudoscience.

85. Theories and causes of crime. University of Glasgow. 9 p. URL: https://www.sccjr.ac.uk/wp-content/uploads/2016/02/SCCJR-Causes-of-Crime.pdf.

86. Kavish N., Boutwell B. The unified crime theory and the social correlates of crime and violence: problems and solutions. *Journal of Criminal Psychology*. 2018. Vol. 8, no. 4. P. 287–301. URL: https://doi.org/10.1108/jcp-06-2018-0028.

87. Ilan J. Dorine W. Biological theories of crime versus psychological theories of crime – Comparison and evaluation of their contributions to our understanding of crime and/or criminal justice. 2017. 23 p. DOI: 10.13140/RG.2.2.14740.14726.

88. From 1957 to Nowadays: A Brief History of Epigenetics / P. Peixoto et al. *International Journal of Molecular Sciences*. 2020. Vol. 21, no. 20. DOI: https://doi.org/10.3390/ijms21207571.

89. Tremblay R. E. Developmental origins of disruptive behaviour problems: the 'original sin' hypothesis, epigenetics and their consequences for prevention. *Journal of Child Psychology and Psychiatry*. 2010. Vol. 51, no. 4. P. 341–367. DOI: https://doi.org/10.1111/j.1469-7610.2010.02211.x.

90. Hong S. Environmental and Geographic Determinism: Jared Diamond and His Ideas. In: Wiarda, H.J. (eds) Grand Theories and Ideologies in the Social Sciences. Palgrave Macmillan, New York. 2010. DOI: https://doi.org/10.1057/9780230112612_9

91. Tremblay R. E., Vitaro F., Côté S. M. Developmental Origins of Chronic Physical Aggression: A Bio-Psycho-Social Model for the Next Generation of Preventive Interventions. *Annual review of psychology*, *№ 69*. Pp. 383–407. 2018. DOI: https://doi.org/10.1146/annurev-psych-010416-044030.

92. Gene expression analysis of MAOA and the clock gene ARNTL in individuals with bipolar disorder compared to healthy controls / S. Bengesser et al. *The World Journal of Biological Psychiatry*. 2021. P. 1–19. DOI: https://doi.org/10.1080/15622975.2021.1973816.

93. Anxiety, aggression, reward sensitivity, and forebrain dopamine receptor expression in a laboratory rat model of early-life disadvantage / J. S. Lonstein et

al. *Developmental Psychobiology*. 2023. Vol. 65, no. 7. DOI: https://doi.org/10.1002/dev.22421.

94. Genes and Aggressive Behavior: Epigenetic Mechanisms Underlying Individual Susceptibility to Aversive Environments / S. Palumbo et al. *Frontiers in Behavioral Neuroscience*. 2018. Vol. 12. DOI: https://doi.org/10.3389/fnbeh.2018.00117.

95. Genetic and Environmental Influences on the Developmental Course of Attention-Deficit/Hyperactivity Disorder Symptoms From Childhood to Adolescence / J.-B. Pingault et al. *JAMA Psychiatry*. 2015. Vol. 72, no. 7. P. 651. DOI: https://doi.org/10.1001/jamapsychiatry.2015.0469.

96. Iofrida C., Palumbo S., Pellegrini S. Molecular genetics and antisocial behavior: Where do we stand?. *Experimental Biology and Medicine*. 2014. Vol. 239, no. 11. P. 1514–1523. DOI: https://doi.org/10.1177/1535370214529508.

97. Genes and Aggressive Behavior: Epigenetic Mechanisms Underlying Individual Susceptibility to Aversive Environments / S. Palumbo et al. *Frontiers in Behavioral Neuroscience*. 2018. Vol. 12. DOI: https://doi.org/10.3389/fnbeh.2018.00117.

98. Dee G., Ryznar R., Dee C. Epigenetic Changes Associated with Different Types of Stressors and Suicide. *Cells*, № *12*(9). 2023. DOI: https://doi.org/10.3390/cells12091258.

99. Leshem R., Weisburd D. Epigenetics and Hot Spots of Crime: Rethinking the Relationship Between Genetics and Criminal Behavior. *Journal of Contemporary Criminal Justice*. 2019. Vol. 35, no. 2. P. 186–204. DOI: https://doi.org/10.1177/1043986219828924.

100. Agnew R. A Theory Of Crime Resistance And Susceptibility. *Criminology*. 2016. Vol. 54, no. 2. P. 181–211. DOI: https://doi.org/10.1111/1745-9125.12104.

101. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 1 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 09.02.2026).

102. Carpiniello B. The Mental Health Costs of Armed Conflicts–A Review of Systematic Reviews Conducted on Refugees, Asylum-Seekers and People Living in War Zones. *International Journal of Environmental Research and Public Health*. 2023. Vol. 20, no. 4. P. 2840. DOI: https://doi.org/10.3390/ijerph20042840.

103. Hassan G, Ventevogel P, Jefee-Bahloul H, Barkil-Oteo A, Kirmayer LJ. Mental health and psychosocial wellbeing of Syrians affected by armed conflict. *Epidemiology and Psychiatric Sciences*. 2016, № 25(2). Pp. 129-141. DOI: 10.1017/S2045796016000044.

104. Childhood traumas: an outline and overview. *American Journal of Psychiatry*. 1991. Vol. 148, no. 1. P. 10–20. DOI: https://doi.org/10.1176/ajp.148.1.10.

105. Вплив війни на психічне здоров'я – колосальний, – Віктор Ляшко. *Міністерство охорони здоров'я України*. 2022. URL: https://www.kmu.gov.ua/news/vpliv-vijni-na-psihichne-zdorovya-kolosalnij-viktor-lyashko (дата звернення: 09.02.2026).

106. Психічне здоров'я в умовах війни: як громадські організації підтримувані ПРООН надають психологічну допомогу українцям. United Nations Development Programme. URL: https://www.undp.org/uk/ukraine/news/

psykhichne-zdorovya-v-umovakh-viyny-yak-hromadski-orhanizatsiyi-pidtrymuvani-proon-nadayut-psykholohichnu-dopomohu-ukrayintsyam.

107. Зеленська про програму ментального здоров'я: Виявилося, що «сильні не ходять до психологів». *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-society/3703135-zelenska-pro-programu-mentalnogo-zdorova-viavilosa-so-silni-ne-hodat-do-psihologiv.html (дата звернення: 09.02.2026).

108. У межах Всеукраїнської програми ментального здоров'я визначили пріоритетні проєкти. *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-society/3695613-u-mezah-vseukrainskoi-programi-mentalnogo-zdorova-viznacili-prioritetni-proekti.html (дата звернення: 09.02.2026).

109. Маємо переплавити жахливий досвід на посттравматичне зростання – перша леді на Міжвідомчій координаційній раді з питань охорони психічного здоров'я – Офіційне інтернет-представництво Президента України. *Офіційне інтернет-представництво Президента України*. URL: https://www.president.gov.ua/news/mayemo-pereplaviti-zhahlivij-dosvid-na-posttravmatichne-zros-80849 (дата звернення: 09.02.2026).

110. Mental health of migrants with pre-migration exposure to armed conflict: a systematic review and meta-analysis / C. Mesa-Vieira et al. *The Lancet Public Health*. 2022. Vol. 7, no. 5. P. e469-e481. DOI: https://doi.org/10.1016/s2468-2667(22)00061-5.

111. Psychological well-being of Ukrainian students three months after the emerge of full-scale war / I. Pinchuk et al. *Psychiatria Polska*. 2024. Vol. 58, no. 1. P. 121–151. DOI: https://doi.org/10.12740/pp/177073.

112. Prevalence of depression and posttraumatic stress disorder in adult civilian survivors of war who stay in war-afflicted regions. A systematic review and meta-analysis of epidemiological studies / N. Morina et al. *Journal of Affective Disorders*. 2018. Vol. 239. P. 328–338. DOI: https://doi.org/10.1016/j.jad.2018.07.027.

113. Association of Torture and Other Potentially Traumatic Events With Mental Health Outcomes Among Populations Exposed to Mass Conflict and Displacement / Z. Steel et al. *JAMA*. 2009. Vol. 302, no. 5. P. 537. DOI: https://doi.org/10.1001/jama.2009.1132.

114. Depression in Gulf War veterans: a systematic review and meta-analysis / J. D. Blore et al. *Psychological Medicine*. 2015. Vol. 45, no. 8. P. 1565–1580. URL: https://doi.org/10.1017/s0033291714001913.

115. Freeman J. A. The mental, reproductive, and physical health impacts of female children's association with armed forces and groups. *Child Abuse & Neglect*. 2020. Vol. 107. P. 104626. DOI: https://doi.org/10.1016/j.chiabu.2020.104626.

116. Zabłocka-Żytka L., Lavdas M. The stress of war. Recommendations for the protection of mental health and wellbeing for both Ukrainian refugees as well as Poles supporting them. *Psychiatria Polska*. 2023. Vol. 57, no. 4. P. 729–746. URL: https://doi.org/10.12740/pp/156157.

117. Inter-Agency Standing Committee (IASC) (2007). IASC Guidelines on Mental Health and Psychosocial Support in Emergency Settings. Geneva: IASC. 189 p. URL: https://interagencystandingcommittee.org/sites/default/files/migrated/2020-11/

IASC%20Guidelines%20on%20Mental%20Health%20and%20Psychosocial%20Support%20in%20Emergency%20Settings%20%28English%29.pdf.

118. Форма № 47. Звіт про мережу та діяльність медичних закладів. Міністерство охорони здоров'я України. 2023. URL: http://medstat.gov.ua/im/upload/F47_R0_2023.xls.

119. 10 цікавих фактів про психологів та психологію – Київська обласна військова адміністрація. *Київська обласна військова адміністрація*. URL: https://koda.gov.ua/10-czikavyh-faktiv-pro-psyhologiv-ta-psyhologiyu/ (дата звернення: 09.02.2026).

120. Miller K. E., Rasmussen A. The mental health of civilians displaced by armed conflict: an ecological model of refugee distress. *Epidemiology and psychiatric sciences*, № *26*(2). 2017. Pp. 129–138. DOI: https://doi.org/10.1017/S2045796016000172.

121. Про соціальні послуги : Закон України від 17.01.2019 № 2671-VIII : станом на 7 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2671-19#Text (дата звернення: 09.02.2026).

122. Regarding the implementation of foreign psychotherapeutic approaches in the mental health protection system of the population of Ukraine in conditions of war / N. O. Nekrasova et al. *Psychiatry Neurology and Medical Psychology*. 2024. No. 23. P. 84–95. DOI: https://doi.org/10.26565/2312-5675-2024-23-10.

123. Khamis V. Coping with war trauma and psychological distress among school-age Palestinian children. *American Journal of Orthopsychiatry*. 2015. Vol. 85, no. 1. P. 72–79. URL: https://doi.org/10.1037/ort0000039.

124. Sörensen S., Hirsch J. K., Lyness J. M. Optimism and Planning for Future Care Needs among Older Adults. *GeroPsych*. 2014. Vol. 27, no. 1. P. 5–22. URL: https://doi.org/10.1024/1662-9647/a000099.

125. Hayes S.C., Pierson H. Acceptance and Commitment Therapy. In: Freeman, A., Felgoise, S.H., Nezu, C.M., Nezu, A.M., Reinecke, M.A. (eds) Encyclopedia of Cognitive Behavior Therapy. Springer, Boston, MA. 2005. DOI: https://doi.org/10.1007/0-306-48581-8_1/

126. Development and evaluation of an 1-day Acceptance and Commitment Therapy workshop for Veterans with comorbid chronic pain, TBI, and psychological distress: Outcomes from a pilot study / L. Dindo et al. *Contemporary Clinical Trials*. 2020. Vol. 90. DOI: https://doi.org/10.1016/j.cct.2020.105954.

127. Denov M. Encountering children and child soldiers during military deployments: the impact and implications for moral injury. *European Journal of Psychotraumatology*. 2022. Vol. 13, no. 2. DOI: https://doi.org/10.1080/20008066.2022.2104007.

128. Global burden of post-traumatic stress disorder and major depression in countries affected by war between 1989 and 2019: a systematic review and meta-analysis / T. H. Hoppen et al. *BMJ Global Health*. 2021. Vol. 6, no. 7. DOI: https://doi.org/10.1136/bmjgh-2021-006303.

129. Про затвердження Порядку видачі та анулювання спеціального дозволу на зайняття народною медициною (цілительством) : Постанова Каб. Міністрів України від 03.12.2012 № 1145 : станом на 10 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1145-2012-п#Text.

130. Про порядок видачі атестаційно-експертного висновку, що підтверджує наявність в особи цілительських здібностей : Наказ МОЗ України від 23.09.2013 № 822 : станом на 8 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/z1943-13#Text.

131. Національний класифікатор України "Класифікатор професій". *Міністерство економіки, довкілля та сільського господарства України*. URL: https://www.me.gov.ua/Profession/List?lang=uk-UA&id=d4162ef8-2771-4ac5-99ef-1d4b6f5336af&tag=KlasifikatorProfesii-Poshuk (дата звернення: 09.02.2026).

132. Радиш Я. Ф., Євтушенко В.В. Українська народна медицина як національний феномен: генеза та перспективи розвитку (до проблеми державного управління у сфері народної медицини і цілительства). *Інвестиції: практика та досвід*. 2015. № 12. С. 63–71. URL: http://www.investplan.com.ua/pdf/12_2015/16.pdf.

Information about the authors:
Dumchikov Mykhailo Oleksandrovych,
Doctor of Law, Associate Professor,
Associate Professor of Criminal Legal Disciplines
and Proceedings Department,
Academic and Research Institute of Law,
Sumy State University,
59, Petropavlivska St., Academic Building No. 3, Sumy, 40000, Ukraine
https://orcid.org/0000-0002-4244-2419

Yanishevska Kateryna Dmytrivna,
Candidate of Law, Associate Professor,
Associate Professor of Criminal Legal Disciplines
and Proceedings Department,
Academic and Research Institute of Law,
Sumy State University,
59, Petropavlivska St., Academic Building No. 3, Sumy, 40000, Ukraine
https://orcid.org/0000-0002-3648-5543

Murach Dmytro Vasylovych,
PhD student,
Academic and Research Institute of Law,
Sumy State University,
59, Petropavlivska St., Academic Building No. 3, Sumy, 40000, Ukraine
https://orcid.org/0000-0002-4645-1275

DOI https://doi.org/10.30525/978-9934-26-686-7-7

ПРО ДЕТЕКТИВНУ (РОЗШУКОВУ) ДІЯЛЬНІСТЬ У ВІЙСЬКОВІЙ КРИМІНАЛІСТИЦІ (НАЦІОНАЛЬНИЙ І МІЖНАРОДНИЙ ВИМІР)

Калюга К. В.

ВСТУП

Повномасштабна збройна агресія проти України спричинила безпрецедентне зростання кількості воєнних злочинів, що зумовило докорінну трансформацію підходів до їх документування, розслідування та доказування. Сучасні умови збройного конфлікту характеризуються високою інтенсивністю бойових дій, масштабністю руйнувань, переміщенням цивільного населення, окупацією окремих територій, а також активним використанням цифрових технологій у військовій сфері. У таких обставинах традиційні криміналістичні методики виявляються недостатніми без їх суттєвої модернізації та інтеграції з новітніми інформаційно-аналітичними інструментами. Це зумовлює необхідність формування цілісної концепції детективної діяльності у сфері військової криміналістики як окремого напряму наукового осмислення.

Воєнні злочини відрізняються від загальнокримінальних правопорушень як за своєю правовою природою, так і за механізмом вчинення, структурою суб'єктного складу та особливостями доказування. Вони нерозривно пов'язані з контекстом збройного конфлікту, що потребує встановлення не лише факту вчинення конкретного діяння, а й його зв'язку з бойовими діями, військовими операціями або політикою держави-агресора. Особливої складності набуває доведення індивідуальної кримінальної відповідальності в умовах ієрархічної військової організації, де значна частина рішень приймається колегіально або в межах вертикалі командування. Відтак документування командної відповідальності, реконструкція ланцюгів наказів і встановлення реального контролю над підлеглими потребують застосування комплексних аналітичних та криміналістичних методів.

Детективна діяльність у справах про воєнні злочини має багатовимірний характер. Вона поєднує процесуальні дії, оперативно-розшукову роботу, аналітичну обробку великих масивів інформації, використання цифрових доказів, методи відкритої розвідки (OSINT), криміналістичне моделювання подій та міжнародну співпрацю. Сучасні воєнні злочини дедалі частіше фіксуються за допомогою супутникових знімків, відеозаписів із безпілотних літальних апаратів, матеріалів соціальних мереж, геолокаційних даних, перехоплених комунікацій тощо. Це трансформує доказову систему, формуючи гібридну модель, у якій поєднуються матеріальні, цифрові та інтелектуальні джерела інформації.

Особливої уваги потребує здійснення детективної діяльності на тимчасово окупованих або щойно деокупованих територіях. Обмежений доступ до місць подій, знищення або пошкодження об'єктів інфраструктури, мінна небезпека,

психологічний стан потерпілих, свідків і очевидців, ризики для безпеки працівників правоохоронних органів істотно ускладнюють процес доказування. У таких умовах важливого значення набувають дистанційні форми документування, збереження цифрових слідів, створення аналітичних баз даних, а також взаємодія з міжнародними партнерами та громадськими ініціативами, що здійснюють первинну фіксацію подій.

Міжнародний вимір розслідування воєнних злочинів зумовлює необхідність узгодження національних процедур із міжнародними стандартами доказування. Співпраця з іноземними правоохоронними органами, участь у спільних слідчих групах, обмін інформацією, забезпечення збереження та автентичності доказів відповідно до вимог міжнародного кримінального правосуддя стають невід'ємними складовими сучасної детективної діяльності. Таким чином, вона набуває не лише внутрішньодержавного, а й транснаціонального характеру.

Актуальність дослідження зумовлена потребою теоретичного узагальнення новітньої практики розслідування воєнних злочинів, формування системної моделі детективної діяльності у військовій криміналістиці та визначення її структурних елементів. Незважаючи на наявність значної кількості наукових праць у сфері міжнародного кримінального права та криміналістики, комплексне осмислення детективної діяльності як самостійного інституційного та методологічного феномену в умовах повномасштабного збройного конфлікту сьогодні залишається недостатньо розробленим.

Метою дослідження є обґрунтування теоретичних засад детективної діяльності у справах про воєнні злочини, аналіз її організаційних, процесуальних та аналітичних компонентів, а також визначення основних проблем і перспектив подальшого розвитку. Для досягнення поставленої мети передбачається вирішення завдань щодо систематизації суб'єктного складу детективної діяльності, дослідження механізмів встановлення особи невідомого злочинця та документування командної відповідальності, аналізу використання цифрових технологій і відкритих джерел інформації, а також оцінки ролі міжнародної співпраці.

Наукова новизна роботи полягає у формуванні комплексної концепції детективної діяльності у військовій криміналістиці як інтегративної системи, що поєднує кримінально-правові, кримінально-процесуальні, криміналістичні та інформаційно-аналітичні компоненти. Запропонований підхід дозволяє розглядати детективну діяльність не лише як сукупність окремих слідчих дій, а як стратегічно організований процес документування воєнних злочинів із використанням сучасних технологій та міжнародних стандартів доказування.

Дослідження спрямоване на формування науково обґрунтованої моделі детективної діяльності, здатної забезпечити ефективне розслідування, фіксацію та притягнення до відповідальності осіб, винних у вчиненні воєнних злочинів, в умовах сучасних викликів і трансформацій кримінального правосуддя.

1. Загальна характеристика детективної діяльності у військовій криміналістиці

Детективна діяльність у військовій криміналістиці є складною міждисциплінарною формою професійної діяльності, що поєднує пізнавальні, аналітичні та практичні компоненти, спрямовані на виявлення, фіксацію, дослідження й використання інформації про воєнні та пов'язані з ними злочини. Вона здійснюється в умовах збройного конфлікту та воєнного стану, що зумовлює підвищені вимоги до оперативності, безпеки, доказової надійності та міжнародної сумісності результатів такої діяльності [1][2][3][4].

За своєю сутністю детективна діяльність не зводиться виключно до процесуального досудового розслідування чи оперативно-розшукової роботи. Вона має інтегративний характер і охоплює сукупність процесуально врегульованих та позапроцесуальних дій, аналітичну обробку великих масивів даних, використання спеціальних знань, криміналістичних методик, цифрових технологій, а також елементів кримінального аналізу та прогнозування. Саме така комплексність дозволяє ефективно встановлювати фактичні дані в кримінальних провадженнях щодо воєнних злочинів і забезпечувати належний рівень доказування як на національному, так і на міжнародному рівнях. Зокрема у співвідношенні зі слідчою та оперативно-розшуковою діяльністю детективна діяльність виступає як узагальнювальна й координуюча категорія. Слідча діяльність має чітко визначені процесуальні межі та спрямована на збирання, перевірку й оцінку доказів у межах кримінального провадження. Оперативно-розшукова діяльність, своєю чергою, зорієнтована на негласне здобуття інформації, попередження та припинення злочинів, встановлення осіб, причетних до їх вчинення. Детективна діяльність поєднує ці складові з аналітичними процедурами, криміналістичним моделюванням події злочину, встановленням прихованих зв'язків між суб'єктами, подіями та процесами, що особливо важливо в умовах війни. Специфіка воєнного стану істотно трансформує зміст і форми детективної діяльності. Обмежений або повністю відсутній доступ до місць подій, активні бойові дії, мінування територій, руйнування інфраструктури, масовість злочинів та значна кількість потерпілих і свідків ускладнюють традиційні криміналістичні процедури. У таких умовах особливого значення набувають дистанційні способи збирання інформації, використання супутникових знімків, безпілотних літальних апаратів,

---

[1] Величко О. О. Участь прокурора в доказуванні воєнних злочинів: стан наукових досліджень. *Аналітично-порівняльне правознавство.* 2025. Т. 5. № 3. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.19.

[2] Єфіменко Т. С. Особливості доказування у кримінальних провадженнях щодо воєнних злочинів. *Вісник Кримінологічної асоціації України.* 2024. № 3. DOI: https://doi.org/10.32631/vca.2024.3.25.

[3] Кудінов С. С., Шехавцов Р. М. Особливості організації розслідування воєнних злочинів в Україні в умовах воєнного стану. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. Т. 4. № 91. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.46.

[4] Погоріла С. І. Використання OSINT-технологій у розслідуванні воєнних злочинів: сучасний стан і перспективи. *Актуальні проблеми сучасної науки в дослідженнях молодих учених.* Вінниця : ХНУВС, 2025. С. 346–348. dspace.univd.edu.ua.

геолокаційних даних, відкритих джерел інформації, а також міжнародних механізмів фіксації та збереження доказів. Крім того, детективна діяльність у період війни має яскраво виражений міжнародний вимір. Документування воєнних злочинів здійснюється з урахуванням стандартів міжнародного гуманітарного та кримінального права, що зумовлює необхідність забезпечення належної якості доказів, їхньої автентичності, збереження ланцюга володіння та можливості подальшого використання в міжнародних судових інституціях. У цьому контексті детективна діяльність виходить за межі суто національної правозастосовної практики та стає складовою глобальної системи протидії найтяжчим міжнародним злочинам[567].

Отже, детективна діяльність у військовій криміналістиці в умовах війни є самостійним, комплексним видом професійної діяльності, який забезпечує ефективне поєднання процесуальних, оперативно-розшукових та аналітичних інструментів, адаптованих до екстремальних умов збройного конфлікту. Її значення полягає не лише у встановленні обставин конкретних кримінальних правопорушень, а й у формуванні доказової бази для притягнення винних до відповідальності, відновлення справедливості та забезпечення історичної правди про злочини війни.

2. Система суб'єктів детективної діяльності у справах про воєнні злочини

Система суб'єктів детективної діяльності у справах про воєнні злочини в умовах збройного конфлікту та воєнного стану є складною, багаторівневою та міжінституційною. Її формування зумовлене як внутрішньодержавними потребами ефективного кримінального переслідування осіб, винних у вчиненні воєнних і пов'язаних із ними злочинів, так і міжнародними зобов'язаннями України у сфері міжнародного гуманітарного та міжнародного кримінального права. Ключову роль у здійсненні детективної діяльності відіграють слідчі органів досудового розслідування, передусім слідчі органів Національної поліції України, Державного бюро розслідувань та Служби безпеки України у межах їх предметної підслідності. Саме на цих суб'єктів покладено основний обсяг процесуально регламентованої діяльності щодо виявлення, фіксації, вилучення та первинної оцінки доказів воєнних злочинів. В умовах війни їх діяльність набуває особливої специфіки, оскільки здійснюється за обмеженого доступу до місць подій, за наявності загроз життю та здоров'ю, а також за необхідності

[5] Кудінов С. С., Шехавцов Р. М. Особливості організації розслідування воєнних злочинів в Україні в умовах воєнного стану. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. Т. 4. № 91. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.46.

[6] Погорецький М. А. Документування і доказування міжнародних злочинів в Україні: процесуально-криміналістичні та цифрові стандарти прийнятності доказів для Міжнародного кримінального суду та спеціального військового трибуналу. *Аналітично-порівняльне правознавство.* 2025. Т. 3. № 6. С. 94–114. DOI: https://doi.org/10.24144/2788-6018.2025.06.3.94.

[7] Тимошко В. В. Використання спеціальних знань під час документування та розслідування воєнних злочинів. *Вісник кримінологічної асоціації України.* 2026. № 31(1). С. 307–314. DOI: https://doi.org/10.24144/vca.2026.31.1.307.

документування злочинів, учинених у межах масштабних і системних збройних дій. Важливе місце в системі суб'єктів детективної діяльності посідають прокурори, які відповідно до кримінального процесуального законодавства України здійснюють процесуальне керівництво досудовим розслідуванням. У справах про воєнні злочини роль прокурора виходить за межі класичного процесуального контролю та включає формування загальної стратегії розслідування, визначення його пріоритетів, координацію дій між різними правоохоронними органами, а також забезпечення дотримання міжнародних стандартів доказування. Особливого значення набуває орієнтація прокурорів на стандарти Міжнародного кримінального суду, зокрема щодо доведення контексту збройного конфлікту, наявності ланцюга командування, елементів командної відповідальності та системності вчинення злочинів. У релевантних кримінальних провадженнях суб'єктами детективної діяльності можуть виступати також детективи Національного антикорупційного бюро України та Бюро економічної безпеки України. Їх участь є обґрунтованою у випадках, коли воєнні злочини поєднуються з корупційними, економічними або службовими правопорушеннями, зокрема розкраданням військового майна, зловживанням службовим становищем в умовах воєнного стану, незаконним використанням міжнародної гуманітарної допомоги. У таких провадженнях детективна діяльність набуває комплексного характеру, поєднуючи криміналістичні, фінансово-аналітичні та оперативно-розшукові методи. Окрему, надзвичайно важливу групу суб'єктів детективної діяльності становлять міжнародні слідчі групи та представники міжнародних організацій, які залучаються до документування воєнних злочинів. Йдеться, зокрема, про спільні слідчі групи (Joint Investigation Teams), створені за участю України, держав-членів Європейського Союзу, Євроюсту, а також про співпрацю з Офісом прокурора Міжнародного кримінального суду. Діяльність таких суб'єктів спрямована не лише на збір доказів, а й на їх аналітичну систематизацію, перевірку відповідності міжнародним стандартам та підготовку матеріалів для можливого міжнародного кримінального переслідування. Ефективність цієї діяльності безпосередньо залежить від узгодженості дій усіх суб'єктів, чіткого розмежування їх повноважень, а також спільного розуміння цілей розслідування воєнних злочинів як на рівні національного правосуддя, так і в контексті міжнародної кримінальної юстиції[89].

[8] Римський статут Міжнародного кримінального суду від 17 липня 1998 р. *Рада. Верховна Рада України. Законодавство України.* URL : https://zakon.rada.gov.ua/laws/show/995_588#Text.

[9] Чернецька О. В. Міжнародне співробітництво під час розслідування воєнних кримінальних правопорушень. Ірпінський юридичний часопис. 2025. № 2(19). С. 266–273. DOI: https://doi.org/10.33244/2617-4154-2(19)-2025-266-273.

3. Встановлення особи злочинця та документування командної відповідальності

Встановлення особи злочинця у справах про воєнні злочини є одним із найбільш складних і водночас принципово важливих завдань детективної діяльності у військовій криміналістиці. Специфіка цього завдання зумовлена як особливими умовами вчинення злочинів під час збройного конфлікту, так і колективним, ієрархічним характером військової діяльності, у межах якої протиправні діяння часто реалізуються не ізольовано, а як елемент організованої системи командування та підпорядкування. На відміну від «звичайних» кримінальних правопорушень, у воєнних злочинах ідентифікація особи злочинця не обмежується встановленням безпосереднього виконавця. Детективна діяльність спрямовується на з'ясування повного кола причетних осіб, включаючи тих, хто віддавав накази, забезпечував умови для їх виконання, здійснював контроль або свідомо не запобіг злочинним діям. У цьому контексті особливого значення набуває концепція індивідуальної кримінальної відповідальності у міжнародному гуманітарному праві, що передбачає відповідальність як за пряме вчинення злочину, так і за співучасть, підбурювання, пособництво або командну бездіяльність. Ідентифікація військовослужбовців як потенційних суб'єктів воєнних злочинів здійснюється із застосуванням комплексу криміналістичних, інформаційно-аналітичних та технічних засобів. До традиційних джерел ідентифікації належать службові документи, військові квитки, жетони, формений одяг, розпізнавальні знаки, шеврони, символіка підрозділів, а також дані військового обліку. Водночас у сучасних умовах збройного конфлікту дедалі більшого значення набувають цифрові сліди діяльності військовослужбовців. До таких слідів належать матеріали фото- та відеофіксації, записи з безпілотних літальних апаратів, супутникові знімки, дані мобільного зв'язку, геолокаційна інформація, а також контент із соціальних мереж і месенджерів. Детективна діяльність у цьому аспекті полягає не лише у збиранні зазначених даних, а й у їхній систематизації, співставленні та верифікації з метою достовірного встановлення особи конкретного військовослужбовця, його належності до певного підрозділу та фактичної присутності у місці вчинення злочину. Однією з ключових особливостей детективної діяльності у військовій криміналістиці є необхідність встановлення ланцюга командування. Що передбачає реконструкцію структури військового підрозділу, визначення посадових обов'язків кожної особи, аналіз службових наказів, рапортів, журналів бойових дій, а також неформальних каналів управління. Особливе значення має з'ясування того, чи усвідомлювали командири злочинний характер відданих наказів, чи мали вони реальну можливість запобігти вчиненню злочину та чи вживали для цього необхідних заходів. У цьому аспекті детективна діяльність тісно пов'язана з доктриною командної відповідальності, що визнається як національним кримінальним правом, так і практикою міжнародних кримінальних судових інституцій. Детективи та слідчі мають не лише встановити формальну підпорядкованість, а й довести фактичний контроль командира над підлеглими, що є вирішальним для кваліфікації його дій або бездіяльності. Найскладнішим елементом детективної діяльності у справах про

воєнні злочини є доведення персональної участі конкретної особи у злочині. Йдеться не лише про встановлення фізичної присутності особи на місці події, а й про доведення її активної ролі, форми вини, наміру та усвідомлення протиправного характеру власних дій або отриманих наказів. Детективна діяльність у цьому напрямі базується на комплексному аналізі доказів різної природи: показань свідків і потерпілих, матеріалів відеофіксації, цифрових слідів, службових документів, результатів експертних досліджень. Особливу роль відіграє криміналістичний аналіз поведінки особи, що дозволяє встановити послідовність її дій, мотивацію та ступінь усвідомлення наслідків. Саме комплексність дозволяє забезпечити індивідуалізацію кримінальної відповідальності та уникнути колективного або абстрактного покладання вини. Специфіка детективної діяльності щодо встановлення особи злочинця у військовій криміналістиці полягає у поєднанні ідентифікаційних, аналітичних та доказових процедур, спрямованих на всебічне відтворення ролі кожного учасника воєнного злочину. Це забезпечує відповідність розслідувань як вимогам національного кримінального процесу, так і стандартам міжнародного кримінального правосуддя[101112].

4. Аналітична детективна діяльність у структурі військової криміналістики

Аналітична детективна діяльність посідає ключове місце у структурі військової криміналістики та є визначальним чинником ефективності розслідування воєнних злочинів. Її значення зумовлене насамперед масштабністю та складністю таких злочинів, множинністю джерел інформації, колективним характером протиправної діяльності та необхідністю встановлення системних закономірностей злочинної поведінки в умовах збройного конфлікту. На відміну від класичних форм слідчої діяльності, орієнтованих переважно на аналіз окремого епізоду, аналітична детективна діяльність має комплексний і стратегічний характер. Вона спрямована на обробку, узагальнення та інтерпретацію великих масивів різнорідних даних з метою виявлення прихованих зв'язків, причинно-наслідкових залежностей і повторюваних моделей злочинної поведінки. В умовах сучасної війни детективна діяльність здійснюється в середовищі надзвичайно великих інформаційних потоків. До них належать показання великої кількості свідків і потерпілих, матеріали кримінальних проваджень, цифрові дані з мобільних пристроїв, інформація з відкритих джерел (OSINT), супутникові знімки, матеріали міжнародних правозахисних організацій, звіти моніторингових місій, а також аналітичні продукти спільних слідчих груп. Аналітична детективна

[10] Freeman L. Digital Evidence and War Crimes Prosecutions: The Impact of New Technologies on International Criminal Investigations. Cambridge : Cambridge University Press, 2020. 350 p.

[11] International Criminal Court, Office of the Prosecutor. Strategic Plan 2023–2025. The Hague : ICC, 2023. 40 p. URL : https://www.icc-cpi.int/sites/default/files/2023-07/2023-2025-Strategic-Plan.pdf.

[12] Mettraux G. The Law of Command Responsibility. Oxford : Oxford University Press, 2009. 522 p.

діяльність у цьому контексті полягає не лише у збиранні зазначених даних, а насамперед у їх структуризації, класифікації та інтеграції. Використання методів аналізу великих масивів даних (Big Data) дозволяє об'єднувати розрізнені факти в єдину аналітичну систему, виявляти повторювані події, типові сценарії злочинної діяльності, а також просторово-часові закономірності вчинення воєнних злочинів. Особливого значення набуває кореляційний аналіз, який дозволяє встановлювати зв'язки між подіями, особами та підрозділами, навіть за відсутності прямих доказів. Такий підхід є надзвичайно важливим у ситуаціях, коли доступ до місця події обмежений або відсутній, а доказова база формується за рахунок непрямих і цифрових джерел. Одним із центральних завдань такої аналітичної детективної діяльності є встановлення моделей злочинної поведінки у воєнних злочинах. Йдеться про виявлення повторюваних способів дій, типових форм насильства, однакових підходів до вибору жертв, а також характерних ознак організації та виконання злочинних наказів. Військова криміналістика виходить з того, що воєнні злочини рідко мають випадковий характер. Навпаки, вони часто є елементом системної політики або практики, що реалізується через конкретні військові підрозділи, командирів і виконавців. Аналітична детективна діяльність дозволяє виявити такі системні риси, що має вирішальне значення для доведення не лише окремих епізодів, а й загального злочинного контексту. Моделювання злочинної поведінки включає аналіз способів підготовки та вчинення злочинів, використаних засобів і методів, реакції виконавців на зовнішні обставини, а також їхню поведінку після вчинення злочину. На основі такого аналізу формуються узагальнені криміналістичні моделі, які дозволяють прогнозувати подальші дії злочинців, визначати найбільш імовірних суб'єктів злочину та оптимізувати тактичні рішення детективів і слідчих. Криміналістичний аналіз є методологічною основою аналітичної детективної діяльності у військовій криміналістиці. Він поєднує логічні, статистичні, психологічні та інформаційні методи дослідження, спрямовані на пізнання механізму злочинної діяльності у її цілісності. У справах про воєнні злочини криміналістичний аналіз застосовується для відновленні подій, встановлення ролей окремих осіб, аналізу командних рішень та оцінки їх відповідності нормам міжнародного гуманітарного права. Особливу роль відіграє аналіз сукупності доказів, коли кожен окремий доказ може мати обмежену доказову силу, але в поєднанні з іншими утворює логічно узгоджену та переконливу систему. Аналітична детективна діяльність також передбачає використання профілювання осіб, причетних до воєнних злочинів, з урахуванням їхніх посадових функцій, попереднього досвіду, стилю управління та поведінкових характеристик. Це дозволяє більш точно визначати ступінь їхньої відповідальності та диференціювати роль виконавців і командирів. Аналітична детективна діяльність у військовій криміналістиці в такому сенсі виступає не допоміжним, а системоутворюючим елементом розслідування воєнних злочинів. Вона забезпечує перехід від фрагментарного збирання фактів до цілісного розуміння злочинної діяльності як соціально-правового та організаційного явища. Саме завдяки аналітичному підходу стає можливим доведення системності воєнних злочинів, встановлення причинно-наслідкових зв'язків між рішеннями

командування та діями виконавців, а також формування доказової бази, придатної для використання як у національних судах, так і в міжнародних судових інституціях[13][14][15][16][17][18][19][20].

5. Використання OSINT у детективній діяльності щодо воєнних злочинів

Зазначимо, що сьогодні використання відкритих джерел інформації (Open Source Intelligence, OSINT) у сучасній детективній діяльності стало одним із ключових інструментів військової криміналістики. У контексті збройного конфлікту та воєнного стану OSINT набуває особливого значення, оскільки дозволяє отримувати, перевіряти та аналізувати інформацію про воєнні злочини за умов обмеженого доступу до місця події, відсутності безпосереднього контролю над територіями або неможливості негайного проведення слідчих (розшукових) дій. Сутність використання OSINT у детективній діяльності полягає в системному зборі та аналітичній обробці інформації, що міститься у відкритих і загальнодоступних джерелах, з подальшим її процесуальним закріпленням та використанням у доказуванні. На відміну від оперативно-розшукових заходів, OSINT не передбачає негласного втручання у приватне життя, однак потребує високого рівня методичної підготовки та критичного мислення з боку правоохоронців (слідчих, детективів тощо). Соціальні мережі є одним із найпотужніших джерел OSINT у розслідуванні воєнних злочинів. Публікації військовослужбовців, очевидців, місцевих жителів, журналістів

[13] Eurojust. Core International Crimes Casework Report 2023. The Hague : Eurojust, 2023. 52 p. URL : https://www.eurojust.europa.eu/publication/core-international-crimes-casework-report-2023.

[14] European Union Agency for Criminal Justice Cooperation (Eurojust). Guidelines for Prosecuting Core International Crimes. The Hague : Eurojust, 2023. 78 p. URL : https://www.eurojust.europa.eu/publication/guidelines-prosecuting-core-international-crimes.

[15] International Criminal Court. Policy on Case Selection and Prioritisation. The Hague : International Criminal Court, 2023. 28 p. URL : https://www.icc-cpi.int/sites/default/files/2023-02/2023-Policy-on-Case-Selection-and-Prioritisation.pdf.

[16] International Criminal Court. Prosecutor v. Jean-Pierre Bemba Gombo. Judgment pursuant to Article 74 of the Statute. ICC-01/05-01/08-3343. 21 March 2016. URL : https://www.icc-cpi.int/court-record/icc-01/05-01/08-3343.

[17] United Nations Independent International Commission of Inquiry on Ukraine. Report of the Independent International Commission of Inquiry on Ukraine. Geneva : United Nations, 2023. URL : https://www.ohchr.org/en/hr-bodies/hrc/iicihr-ukraine.

[18] United Nations. Berkeley Protocol on Digital Open Source Investigations. New York ; Geneva : United Nations, 2022. 132 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

[19] United Nations. Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Istanbul Protocol). 2022 revised edition. New York : United Nations, 2022. 224 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/istanbul-protocol.

[20] Werle G., Jeßberger F. Principles of International Criminal Law. 4th ed. Oxford : Oxford University Press, 2023. 711 p.

та пропагандистських ресурсів нерідко містять відомості про час, місце та обставини вчинення злочинів, участь конкретних осіб або підрозділів, а також про ланцюг командування. У детективній діяльності інформація із соціальних мереж використовується для: ідентифікації осіб, причетних до воєнних злочинів; встановлення їхнього місця перебування у визначений проміжок часу; підтвердження належності до конкретного військового підрозділу; відтворення подій та перевірки показань свідків. Водночас соціальні мережі є середовищем високого рівня дезінформації, маніпуляцій та постановочних матеріалів. У зв'язку з цим детективна діяльність у сфері OSINT передбачає обов'язкову перевірку автентичності акаунтів, часу та місця публікацій, аналіз метаданих, зіставлення інформації з іншими джерелами та використання принципу множинного підтвердження. Відео- та фотоматеріали, отримані з відкритих джерел, відіграють особливо важливу роль у документуванні воєнних злочинів. Вони дозволяють фіксувати наслідки обстрілів, авіаударів, знищення цивільної інфраструктури, поводження з військовополоненими та цивільним населенням. У детективній діяльності такі матеріали використовуються для: встановлення факту вчинення злочину; визначення типу застосованого озброєння; ідентифікації осіб, техніки та символіки підрозділів; відтворення послідовності подій. Особливе значення має криміналістичний аналіз зображень, який включає перевірку цілісності файлів, аналіз тіней, погодних умов, об'єктів місцевості, зіставлення з іншими відео- та фотоданими. Детективна діяльність у цій сфері вимагає залучення спеціальних знань і експертів, а також чіткого дотримання вимог процесуального оформлення доказів. Супутникові знімки та геолокаційні дані є одним із найбільш об'єктивних і переконливих джерел OSINT у розслідуванні воєнних злочинів. Вони дозволяють фіксувати зміни місцевості, переміщення військової техніки, наслідки бойових дій та руйнування цивільних об'єктів у динаміці (дані використовуються для: підтвердження місця і часу вчинення злочину; встановлення маршрутів переміщення підрозділів; зіставлення показань свідків з об'єктивними даними; доведення системного характеру злочинної діяльності. Геолокаційні дані, отримані з цифрових пристроїв, застосовуються для встановлення місця перебування конкретних осіб у критичний момент, що має вирішальне значення для доведення персональної участі у воєнному злочині. Ключовою особливістю використання OSINT у детективній діяльності є необхідність його належного процесуального закріплення. Інформація з відкритих джерел сама по собі не завжди має статус доказу, однак може слугувати підставою для проведення слідчих (розшукових) дій, формування слідчих версій та отримання процесуально допустимих доказів. Взагалі, у міжнародному вимірі OSINT дедалі активніше використовується у практиці міжнародних кримінальних трибуналів і Міжнародного кримінального суду, що зумовлює необхідність дотримання високих стандартів верифікації, збереження ланцюга доказів та документування джерел походження інформації. OSINT у детективній діяльності у військовій криміналістиці – це стратегічно важливий інструмент встановлення фактичних даних у справах про воєнні злочини. Його ефективність залежить від поєднання технічних можливостей,

аналітичного мислення та чіткого дотримання процесуальних і етичних стандартів[21][22][23][24].

6. Особливості детективної діяльності на тимчасово окупованих територіях

Детективна діяльність у справах про воєнні злочини, вчинені на тимчасово окупованих територіях, характеризується особливою складністю та специфічними умовами здійснення. Відсутність ефективного контролю з боку державних органів України, обмежений або повністю відсутній доступ до місця події, постійна загроза життю та безпеці осіб, а також активна протидія з боку окупаційних адміністрацій зумовлюють необхідність застосування нетрадиційних підходів до збору та аналізу доказової інформації. У таких умовах детективна діяльність виходить за межі класичної моделі безпосереднього огляду місця події та проведення слідчих (розшукових) дій. Вона набуває відкладеного, дистанційного та багаторівневого характеру, поєднуючи елементи криміналістичного аналізу, аналітичної роботи, використання цифрових технологій та міжнародної співпраці. Однією з ключових проблем детективної діяльності на тимчасово окупованих територіях є фактична неможливість своєчасного та повноцінного огляду місця події. Детективи та слідчі позбавлені можливості безпосередньо фіксувати сліди злочину, вилучати речові докази, проводити слідчі експерименти та інші процесуальні дії у момент вчинення злочину або одразу після нього. У зв'язку з цим особливого значення набуває криміналістичне відтворення (реконструкція) подій, що ґрунтується на аналізі непрямих доказів, цифрових слідів, матеріалів відкритих джерел та свідчень осіб, які залишили окуповану територію. Детективна діяльність у таких умовах орієнтується не стільки на фіксацію окремих слідів, скільки на відтворення загальної картини злочину з урахуванням часових, просторових і поведінкових чинників. Важливим напрямом детективної діяльності на тимчасово окупованих територіях є робота з внутрішньо переміщеними особами, біженцями та іншими свідками, які залишили зону окупації. Саме ці особи часто виступають основним джерелом первинної інформації про вчинені воєнні злочини, їхніх виконавців та обставини. Особливістю допиту таких свідків є їхній психологічний стан, зумовлений пережитим насильством, тривалим перебуванням у зоні бойових дій, страхом репресій щодо родичів, які залишилися на окупованій території. Детективна діяльність у цьому контексті потребує застосування спеціальних тактичних

[21] Eurojust. Core International Crimes Casework Report 2023. The Hague : Eurojust, 2023. 52 p. URL : https://www.eurojust.europa.eu/publication/core-international-crimes-casework-report-2023.

[22] International Criminal Court. Prosecutor v. Jean-Pierre Bemba Gombo. Judgment pursuant to Article 74 of the Statute. ICC-01/05-01/08-3343. 21 March 2016. URL : https://www.icc-cpi.int/court-record/icc-01/05-01/08-3343.

[23] United Nations Independent International Commission of Inquiry on Ukraine. Report of the Independent International Commission of Inquiry on Ukraine. Geneva : United Nations, 2023. URL : https://www.ohchr.org/en/hr-bodies/hrc/iicihr-ukraine.

[24] United Nations. Berkeley Protocol on Digital Open Source Investigations. New York ; Geneva : United Nations, 2022. 132 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

прийомів, спрямованих на мінімізацію повторної травматизації, забезпечення безпеки свідків та отримання максимально повних і достовірних показань. Значну роль відіграє також фіксація показань у формі, придатній для подальшого використання у судових провадженнях, зокрема в міжнародних судових інституціях. Це вимагає дотримання стандартів документування, передбачених міжнародним гуманітарним правом і практикою Міжнародного кримінального суду. Умови тимчасової окупації зумовлюють широке застосування дистанційного документування воєнних злочинів як одного з ключових інструментів детективної діяльності. Йдеться про збирання та аналіз інформації без фізичної присутності на місці події, з використанням цифрових технологій, OSINT, супутникових знімків, відео- та фотоматеріалів, а також матеріалів міжнародних і неурядових організацій. Дистанційне документування дозволяє фіксувати факти злочинів у режимі реального часу або з мінімальною затримкою, зберігати докази до моменту деокупації територій та формувати первинну доказову базу. При цьому детективна діяльність повинна бути спрямована на забезпечення автентичності, цілісності та перевірюваності таких матеріалів, що має вирішальне значення для їх подальшого процесуального використання. Особливістю детективної діяльності на тимчасово окупованих територіях є її відкладений характер. Первинне документування злочинів здійснюється заочно, тоді як повноцінне досудове розслідування, включно з оглядом місця події, експертними дослідженнями та вилученням речових доказів, часто можливе лише після деокупації відповідної території. Такий підхід вимагає стратегічного планування детективної діяльності, збереження та систематизації зібраної інформації, а також підготовки до повторного або додаткового документування злочинів у майбутньому. Водночас він дозволяє забезпечити безперервність розслідування та недопущення втрати доказів навіть за відсутності доступу до місця події. Можна сказати, що, детективна діяльність на тимчасово окупованих територіях виступає самостійним і надзвичайно складним напрямом військової криміналістики. Вона поєднує елементи криміналістичного аналізу, психології, цифрових технологій та міжнародного співробітництва, забезпечуючи можливість документування воєнних злочинів навіть у найскладніших умовах. А ефективність такої діяльності має вирішальне значення не лише для притягнення винних осіб до кримінальної відповідальності, а й для відновлення історичної справедливості, захисту прав потерпілих та формування доказової бази для міжнародної кримінальної юстиції [25][26][27][28].

[25] International Criminal Court. Prosecutor v. Jean-Pierre Bemba Gombo. Judgment pursuant to Article 74 of the Statute. ICC-01/05-01/08-3343. 21 March 2016. URL : https://www.icc-cpi.int/court-record/icc-01/05-01/08-3343.

[26] United Nations Independent International Commission of Inquiry on Ukraine. Report of the Independent International Commission of Inquiry on Ukraine. Geneva : United Nations, 2023. URL : https://www.ohchr.org/en/hr-bodies/hrc/iicihr-ukraine.

[27] United Nations. Berkeley Protocol on Digital Open Source Investigations. New York ; Geneva : United Nations, 2022. 132 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

[28] United Nations. Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Istanbul Protocol). 2022 revised edition. New York : United Nations, 2022. 224 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/istanbul-protocol.

7. Міжнародна детективна співпраця

Міжнародна детективна співпраця у сфері розслідування воєнних злочинів є невід'ємною складовою сучасної військової криміналістики та зумовлена транснаціональним характером таких правопорушень, масштабністю їх наслідків, а також необхідністю дотримання міжнародних стандартів доказування. В умовах збройних конфліктів національні правоохоронні органи об'єктивно потребують координації з міжнародними інституціями, що володіють спеціальними мандатами, досвідом та ресурсами для документування і правової оцінки воєнних злочинів. Однією з найбільш ефективних форм такої взаємодії є створення спільних слідчих груп (Joint Investigation Teams – JIT). Їх діяльність дозволяє об'єднати зусилля правоохоронних органів кількох держав, забезпечити оперативний обмін інформацією, спільне планування слідчих та детективних дій, а також узгоджене використання доказів у національних та міжнародних кримінальних провадженнях. У межах JIT формується єдиний підхід до збору, фіксації та збереження доказів, що має особливе значення для подальшого їх використання в міжнародних судових інстанціях. Важливим напрямом міжнародної детективної співпраці є взаємодія з Міжнародним кримінальним судом. Вона охоплює передачу матеріалів кримінальних проваджень, аналітичних звітів, результатів експертних досліджень, а також координацію дій щодо ідентифікації осіб, які можуть нести індивідуальну кримінальну відповідальність за воєнні злочини. При цьому національні органи досудового розслідування адаптують свою детективну діяльність до стандартів доказування, що застосовуються МКС, зокрема щодо доведення ланцюга командування, наявності умислу та усвідомлення протиправного характеру вчинених дій. Обмін доказовою інформацією між державами та міжнародними організаціями становить окремий напрям міжнародної детективної співпраці. Він включає передачу матеріалів фото- і відеофіксації, супутникових знімків, цифрових даних, результатів OSINT-досліджень, а також свідчень потерпілих, свідків та очевидців. Такий обмін потребує дотримання принципів належної процесуальної форми, захисту персональних даних та забезпечення автентичності доказів, що є критично важливим для їх подальшої правової оцінки. Загалом міжнародна детективна співпраця сприяє уніфікації підходів до розслідування воєнних злочинів, підвищує ефективність документування міжнародних злочинів та створює передумови для невідворотності покарання осіб, винних у грубих порушеннях норм міжнародного гуманітарного права. У контексті військової криміналістики вона виступає важливим інструментом інтеграції національних і міжнародних механізмів правосуддя та зміцнення міжнародної кримінальної юстиції загалом[29] [30] [31].

[29] Bantekas I., Nash S. International Criminal Law. London ; New York : Routledge, 2022. 384 p.

[30] Schmitt M. N. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. xli, 598 p. DOI: https://doi.org/10.1017/9781316822524.

[31] United Nations Office on Drugs and Crime (UNODC). Manual on Mutual Legal Assistance and Extradition. Vienna : United Nations Office on Drugs and Crime, 2018. 456 p. URL : https://www.unodc.org/documents/organized-crime/MLA_Manual_E.pdf.

Тактичні прийоми детективної діяльності у військовій криміналістиці становлять сукупність спеціальних методів і способів організації та здійснення слідчих і аналітичних дій, спрямованих на ефективне викриття воєнних злочинів та встановлення осіб, причетних до їх вчинення. Їх застосування зумовлене складністю військових злочинів, багаторівневістю командних структур, маскуванням протиправної діяльності та активною протидією з боку організованих військових формувань. Однією з базових особливостей тактичних прийомів у військовій криміналістиці є їх спрямованість не лише на фіксацію окремого злочинного діяння, а й на відтворення цілісного механізму злочину, що включає підготовку, прийняття рішень, віддання наказів, виконання та приховування наслідків. У цьому контексті детективна діяльність виходить за межі класичного встановлення факту злочину та набуває системного характеру, орієнтованого на викриття організованої та ієрархічно вибудуваної злочинної поведінки. Одним із ключових тактичних прийомів є приховане встановлення особи злочинця, яке передбачає поетапне накопичення доказової інформації без передчасного розкриття інтересу правоохоронних органів до конкретної особи. Такий підхід дозволяє запобігти знищенню доказів, узгодженню показань між співучасниками та втечі підозрюваних. Прихована ідентифікація злочинців здійснюється шляхом комплексного аналізу цифрових слідів, матеріалів відкритих джерел інформації (OSINT), службових і бойових документів, фото- та відеоматеріалів, перехоплених комунікацій, а також шляхом зіставлення фактичних даних із відомостями про структуру, підпорядкованість і дислокацію військових підрозділів. Такий тактичний прийом дозволяє поступово звужувати коло причетних осіб і переходити до процесуальних дій лише за наявності достатньої доказової бази.

Особливе місце у системі тактичних прийомів посідає документування командної відповідальності, що є однією з визначальних рис розслідування воєнних злочинів. Детективна діяльність у цьому напрямі спрямована на встановлення не лише безпосередніх виконавців протиправних дій, а й осіб командного та керівного складу, які віддавали злочинні накази, санкціонували їх виконання, створювали умови для вчинення злочинів або свідомо не вживали заходів для їх припинення. Документування командної відповідальності потребує ретельного аналізу ланцюга командування, формального і фактичного підпорядкування, порядку прийняття рішень, характеру та змісту відданих наказів, а також встановлення обізнаності командирів щодо протиправного характеру дій підлеглих і можливих наслідків таких дій. У цьому контексті тактичні прийоми детективної діяльності мають відповідати міжнародним стандартам доведення, зокрема принципам індивідуальної кримінальної відповідальності та відповідальності командирів, сформульованим у практиці міжнародних кримінальних трибуналів і Міжнародного кримінального суду. Важливою умовою ефективності тактичних прийомів є поєднання слідчих і аналітичних методів детективної діяльності. Класичні слідчі дії – допити, огляди, обшуки, експертизи, тимчасовий доступ до речей і документів – доповнюються криміналістичним аналізом великих масивів інформації, побудовою аналітичних моделей, реконструкцією подій у просторі й часі, встановленням типових схем та повторюваних елементів

злочинної поведінки. Такий синтез дозволяє не лише фіксувати окремі докази, а й формувати цілісну доказову концепцію кримінального провадження. Окрему увагу в межах тактичних прийомів приділено урахуванню психологічних особливостей підозрюваних, свідків і потерпілих. Розуміння мотивації, рівня підпорядкованості, страху відповідальності, групової лояльності або ідеологічної обумовленості поведінки осіб, причетних до воєнних злочинів, дозволяє обирати найбільш ефективні тактичні прийоми комунікації, допиту, перевірки показань і викриття неправдивої інформації. Загалом тактичні прийоми детективної діяльності у військовій криміналістиці мають комплексний, багаторівневий і міждисциплінарний характер. Вони спрямовані на досягнення головної мети розслідування – повне, всебічне й об'єктивне встановлення обставин воєнного злочину, ролі кожного учасника та забезпечення невідворотності кримінальної відповідальності з дотриманням національних і міжнародних стандартів кримінального провадження[32][33][34][35].

8. Проблеми та перспективи розвитку детективної діяльності

Взагалі, детективна діяльність у сфері розслідування воєнних злочинів характеризується високим рівнем складності, що зумовлено як об'єктивними умовами збройного конфлікту, так і недосконалістю нормативно-правового та організаційного забезпечення. Аналіз проблем і перспектив її розвитку має важливе значення для формування ефективної моделі військової криміналістики, здатної відповідати сучасним викликам війни та післявоєнного правосуддя. Серед ключових проблем детективної діяльності насамперед можна виокремити правові обмеження, пов'язані з фрагментарністю національного законодавства у сфері розслідування воєнних злочинів та його неповною узгодженістю з нормами міжнародного гуманітарного і кримінального права. Чинні процесуальні механізми не завжди враховують специфіку масових злочинів, вчинених у зоні бойових дій або на тимчасово окупованих територіях, що ускладнює належне збирання, фіксацію та збереження доказів. Додатковою проблемою є складність реалізації міжнародної юрисдикції, зокрема у випадках, коли підозрювані перебувають за межами досяжності національних правоохоронних органів або користуються фактичним імунітетом, зумовленим військовим чи політичним статусом. Окрему групу проблем становлять етичні дилеми детективної діяльності, які особливо загострюються в умовах війни. Йдеться, зокрема, про баланс між необхідністю ефективного документування воєнних злочинів і

[32] Ambos K. Treatise on International Criminal Law. Volume III: International Criminal Procedure. 2nd ed. Oxford : Oxford University Press, 2024. 912 p. DOI: https://doi.org/10.1093/law/9780192844262.001.0001.

[33] Cryer R., Friman H., Robinson D., Wilmshurst E. An Introduction to International Criminal Law and Procedure. 4th ed. Cambridge : Cambridge University Press, 2019. 536 p. DOI: https://doi.org/10.1017/9781108689279.

[34] International Criminal Court. Policy on Case Selection and Prioritisation. The Hague : Office of the Prosecutor, ICC, 2023. 28 p. URL : https://www.icc-cpi.int/sites/default/files/2023-02/2023-Policy-on-Case-Selection-and-Prioritisation.pdf.

[35] Sluiter G., Harnisch C., Buisman C., Zahar A. International Criminal Procedure: Principles and Rules. Oxford : Oxford University Press, 2013. 1176 p. DOI: https://doi.org/10.1093/law/9780199658022.001.0001.

дотриманням прав людини, захистом приватності потерпілих, свідків та підозрюваних, а також про допустимі межі використання цифрових даних, матеріалів із соціальних мереж, супутникових знімків і перехоплених комунікацій. Використання таких джерел інформації, з одного боку, значно підвищує ефективність розслідування, а з іншого – породжує ризики порушення принципів законності, пропорційності та недопущення вторинної віктимізації потерпілих. Не менш суттєвими є організаційні та кадрові проблеми, зокрема дефіцит спеціалізованих детективів і аналітиків, недостатній рівень підготовки кадрів у сфері міжнародного кримінального права та військової криміналістики, а також обмеженість технічних і фінансових ресурсів. В умовах війни ці проблеми посилюються постійною загрозою безпеці працівників правоохоронних органів і необхідністю оперативного реагування на велику кількість кримінальних проваджень. Водночас перспективи розвитку детективної діяльності у справах про воєнні злочини пов'язані насамперед з удосконаленням законодавства та практики його застосування. Актуальним є подальше гармонізування національного кримінального і кримінального процесуального законодавства з нормами міжнародного гуманітарного права та стандартами Міжнародного кримінального суду, зокрема щодо визначення складів воєнних злочинів, форм відповідальності та правил доказування. Важливим напрямом є нормативне врегулювання використання цифрових доказів і результатів OSINT-аналізу з метою забезпечення їх допустимості та надійності у кримінальному провадженні. Перспективним напрямом розвитку є також впровадження сучасних аналітичних і інформаційних технологій, включаючи системи обробки великих масивів даних, штучний інтелект, геоінформаційні системи та криміналістичне моделювання. Такі інструменти здатні істотно підвищити ефективність детективної діяльності, сприяти встановленню системних злочинних практик і виявленню прихованих зв'язків між подіями, особами та військовими підрозділами. Вирішальне значення для подальшого розвитку детективної діяльності має розширення міжнародної співпраці, зокрема участь у спільних слідчих групах, обмін доказовою та аналітичною інформацією, залучення експертної підтримки міжнародних організацій. Така взаємодія не лише підвищує якість розслідування воєнних злочинів, а й створює підґрунтя для ефективного притягнення винних осіб до відповідальності на національному та міжнародному рівнях, що є важливим елементом відновлення справедливості та верховенства права в умовах збройного конфлікту і післявоєнного періоду[36][37][38].

[36] Eurojust. Joint Investigation Teams – Practical Guide. 2nd ed. The Hague : Eurojust, 2023. 88 p. URL : https://www.eurojust.europa.eu/publication/joint-investigation-teams-practical-guide.

[37] International Criminal Court, Office of the Prosecutor. Strategic Plan 2023–2025. The Hague : ICC, 2023. 40 p. URL : https://www.icc-cpi.int/sites/default/files/2023-07/2023-2025-Strategic-Plan.pdf.

[38] United Nations Office on Drugs and Crime (UNODC). Handbook on Complementarity: An Introduction to the Role of National Courts and the ICC in Prosecuting International Crimes. Vienna : United Nations, 2023. 132 p. URL : https://www.unodc.org/documents/justice-and-prison-reform/Handbook_on_Complementarity.pdf.

ВИСНОВКИ

У результаті проведеного дослідження сформовано цілісне теоретико-прикладне бачення детективної діяльності у сфері військової криміналістики як комплексного, багаторівневого та інтегративного виду професійної діяльності, спрямованого на ефективне документування, розслідування та доказування воєнних злочинів в умовах збройного конфлікту. Доведено, що сучасна модель детективної діяльності виходить за межі традиційного розуміння слідчої роботи та набуває стратегічного характеру, поєднуючи процесуальні, аналітичні, технологічні та міжнародно-кооперaційні компоненти.

Обґрунтовано, що воєнні злочини мають специфічну правову та криміналістичну природу, яка зумовлює особливості їх доказування. На відміну від загальнокримінальних правопорушень, у справах про воєнні злочини необхідно встановлювати контекст збройного конфлікту, зв'язок діяння з воєнними діями, а також відповідність поведінки суб'єкта ознакам міжнародного гуманітарного права. Це обумовлює підвищені вимоги до аналітичної роботи, систематизації доказів і відтворення повної картини події у її політичному, військовому та соціальному вимірі.

Встановлено, що система суб'єктів детективної діяльності у справах про воєнні злочини має складний інституційний характер. Вона охоплює національні органи досудового розслідування, прокурорів, спеціалізовані підрозділи, експертні установи, аналітичні центри, а також міжнародні інституції та партнерські структури. Ефективність такої діяльності залежить від належної координації між цими суб'єктами, розмежування компетенції та уніфікації стандартів доказування відповідно до міжнародних вимог.

Окрему увагу приділено проблематиці встановлення особи невідомого злочинця та документування командної відповідальності. Доведено, що в умовах ієрархічної військової організації ключового значення набуває реконструкція вертикалі управління, встановлення фактичного контролю командира над підлеглими, аналіз наказів, комунікацій і поведінкових моделей. Це потребує використання комплексних криміналістичних методів, включаючи криміналістичне моделювання, аналіз великих масивів даних та цифрових слідів тощо.

У роботі аргументовано, що аналітична детективна діяльність є системоутворюючим елементом сучасної військової криміналістики. Вона забезпечує інтеграцію розрізнених доказів, формування логічних зв'язків між окремими епізодами, виявлення закономірностей злочинної поведінки та ідентифікацію причетних осіб. Особливу роль у цьому процесі відіграють інформаційно-аналітичні технології, зокрема обробка великих масивів даних, геопросторовий аналіз, цифрова верифікація матеріалів та використання методів відкритої розвідки (OSINT).

Доведено, що цифрові докази стають одним із ключових джерел інформації у справах про воєнні злочини. Супутникові знімки, відеоматеріали, дані соціальних мереж, геолокаційні координати, електронні комунікації формують нову доказову реальність, яка потребує забезпечення автентичності, цілісності та допустимості таких матеріалів у судовому процесі. Водночас їх використання ставить питання щодо методологічної стандартизації, належного збереження та експертної оцінки.

Проаналізовано особливості здійснення детективної діяльності на тимчасово окупованих та деокупованих територіях. Встановлено, що такі умови створюють комплекс додаткових ризиків та процесуальних труднощів, пов'язаних із безпекою, обмеженим доступом до місць подій, руйнуванням матеріальних слідів і психологічним станом потерпілих. Це обумовлює необхідність застосування дистанційних форм документування, попередньої фіксації інформації та поетапного відновлення доказової бази.

Важливим стратегічним напрямом розвитку детективної діяльності визначено міжнародну співпрацю. Бо участь у спільних слідчих групах, обмін інформацією з іноземними партнерами, взаємодія з міжнародними судовими інституціями сприяють підвищенню ефективності розслідувань та забезпечують відповідність доказової бази міжнародним стандартам. Такий підхід формує передумови для притягнення винних осіб до відповідальності як у національних судах, так і на міжнародному рівні.

Узагальнюючи результати дослідження, можна стверджувати, що детективна діяльність у сфері військової криміналістики є самостійним комплексним напрямом професійної та наукової діяльності, який потребує подальшого теоретичного осмислення та методичного вдосконалення. Перспективи її розвитку пов'язані з удосконаленням нормативного регулювання, впровадженням сучасних цифрових технологій, підвищенням рівня професійної підготовки кадрів, а також із розширенням міжнародної кооперації. Запропонована концепція детективної діяльності створює методологічне підґрунтя для формування ефективної системи розслідування воєнних злочинів, здатної забезпечити належне документування, доказування та притягнення до відповідальності осіб, винних у порушенні норм міжнародного гуманітарного права в умовах сучасного збройного конфлікту.

АНОТАЦІЯ

У досліджені здійснено комплексне теоретико-прикладне дослідження детективної діяльності у сфері військової криміналістики в умовах сучасного збройного конфлікту. Актуальність теми зумовлена безпрецедентним зростанням кількості воєнних злочинів, ускладненням механізмів їх вчинення та необхідністю забезпечення ефективного документування і доказування відповідно до національних і міжнародних стандартів. У роботі обґрунтовано, що традиційні підходи до криміналістичного забезпечення досудового розслідування потребують концептуального оновлення з урахуванням транснаціонального характеру воєнних злочинів, специфіки командної структури військових формувань та активного використання цифрових технологій у сучасних бойових діях.

Проаналізовано сутність детективної діяльності як багатовимірної системи, що поєднує процесуальні, організаційні, аналітичні та інформаційно-технологічні компоненти. Визначено, що її зміст виходить за межі класичного розуміння слідчої діяльності та включає комплекс заходів із встановлення обставин події, ідентифікації осіб, причетних до вчинення злочину, документування командної відповідальності, а також інтеграції доказів із різнорідних джерел. Особливу увагу приділено встановленню індивідуальної

кримінальної відповідальності в умовах ієрархічної військової організації, що передбачає реконструкцію вертикалі управління, аналіз наказів, комунікацій та фактичного контролю над підлеглими.

Окремий блок дослідження присвячено аналітичній детективній діяльності та криміналістичному моделюванню як ключовим інструментам систематизації доказової інформації. Доведено, що використання цифрових доказів, геопросторового аналізу, великих масивів даних, матеріалів відкритих джерел (OSINT) і супутникових знімків формує нову доказову реальність, яка потребує належної методологічної стандартизації та забезпечення автентичності й допустимості інформації. Обґрунтовано, що цифровізація розслідувань істотно розширює можливості документування воєнних злочинів, водночас висуваючи підвищені вимоги до професійної підготовки суб'єктів детективної діяльності.

Проаналізовано особливості здійснення розслідувань на тимчасово окупованих і деокупованих територіях, де обмежений доступ до місць подій, руйнування матеріальних слідів та ризики для безпеки учасників кримінального провадження зумовлюють необхідність застосування дистанційних форм документування та поетапного відновлення доказової бази. Наголошено на стратегічному значенні міжнародної співпраці, участі у спільних слідчих групах та узгодженні процедур доказування з міжнародними стандартами, що забезпечує перспективу притягнення винних осіб до відповідальності як на національному, так і на міжнародному рівнях.

У результаті дослідження сформульовано концептуальну модель детективної діяльності у військовій криміналістиці як інтегративної системи, здатної забезпечити ефективне розслідування та доказування воєнних злочинів в умовах сучасних викликів. Отримані висновки можуть бути використані для вдосконалення теоретичних засад криміналістики, розвитку методик розслідування воєнних злочинів та підвищення практичної ефективності діяльності правоохоронних органів.

Ключові слова: OSINT, військова криміналістика, воєнні злочини, детективна діяльність, доказування, командна відповідальність, криміналістичне моделювання, міжнародне гуманітарне право, міжнародна кримінальна юстиція. міжнародна співпраця, спільні слідчі групи, цифрові докази.

Література

1. Ambos K. Treatise on International Criminal Law. Volume III: International Criminal Procedure. 2nd ed. Oxford : Oxford University Press, 2024. 912 p. DOI: https://doi.org/10.1093/law/9780192844262.001.0001.

2. Bantekas I., Nash S. International Criminal Law. London ; New York : Routledge, 2022. 384 p.

3. Cryer R., Friman H., Robinson D., Wilmshurst E. An Introduction to International Criminal Law and Procedure. 4th ed. Cambridge : Cambridge University Press, 2019. 536 p. DOI: https://doi.org/10.1017/9781108689279.

4. Eurojust. Core International Crimes Casework Report 2023. The Hague : Eurojust, 2023. 52 p. URL : https://www.eurojust.europa.eu/publication/core-international-crimes-casework-report-2023.

5. Eurojust. Joint Investigation Teams – Practical Guide. 2nd ed. The Hague : Eurojust, 2023. 88 p. URL : https://www.eurojust.europa.eu/publication/joint-investigation-teams-practical-guide.

6. European Union Agency for Criminal Justice Cooperation (Eurojust). Guidelines for Prosecuting Core International Crimes. The Hague : Eurojust, 2023. 78 p. URL : https://www.eurojust.europa.eu/publication/guidelines-prosecuting-core-international-crimes.

7. Freeman L. Digital Evidence and War Crimes Prosecutions: The Impact of New Technologies on International Criminal Investigations. Cambridge : Cambridge University Press, 2020. 350 p.

8. International Criminal Court, Office of the Prosecutor. Strategic Plan 2023–2025. The Hague : ICC, 2023. 40 p. URL : https://www.icc-cpi.int/sites/default/files/2023-07/2023-2025-Strategic-Plan.pdf.

9. International Criminal Court. Policy on Case Selection and Prioritisation. The Hague : International Criminal Court, 2023. 28 p. URL : https://www.icc-cpi.int/sites/default/files/2023-02/2023-Policy-on-Case-Selection-and-Prioritisation.pdf.

10. International Criminal Court. Policy on Case Selection and Prioritisation. The Hague : Office of the Prosecutor, ICC, 2023. 28 p. URL : https://www.icc-cpi.int/sites/default/files/2023-02/2023-Policy-on-Case-Selection-and-Prioritisation.pdf.

11. International Criminal Court. Prosecutor v. Jean-Pierre Bemba Gombo. Judgment pursuant to Article 74 of the Statute. ICC-01/05-01/08-3343. 21 March 2016. URL : https://www.icc-cpi.int/court-record/icc-01/05-01/08-3343.

12. Mettraux G. The Law of Command Responsibility. Oxford : Oxford University Press, 2009. 522 p.

13. Schmitt M. N. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge : Cambridge University Press, 2017. xli, 598 p. DOI: https://doi.org/10.1017/9781316822524.

14. Sluiter G., Harnisch C., Buisman C., Zahar A. International Criminal Procedure: Principles and Rules. Oxford : Oxford University Press, 2013. 1176 p. DOI: https://doi.org/10.1093/law/9780199658022.001.0001.

15. United Nations Independent International Commission of Inquiry on Ukraine. Report of the Independent International Commission of Inquiry on Ukraine. Geneva : United Nations, 2023. URL : https://www.ohchr.org/en/hr-bodies/hrc/iicihr-ukraine.

16. United Nations Office on Drugs and Crime (UNODC). Handbook on Complementarity: An Introduction to the Role of National Courts and the ICC in Prosecuting International Crimes. Vienna : United Nations, 2023. 132 p. URL : https://www.unodc.org/documents/justice-and-prison-reform/Handbook_on_Complementarity.pdf.

17. United Nations Office on Drugs and Crime (UNODC). Manual on Mutual Legal Assistance and Extradition. Vienna : United Nations Office on Drugs and Crime, 2018. 456 p. URL : https://www.unodc.org/documents/organized-crime/MLA_Manual_E.pdf.

18. United Nations. Berkeley Protocol on Digital Open Source Investigations. New York ; Geneva : United Nations, 2022. 132 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

19. United Nations. Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Istanbul Protocol). 2022 revised edition. New York : United Nations, 2022. 224 p. URL : https://www.ohchr.org/en/publications/policy-and-methodological-publications/istanbul-protocol.

20. Werle G., Jeßberger F. Principles of International Criminal Law. 4th ed. Oxford : Oxford University Press, 2023. 711 p.

21. Велічко О. О. Участь прокурора в доказуванні воєнних злочинів: стан наукових досліджень. *Аналітично-порівняльне правознавство.* 2025. Т. 5. № 3. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.19.

22. Єфіменко Т. С. Особливості доказування у кримінальних провадженнях щодо воєнних злочинів. *Вісник Кримінологічної асоціації України.* 2024. № 3. DOI: https://doi.org/10.32631/vca.2024.3.25.

23. Кудінов С. С., Шехавцов Р. М. Особливості організації розслідування воєнних злочинів в Україні в умовах воєнного стану. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. Т. 4. № 91. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.46.

24. Погорецький М. А. Документування і доказування міжнародних злочинів в Україні: процесуально-криміналістичні та цифрові стандарти прийнятності доказів для Міжнародного кримінального суду та спеціального військового трибуналу. *Аналітично-порівняльне правознавство.* 2025. Т. 3. № 6. С. 94–114. DOI: https://doi.org/10.24144/2788-6018.2025.06.3.94.

25. Погоріла С. І. Використання OSINT-технологій у розслідуванні воєнних злочинів: сучасний стан і перспективи. *Актуальні проблеми сучасної науки в дослідженнях молодих учених.* Вінниця : ХНУВС, 2025. С. 346–348. dspace.univd.edu.ua.

26. Римський статут Міжнародного кримінального суду від 17 липня 1998 р. *Рада. Верховна Рада України. Законодавство України.* URL : https://zakon.rada.gov.ua/laws/show/995_588#Text.

27. Тимошко В. В. Використання спеціальних знань під час документування та розслідування воєнних злочинів. *Вісник кримінологічної асоціації України.* 2026. № 31(1). С. 307–314. DOI: https://doi.org/10.24144/vca.2026.31.1.307.

28. Чернецька О. В. Міжнародне співробітництво під час розслідування воєнних кримінальних правопорушень. Ірпінський юридичний часопис. 2025. № 2(19). С. 266–273. DOI: https://doi.org/10.33244/2617-4154-2(19)-2025-266-273.

Information about the author:
Kaliuga Karina Viktorivna,
Doctor of Law, Professor,
Action Head of the Department of Criminal Law, Process and Criminalistics
Institute of Economics and Law of the
Classic Private University,
70 b, Universytetska st., Zaporizhzhia, 69002, Ukraine
https://orcid.org/0000-0002-9941-9690

DOI https://doi.org/10.30525/978-9934-26-686-7-8

CRIMINAL PROCEDURAL AND FORENSIC ASPECTS OF PROVING HATE SPEECH IN THE DIGITAL ENVIRONMENT

Koval A. A., Kazarian E. H.

INTRODUCTION

Countering hate speech on the Internet, social media platforms, and within the public sphere constitutes one of the central challenges facing contemporary democratic societies and represents an important dimension of the implementation of the 2030 Agenda for Sustainable Development. Hate speech undermines the fundamental values of the European Union (EU) – respect for human dignity, equality, freedom, democracy, and the rule of law – and poses a serious threat to human rights, social cohesion, and public security. For Ukraine, which is confronting full-scale armed aggression while simultaneously pursuing a strategic course toward European integration, the issue of hate speech has acquired particular urgency. The escalation of social tensions, the systematic dissemination of disinformation, and the active exploitation of digital platforms as instruments of information warfare contribute to the normalization of hatred and discrimination, thereby directly endangering human rights, societal resilience, and democratic stability.

Hate speech should be regarded not merely as a socio-communicative phenomenon but, above all, as a human rights concern requiring clear and effective legal mechanisms of response. In this regard, European standards developed within the framework of EU law and the Council of Europe play a pivotal role, including the case law of the European Court of Human Rights, recommendations of the Committee of Ministers of the Council of Europe, the work of the European Commission against Racism and Intolerance, and the EU Code of Conduct on Countering Illegal Hate Speech Online.

According to data from the Office of the Prosecutor General of Ukraine, the number of criminal offences recorded under Article 161 of the Criminal Code of Ukraine between 2019 and 2025 has remained consistently high, ranging from 65 to 123 cases annually [1]. The overall trend indicates the persistent and systemic nature of the problem, particularly given the significant latency of such offences.

Accordingly, the detection and investigation of hate speech in the digital environment, especially on social media platforms, remains an issue of exceptional relevance. It is directly linked to the protection of human rights, the safeguarding of information security, the preservation of social harmony, and the effective functioning of democratic institutions in the face of emerging global challenges.

[1] Офіс Генерального прокурора. Офіційний сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

1. Theoretical and Legal Foundations for Countering Hate Speech

In pursuing its European integration trajectory, Ukraine has undertaken commitments to comply with international standards on equality and non-discrimination, including the Convention for the Protection of Human Rights and Fundamental Freedoms [2], the Council of Europe Framework Convention for the Protection of National Minorities, Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech[3], and Recommendation No. R (97) 20 on "hate speech"[4].

Despite these commitments, the use of hateful rhetoric and incitement to hostility continues to proliferate. According to data from the National Police of Ukraine and civil society monitoring organizations, more than 370 instances of public dissemination of hate speech on social media were recorded in 2024 alone. Approximately 70% of these cases involved discrimination on the grounds of nationality, religion, or sexual orientation [5].

Hate speech encompasses calls for discrimination, the promotion of the superiority of one group over another, dehumanization, and the dissemination of hostile or degrading imagery [6]. Its regulation inevitably requires a careful delineation between the constitutionally protected right to freedom of expression and the obligation to safeguard the rights and dignity of vulnerable groups. At the same time, it is worth emphasizing that in everyday communication a significant part of society does not realize that it uses elements of hate speech with regard to certain groups, considering such expressions socially acceptable (for example, "Asians," "Caucasians," etc.)[7].

Criminal liability for hate speech-related offences in Ukraine is governed, inter alia, by Article 161 of the Criminal Code – violation of citizens' equality, Article 300 – distribution of works promoting violence and cruelty, Articles 109 and 110 – public calls for violent change of government and encroachment upon territorial integrity, Article 436 – propaganda of war (in cases where hate speech takes the form of advocating armed aggression or inciting armed conflict), and Article 436-1 – production and dissemination of communist and National Socialist (Nazi) symbols

[2] Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 4 https://zakon.rada.gov.ua/laws/show/995004#Text.

[3] Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech. *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: https://search.coe.int/cm?i=0900001680a67955.

[4] Рекомендація № R (97) 20 Комітету Міністрів державам-членам щодо «мови ненависті». *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech" – Freedom of Expression.

[5] Національна поліція України. Офіційний сайт. URL: https://npu.gov.ua/.

[6] Коваль А. А. Толерантність онлайн: проблеми дотримання прав людини в соціальних мережах та правові шляхи їх вирішення. *Національні інтереси України*. № 5 (10). 2025. С. 616. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-609-619.

[7] Казарян Е. Г. Поняття та особливості мови ворожнечі. *Х Юридичні могилянські читання – 2024 :* матеріали Х всеукраїнської наук.-практ. конф. (м. Миколаїв, 28 квіт. 2024 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2024. С. 23. URL: https://chmnu.edu.ua/wp-content/uploads/Mogilyanski_chitannya_-_2024.pdf.

and propaganda of totalitarian regimes (applicable where hate speech is associated with the glorification of such regimes or the promotion of their ideologies) [8].

Preventing and countering hate speech and incitement to hatred on the Internet, particularly on social media platforms, is inherently complex and multidimensional. A central component of this process is evidentiary activity in criminal proceedings of this category, aimed at ensuring the criminal accountability of perpetrators.

The digital nature of offences related to incitement to hatred and discrimination on social media entails a number of specific features.

First, particular attention must be paid to the detection and preservation of digital traces containing information about the dissemination or incitement of hatred. In addition to complaints submitted by victims, law enforcement authorities conduct proactive monitoring of open sources through specialized cybersecurity units across platforms such as Facebook, X (Twitter), Telegram, TikTok, YouTube, and Instagram. Since the servers of social media platforms are often located outside Ukraine, timely access to relevant data may be complicated. Accordingly, it is essential to employ international legal assistance mechanisms (MLAT requests, Interpol channels) and cooperation frameworks with digital platforms (for example, Facebook Transparency Center).

Currently, both European states and Ukraine utilize specialized digital forensic tools to detect and analyze hate speech in social media. These include data extraction and forensic analysis software such as FTK (Forensic Toolkit), EnCase, and X-Ways Forensics, which are applied to examine storage devices and recover deleted files. Tools such as Cellebrite and Oxygen Forensics are widely used in the examination of mobile devices, enabling the analysis of text messages, call records, and geolocation data.

Network traffic analysis is conducted using Wireshark, while Maltego enables the collection of OSINT data and the mapping of relationships between individuals. Big data analytics technologies, such as Splunk and the ELK Stack, are applied to process large volumes of information and identify behavioral patterns among users. Data decryption tools, including Passware Kit and Elcomsoft, facilitate the recovery of encrypted files and electronic communications[9].

According to international practice, key digital forensic instruments used in the analysis of social media include the following:

1. Pipl – a service that aggregates data from online archives based on a single variable (such as an email address or phone number) and provides access to additional relevant personal information [10].

---

[8] Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[9] Казарян Е. Г. Роль засобів цифрової криміналістики у розпізнаванні мови ворожнечі у соціальних мережах. *XI Юридичні могилянські читання – 2025* : матеріали XI всеукраїнської наук.-практ. конф. (м. Миколаїв, 24 квіт. 2025 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2025. С. 60–61. URL: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2794/1/XI%20Юридичні%20Могилянські%20читання.pdf.

[10] Ziwen T., Channing Z. China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy.* 2021. Vol. 5 (1). Pp. 7–25. DOI: https://doi.org/10.69554/NATU8989.

2. WebPreserver – an automated web and social media archiving tool capable of rapidly collecting online content, expanding hidden replies and comments, and preserving social media profiles from multiple platforms [11].

3. Makeawebsitehub – a resource that regularly updates listings of emerging social interaction applications, which may assist investigators in expanding web-based inquiries and identifying lesser-known platforms potentially containing relevant information [12].

4. TinEye – a reverse image search tool that enables identification of original images and detection of other websites where the same image has been used, thereby assisting in tracing the source of visual content shared on social media[13].

5. TweetBeaver – a tool designed to extract substantial volumes of data from public Twitter (X) accounts and to analyze connections between accounts[14].

Empirical research conducted by foreign scholars indicates that the BiLSTM (Bidirectional Long Short-Term Memory) model demonstrates high accuracy in detecting hate speech. Owing to its enhanced sensitivity to contextual and semantic features, as well as sequential patterns in textual data such as tweets, BiLSTM proves particularly effective in identifying the complex and nuanced manifestations of hate speech[15].

Upon detecting publications, comments, videos, or images that may contain elements of hate speech, the content must be properly preserved by creating screenshots, screen recordings, and saving relevant metadata (URL address, date and time of publication, account identifiers, IP address, hashtags, etc.).

Within the framework of contemporary approaches to criminal investigations, digital forensic tools are acquiring increasing significance in both international and national practice. Their application facilitates the detection, preservation, and substantiation of criminal conduct, thereby contributing to the effective implementation of the principle of inevitability of punishment. Scholarly literature emphasizes the importance of an integrated use of the following instruments:

– keyword- and hashtag-based search mechanisms, with lists developed in accordance with thematic or regional focus;

---

[11] Thouvenin F., Hettich P., Burkert H., Gasser U. 4 web archives. In: Remembering and Forgetting in the Digital Age. *Law, Governance and Technology Series.* 2018. Vol. 38. Springer, Cham. Pp. 84–101. DOI: https://doi.org/10.1007/978-3-319-90230-2_6.

[12] Spencer J. 101 social networking sites you need to know about in 2022. 2021. URL: https://makeawebsitehub.com/social-media-sites/.

[13] Kondal M., Singh, V. Comparative analysis of tineye and google reverse image search engines. *International Journal of Innovative Science and Research Technology.* 2022. Vol. 7 (1). Pp. 205–207. DOI: https://doi.org/10.5281/zenodo.6378256.

[14] Lyndon R., Tse V., Moore L., May-Hobbs M. Disinformation in Brazil: The 2019 Amazon fires on social media. In: Mair M., Meckin R., Elliot M. (Eds) *Investigative Methods: An NCRM Innovation Collection.* Southampton: National Centre for Research Methods. 2022. Pp. 44–53. DOI: https://doi.org/10.5258/NCRM/NCRM.00004547.

[15] Toktarova A., Syrlybay D., Myrzakhmetova B., Anuarbekova G., Rakhimbayeva G., Zhylanbaeva B., Suieuova N., Kerimbekov M. Hate Speech Detection in Social Networks using Machine Learning and Deep Learning Methods. *International Journal of Advanced Computer Science and Applications.* 2023. Vol. 14 (5). P. 396. DOI: https://doi.org/10.14569/IJACSA.2023.0140542.

– Big Data technologies for identifying patterns and visualizing information flows;

– analysis of geolocation data, as well as photo and video materials obtained from open sources and digital platforms;

– application of image and video processing software to detect falsifications or confirm authenticity;

– examination of data extracted from electronic devices, including stored files, messages, and call records;

– identification of users and objects through facial recognition systems combined with database cross-referencing.

Although technologically sophisticated, these instruments substantially expand the possibilities of digital evidentiary practice, including in criminal proceedings related to hate speech offences [16].

Among the current directions of digital forensic research, the following may also be distinguished:

– analysis of data stored in cloud environments, including the identification, extraction, and authentication of information located on remote servers;

– examination of mobile devices, primarily smartphones, aimed at establishing data structure, communication history, deleted objects, and other relevant artifacts;

– analysis of information exchange applications (messengers, social networks, encryption software) used on mobile devices and computers;

– investigation of Internet of Things (IoT) devices – network-connected "smart" devices such as surveillance cameras, trackers, and sensors;

– network forensics, involving the analysis of traffic structure, access logs, IP addresses, and other digital traces within network environments;

– examination of modern interactive devices and virtual assistants (including Amazon Alexa, Google Assistant, Siri) capable of storing voice command records and user activity logs;

– analysis of non-standard data sources not directly related to smartphones, such as local and online databases, instant messaging systems (e.g., AOL IM), operational memory (including volatile memory), segments of the Darknet, anti-forensic tools, deleted or fragmented files, flash drives, cryptocurrencies, and related artifacts;

– digital behavioral analysis of individuals or groups, enabling reconstruction of activity patterns, interactions, social connections, and communication models;

– digital forensic intelligence, including OSINT (open-source intelligence), used to detect threats, verify facts, and identify offenders within the open information environment[17].

Taken together, these areas demonstrate the integrated nature of digital forensics as a field combining legal, technical, linguistic, and social analytical approaches necessary for the effective investigation of crimes committed in the digital environment, including those related to hate speech.

---

[16] Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika:* XVIII. 2022. Т. 18. С. 32.

[17] Reedy P. Interpol review of digitalevidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520. DOI: https://doi.org/10.1016/j.fsisyn.2020.01.015.

Secondly, a distinct stage of proof involves the technical identification of the perpetrator and the establishment of a hate motive. Given the possibility of using anonymous accounts or VPN services, investigators must obtain data from service providers (including IP addresses and connection timestamps), as well as establish a link between a specific account and an identified individual through log files, mobile devices, email accounts, and other digital traces. It is equally essential to ensure the proper preservation of digital evidence: screenshots must be duly documented and certified, with accurate recording of the URL, date, and time of capture.

Particular complexity arises in establishing and proving the motive of hatred, which constitutes a mandatory element of the corpus delicti in relevant criminal offences. It is not sufficient merely to document the dissemination of offensive or inciting statements; it must also be demonstrated that the act was committed specifically out of hatred based on race, nationality, gender, language, religion, sexual orientation, or other protected characteristics. This requires thorough contextual analysis of publications, assessment of the frequency and direction of hostile expressions, and examination of the individual's profile, including preferences, subscriptions, and prior statements.

For criminal liability to arise under the relevant provisions of the Criminal Code of Ukraine, proof of a hate motive is indispensable. This presents challenges for investigators due to the delicate boundary between constitutionally protected freedom of expression and unlawful manifestations of intolerance. In this regard, investigators and judges should take into account the jurisprudence of the European Court of Human Rights (ECtHR), which clearly distinguishes "protected freedom of expression" from "hate speech" that falls outside the scope of protection.

In its case law, the ECtHR has repeatedly emphasized that freedom of expression is not absolute and does not extend to statements that promote hatred, violence, or the dehumanization of individuals based on race, nationality, religion, or other identity characteristics. In particular, in Norwood v. the United Kingdom (2004), the Court declared the applicant's complaint inadmissible. In that case, Mark Anthony Norwood, a member of the British National Party, displayed a poster in his window depicting the burning Twin Towers accompanied by a slogan calling for the expulsion of Islam. The Court held that such conduct was incompatible with the values of the Convention and fell within the scope of Article 17 (prohibition of abuse of rights). The decision underscored that public statements amounting to a general attack on a religious group and inciting hatred are not protected under Article 10 of the Convention, even in the absence of explicit calls for violence. The Court concluded that Norwood's actions constituted an attack on the values of tolerance and non-discrimination [18].

The ECtHR has consistently held that even in the absence of explicit calls for physical violence, statements may qualify as hate speech if they create an atmosphere of intolerance or justify discrimination. In Vejdeland and Others v. Sweden (2012), the Court found no violation of Article 10 of the Convention. The applicants had

[18] Case of Norwood v. the United Kingdom (Applications no. 23131/03): Judgment European Court of Human Rights, 16 November 2004. URL: https://hudoc.echr.coe.int/eng?i=001-67632.

been convicted for distributing homophobic leaflets in students' lockers at a secondary school. Although they argued that their intention was to initiate debate about educational objectivity, the Court considered the content of the leaflets excessively offensive, as homosexuality was described as a "sexual deviation," alleged to have a "morally destructive effect" on society, and falsely associated with the spread of HIV/AIDS and the minimization of pedophilia. The Court emphasized that, even without direct incitement to violence, such allegations were serious and prejudicial. Particular weight was given to the method of distribution–directly targeting schoolchildren, a vulnerable audience, within a school to which the applicants had no lawful access. The sanctions imposed were deemed proportionate and necessary in a democratic society for the protection of the rights of others[19].

The ECtHR further underscores that the decisive factor in assessing alleged hate speech is context, including the socio-political climate, the role of the speaker, and the nature of the intended audience. Thus, in Perinçek v. Switzerland, on 15 October 2015, the ECtHR found a violation of Article 10 of the European Convention on Human Rights concerning freedom of expression.

The applicant, Doğu Perinçek, had publicly described the events of 1915 concerning the Armenians as an "international lie" and was subsequently convicted in Switzerland. While the Court acknowledged that the conviction constituted interference prescribed by law and pursuing a legitimate aim, it concluded that the restriction was not necessary in a democratic society. The statements concerned a matter of public interest, did not amount to incitement to hatred or violence, and were made in a context not characterized by heightened social tension. The penalty was considered disproportionate, and the Court noted the absence of an international obligation requiring Switzerland to criminalize such statements. On these grounds, the ECtHR established a violation of Article 10 of the Convention[20].

The ECtHR further recognizes that hate speech may manifest not only in verbal but also in symbolic forms, including posters, images, metaphors, and ironic constructions. In 2000, a book by Guillaume Faye entitled La Colonisation de l'Europe: Discours vrai sur l'immigration et l'Islam was published in France. The author asserted that Europe was gradually being "colonized" by Muslims, allegedly leading to an ethnic civil war, which he portrayed as a necessary "solution". The text employed expressions such as "ritual rapes" and "territorial partisans". French courts found the author and publishers guilty of incitement to hatred, discrimination, or violence on grounds of origin, race, or religion, imposing fines. The ECtHR held that there had been no violation of Article 10 (freedom of expression). It emphasized that numerous passages in the book portrayed entire communities in a negative light and were capable of arousing feelings of hostility and rejection among readers. The interference was prescribed by law and pursued the legitimate aim of protecting public order and the rights of others. Although the French Government relied on Article 17 of the Convention (prohibition of abuse of rights), the Court opted to assess the case under Article 10, concluding that while the content was inflammatory,

[19] Case of Vejdeland and others v. Sweden (Applications no. 1813/07): Judgment European Court of Human Rights, 9 February 2012. URL: https://hudoc.echr.coe.int/fre?i=001-109046.

[20] Case of Perinçek v. Switzerland (Applications no. 27510/08): Judgment European Court of Human Rights, 15 October 2015. URL: https://hudoc.echr.coe.int/eng?i=001-158235.

it did not reach the threshold required for the complete exclusion of Convention protection[21].

Thirdly, it must be emphasized that in criminal proceedings concerning incitement to hatred, discrimination, or calls to violence on social media, the application of specialized knowledge and expert examinations is pivotal for the correct legal qualification of the act and for substantiating suspicion or indictment.

2. Specific Features of Proving Hate Speech in the Digital Environment

Given the multi-layered nature of digital offences, cases involving hate speech frequently require complex forensic examinations encompassing several fields of expertise: linguistic (semantic and textual) analysis to identify elements of hate speech and incitement to violence; psychological assessment to evaluate the impact of content on the emotional and volitional sphere of recipients; authorship attribution to determine the authorship of disputed texts or images; and computer-technical examination to analyze metadata, IP addresses, timestamps, and sources of upload.

The quality of expert findings largely depends on the precision and correctness of the questions posed. Typical inquiries include: Does the text contain elements of incitement to racial, national, or religious hatred? Are the statements aimed at degrading the dignity of a specific social group? Do the expressions constitute a call for discrimination? Can the disputed post or comment be attributed to a particular individual? Improperly formulated questions may result in inconclusive opinions or necessitate repeated examinations.

For submission of materials for expert analysis, digital evidence must be properly secured and documented, including electronic storage devices, certified copies of web pages, and log extracts. The contextual framework of publication – date, time, platform, user reactions – must be recorded, and a technical specialist or forensic investigator should verify the authenticity and integrity of the data.

In examining linguistic content potentially containing unlawful elements, it is essential to rely on forensic linguistic expertise grounded in philological methodology, particularly linguistics. Specialized linguistic knowledge enables in-depth analysis of texts to determine the existence of speech-related delicts, their communicative orientation and function within a specific context, and, where necessary, the likely author – especially in cases involving anonymous or extremist communications.

Forensic linguistic examination constitutes a specialized scientific analysis of a text or other speech product conducted to answer legally relevant questions. Spoken or written words may, in certain circumstances, acquire legal significance and be treated as actions entailing legal consequences.

The object of such examination is the text as part of a broader discourse, within which communicative norms operating in a particular social or informational

[21] Case of Soulas and others v. France (Applications no. 15948/03): Judgment European Court of Human Rights, 10 October 2008. URL: https://globalfreedomofexpression.columbia.edu/cases/soulas-and-others-v-france/.

environment are assessed. Deviations from these norms may be interpreted as unlawful conduct[22].

Procedurally, forensic linguistic analysis encompasses both formal linguistic structures and semantic content. Its purpose is to identify lexical constructions, stylistic devices, and semantic units that may indicate unlawful expression under specific provisions of criminal or administrative law[23].

In the context of the growing prevalence of information-related offences, particularly in digital environments, linguistic expertise has evolved from an occasional evidentiary tool into a systemic component of forensic practice. This is especially relevant in criminal proceedings involving hate speech, incitement to violence, discrimination, or threats, where a proper legal assessment of textual evidence is impossible without specialized philological knowledge[24].

Within the framework of this research topic, it is appropriate to outline the specific features of expert analysis of linguistic content. Lexical analysis is aimed at identifying words and phrases that carry negative, degrading, derogatory, or aggressive semantics directed at an individual or a group defined by particular characteristics (national, ethnic, religious, social, etc.).

Attention is paid to direct insults and invective language, dehumanizing designations (such as comparisons with animals, objects, or diseases), as well as lexical units calling for exclusion, destruction, or restriction of rights. A statement such as “these [derogatory term] have no right to live among us” contains negatively marked vocabulary and constructs an exclusionary narrative aimed at removing a particular group from the social space.

Syntactic constructions. At the syntactic level, expert examination focuses on identifying forms of linguistic influence, particularly constructions of an imperative or exhortative nature that encourage action or contain explicit or implicit calls to aggression. Special consideration is given to the imperative mood of verbs, rhetorically manipulative questions, and conditional constructions that may justify violence. For example, a phrase such as “the city must be cleansed of them,” while not explicitly calling for violence, demonstrates an imperative orientation and may be interpreted as encouraging hostile action.

Stylistic devices. Linguistic expert examination also encompasses indirect forms of hostility that may be disguised as humor, irony, or artistic expression. The analysis focuses on sarcasm and irony that undermine dignity, hyperbole intensifying negative portrayals, as well as allusions and metaphors understandable to a particular audience. For instance, the statement “they are, as always, ‘extremely useful’ to

---

[22] Ажнюк Л. В. Лінгвістична експертиза як юридичний інструмент. *Магістеріум. Мовознавчі студії*. 2017. Вип. 66. С. 14.

[23] Коваль А. А. Петренко К. Д. Мова ворожнечі у цифровому просторі: особливості розслідування. *Вісник ЛННІ ім. Дідоренко*. 2025. Вип 3 (111). С. 97. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/80. DOI: https://doi.org/10.32782/2786-9156.111.3.

[24] Черняк А. М. Використання спеціальних знань при дослідженні текстів, із закликами до підриву конституційного ладу, порушення територіальної цілісності і недоторканості України. *Вісник кримінального судочинства*. 2023. № 3–4. С. 106. DOI: https://doi.org/10.17721/2413-5372.2022.3-4/101-111.

society," when used in a negative discussion context, may carry a sarcastic connotation and convey contempt without explicit insult.

Context of expression. Contextual analysis is crucial for the accurate interpretation of a statement, as the meaning of particular phrases may substantially change depending on their communicative environment. Experts take into account the author's preceding and subsequent publications, the general theme of the page or channel, audience reactions (comments, shares), and the broader socio-political or informational background. The same phrase may be neutral within an academic debate but acquire characteristics of hate speech if systematically employed in a series of publications targeting a specific social group [25].

Thus, linguistic examination of hate speech is inherently comprehensive in nature and is based on the combined application of lexical, syntactic, stylistic, and contextual analysis. It is precisely the cumulative assessment of these elements that enables a well-reasoned conclusion as to the presence or absence of hate speech indicators in specific digital content.

Moreover, in the context of the development of the information society, the examination of digital traces acquires particular significance in the investigation of hate speech-related offences, as such traces may indicate the presence of a specific motive – intolerance. Taking into account contemporary scientific approaches to determining the necessity of forensic examinations in cases of this category, special emphasis should be placed on the conduct of information and computer forensic examination (ICFE). This type of examination constitutes a subtype of computer-technical expertise within the broader category of engineering and technical forensic examinations. ICFE ensures the identification, preservation, analysis, and safeguarding of digital evidence that might otherwise remain inaccessible.

Through the application of modern technologies, it becomes possible to analyze data obtained from computer devices, mobile phones, cloud services, and social media platforms. This is particularly relevant given that offenders increasingly rely on digital technologies to plan, coordinate, and disseminate unlawful activities, thereby complicating the use of traditional investigative methods. In such circumstances, ICFE often represents the only effective means of obtaining reliable and admissible information [26].

ICFE is aimed at establishing circumstances related to the creation, processing, and storage of information on computer systems and digital media. Its primary task consists in the search, identification, reconstruction, and technical analysis of data generated either by a user or by software within a computer system [27]. For this purpose, experts are provided with various objects of examination, including personal computers, mobile

[25] Ажнюк Л., Ажнюк Б. Семантико-текстуальна лінгвістична експертиза усного й писемного мовлення: науково-методичні рекомендації. Київ, 2022. 47 с.

[26] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 47. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

[27] Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Istoryko-pravovyi chasopys.* 2017. № 1 (9). С. 141.

phones, tablets, data storage devices (hard drives, flash drives), and other electronic devices that may contain traces of criminal activity. The expert may determine whether the submitted object contains information in any form – files, audio, video, correspondence, social media posts–relevant to establishing indicators of a hate motive. Additionally, the expert may assess whether the examined device contains deleted files (graphic, textual, video, audio) and whether such data can be recovered[28].

ICFE is conducted to identify, preserve, and analyze data from digital media that may confirm the preparation or commission of a criminal offence. It plays a pivotal role in the investigation of crimes motivated by intolerance, as it enables the identification of a specific motive through the examination of informational content, electronic correspondence, and communications on social media platforms.

Within the framework of ICFE, specialists analyze computer equipment, mobile devices, and digital storage media in order to detect files containing extremist content indicators, as well as to examine correspondence, browser history, messengers (such as WhatsApp or Telegram), and other sources of digital evidence. The particular features of this examination stem from the need not only to establish the fact of unlawful conduct but also to identify a specific hate motive, uncover organized criminal networks, analyze propaganda materials, and overcome technical barriers associated with modern data encryption methods [29].

Where computer data stored in electronic devices have been created or modified as a result of actions undertaken by an offender or other persons during or in connection with the commission of a criminal offence, such data acquire evidentiary value. They may be seized and analyzed as electronic (digital) traces of the offence. In this context, electronic (digital) traces should be understood as computer information that has arisen or been modified through user interaction with computer systems in connection with criminal activity[30].

One of the principal objectives of ICFE is the identification of a motive of intolerance. In many instances, perpetrators leave digital traces reflecting deliberate actions carried out in the virtual environment aimed at forming, developing, or implementing an ideological, informational, or organizational foundation for committing a violent crime motivated by hostility toward a particular group defined by race, ethnic origin, religion, or worldview. Such traces may include video recordings, textual documents, social media correspondence, or messenger communications containing hostile statements or direct threats against specific social, ethnic, or religious groups. The analysis of such materials makes it possible

[28] Kazarian E. The use of special knowledge in the investigation of murders motivated by racial, national or religious intolerance. *Věda a perspektivy*. 2023. № 12 (31). P. 268–269. DOI: https://doi.org/10.52058/2695-1592-2023-12(31)-260-271.

[29] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 48. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

[30] Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2022. № 4 (100). С. 230. DOI: https://doi.org/10.33766/2524-0323.100.226-236.

to establish a link between the suspect and the ideological platform that inspired or motivated the commission of the offence.

Particular attention during ICFE is paid to digital evidence related to the consumption, dissemination, and interaction of a user with extremist content. Such content may be distributed in open or semi-closed environments, including social media platforms, specialized Telegram channels, Discord servers, forums, or platforms such as Reddit. This may involve viewing videos containing violent or propagandistic narratives, reading and storing texts, memes, manifestos, or similar materials. Typical digital traces of such activity include search history, browser cache, subscription lists, "likes," visited resources, and downloaded files. The identification of these traces enables investigators to reconstruct stages of an individual's ideological transformation – from initial exposure to radical content to the internalization and potential implementation of hostile attitudes through violent actions.

Electronic traces are of particular value in the investigation of serious crimes, including intentional homicide, even where such traces are not directly connected to the moment of the offence. Digital data may contribute to establishing the subjective element of the crime, including motives, purposes, psychological characteristics of the offender, and, in some cases, location data. Of special importance is the analysis of information capable of demonstrating whether the offence was committed on grounds of intolerance. Such information may be reflected in social media posts, correspondence, comments, or publications made before or after the offence[31].

Digital traces stored on remote information carriers and available in open Internet sources – for example, on social media platforms or forums containing extremist content – may be identified and preserved using standard computer tools, including personal computers and web browsers. Methods of documentation include saving web pages in *.html format, printing their contents, and screen recording during the inspection of online resources. Proper documentation is crucial for subsequent forensic analysis and legal assessment of the suspect's actions[32].

Another key direction of ICFE is the recovery of previously deleted information that may hold evidentiary value in criminal proceedings. Through the use of specialized forensic software, such as EnCase, experts are able to restore deleted messages, files, and browser history data[33].

---

[31] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 48. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

[32] Казарян Е. Електронні (віртуальні) сліди в розслідуванні умисних убивств із мотивів расової, національної чи релігійної нетерпимості. *Актуальні питання судової експертизи і криміналістики* : зб. мат-лів міжнар. наук.-практ. конф. з нагоди 100-річчя Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» (м. Харків, 10 лист. 2023 р.). Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2023. С. 169.

[33] Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 49. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

In addition, forensic specialists conduct comprehensive analyses of social media activity in order to identify a suspect's participation in groups promoting violence or intolerance, examine electronic communications, and establish individuals responsible for creating or disseminating hostile materials.

Given that content on social media platforms is frequently deleted, the timely appointment of a forensic examination is of critical importance. Investigators must ensure the immediate preservation of digital evidence and avoid any delay in transferring relevant materials to forensic experts.

In Ukraine, the aforementioned examinations are successfully conducted by a range of expert institutions, including forensic units of the Ministry of Internal Affairs, Research Institutes of Forensic Examinations under the Ministry of Justice, as well as duly certified private experts possessing the required qualifications and licenses. Effective cooperation between investigators and experts must be well-coordinated and carried out in strict compliance with procedural safeguards and confidentiality requirements.

It should also be noted that, in the context of martial law in Ukraine, there has been an observable increase in convictions for offences related to incitement to hatred and discrimination. In particular, between 2019 and 2024, a total of 45 convictions were delivered under Article 161 of the Criminal Code of Ukraine[34].

An analysis of judicial decisions in this category of cases demonstrates that investigative practice remains selective and uneven. A number of challenges arise in proving the constituent elements of such offences, including difficulties in establishing a motive of hatred or discrimination, which complicates the proper legal qualification of acts under Article 161 of the Criminal Code; inadequate documentation and preservation of digital evidence, potentially resulting in acquittals or case dismissals; and judicial difficulties in delineating the boundary between protected expression and statements that incur criminal liability. These issues underscore the relevance and practical significance of the present research and highlight the need for further scholarly development of the identified problems.

CONCLUSIONS

The conducted research made it possible to identify and specify the principal features of evidentiary processes in criminal proceedings concerning the use of hate speech in the digital environment. The proliferation of hate speech on the Internet, particularly on social media platforms, requires a comprehensive response from law enforcement authorities that combines digital forensic tools, forensic examinations, and effective legal mechanisms. Digital evidence serves as a key instrument for establishing the objective truth in such cases; at the same time, it is characterized by increased vulnerability to loss and alteration, as well as by the complexity of identifying its source. Particular importance attaches to the timely collection and preservation of electronic traces, ensuring their procedural admissibility, authenticity, and integrity, and compliance with standards for the preservation of digital information.

[34] Єдиний державний реєстр судових рішень. Офіційний сайт. URL: https://reyestr.court.gov.ua/.

The effective use of digital evidence in criminal proceedings related to hate speech necessitates further improvement of the regulatory framework, the development of unified methodological approaches to the collection and assessment of digital content, and the enhancement of interdisciplinary cooperation among investigators, prosecutors, judges, and experts. Establishing the motive of hatred as a mandatory element of the corpus delicti requires a comprehensive analysis of the content, the context of its dissemination, the behavioral characteristics of the individual, and their digital activity. It is also essential to take into account the case-law of the European Court of Human Rights concerning the assessment of contextual factors and the balance between freedom of expression and the prohibition of discrimination, thereby contributing to the consistency of judicial practice and the safeguarding of the principle of legal certainty.

Based on the findings of the study, it can be concluded that there is a need, first, to update (develop and refine) guidelines for investigators and experts working with digital evidence; second, to elaborate uniform approaches to the legal interpretation of hate speech; and third, to strengthen the specialization and professional training of participants in criminal proceedings in light of contemporary technological challenges. The implementation of these measures will enhance the effectiveness of investigations, ensure the proper substantiation of the motive of intolerance, and secure effective protection of human rights in the digital environment.

SUMMARY

The study examines the criminal procedural and forensic aspects of proving hate speech in the digital environment. The relevance of the topic is обусловед by the growing prevalence of discriminatory and xenophobic expressions on the Internet, particularly on social media platforms, as well as by the complexity of their proper legal qualification and evidentiary substantiation. The specific features of the formation and documentation of digital evidence are analyzed, including its vulnerability to loss or alteration, as well as the challenges associated with establishing authorship and the motive of intolerance. Particular attention is devoted to the role of forensic examinations and the application of digital forensic tools in criminal proceedings of this category. The importance of contextual assessment of statements and the necessity of maintaining a balance between freedom of expression and the prohibition of discrimination are also highlighted.

Based on the findings, the study substantiates the need to improve the regulatory framework, to develop unified methodological approaches to the documentation and evaluation of digital content, and to enhance interdisciplinary cooperation among participants in criminal proceedings. Directions are proposed for updating guidelines for investigators and experts and for elaborating uniform approaches to the legal interpretation of hate speech in accordance with international standards

References

1. Case of Norwood v. the United Kingdom (Applications no. 23131/03): Judgment European Court of Human Rights, 16 November 2004. URL: https://hudoc.echr.coe.int/eng?i=001-67632.

2. Case of Perinçek v. Switzerland (Applications no. 27510/08): Judgment European Court of Human Rights, 15 October 2015. URL: https://hudoc.echr.coe.int/eng?i=001-158235.

3. Case of Soulas and others v. France (Applications no. 15948/03): Judgment European Court of Human Rights, 10 October 2008. URL: https://globalfreedomofexpression.columbia.edu/cases/soulas-and-others-v-france/.

4. Case of Vejdeland and others v. Sweden (Applications no. 1813/07): Judgment European Court of Human Rights, 9 February 2012. URL: https://hudoc.echr.coe.int/fre?i=001-109046.

5. Kazarian E. Peculiarities of information and computer forensics in the investigation of intentional homicides motivated by racial, national, or religious intolerance. *Scientific and Practical Journal "Materials of Scientific Conferences of the Petro Mohyla Black Sea National University"*. 2025. № 1. P. 47. URL: https://www.mspc.mk.ua/index.php/journal/article/view/196. DOI: https://doi.org/10.34132/mspc2025.01.11.10.

6. Kazarian E. The use of special knowledge in the investigation of mu rders motivated by racial, national or religious intolerance. *Věda a perspektivy*. 2023. № 12 (31). P. 268–269. DOI: https://doi.org/10.52058/2695-1592-2023-12(31)-260-271.

7. Kondal M., Singh, V. Comparative analysis of tineye and google reverse image search engines. *International Journal of Innovative Science and Research Technology.* 2022. Vol. 7 (1). Pp. 205–207. DOI: https://doi.org/10.5281/zenodo.6378256.

8. Lyndon R., Tse V., Moore L., May-Hobbs M. Disinformation in Brazil: The 2019 Amazon fires on social media. In: Mair M., Meckin R., Elliot M. (Eds) *Investigative Methods: An NCRM Innovation Collection.* Southampton: National Centre for Research Methods. 2022. Pp. 44–53. DOI: https://doi.org/10.5258/NCRM/NCRM.00004547.

9. Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech. *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: https://search.coe.int/cm?i=0900001680a67955.

10. Reedy P. Interpol review of digitalevidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520. DOI: https://doi.org/10.1016/j.fsisyn.2020.01.015.

11. Spencer J. 101 social networking sites you need to know about in 2022. 2021. URL: https://makeawebsitehub.com/social-media-sites/.

12. Thouvenin F., Hettich P., Burkert H., Gasser U. 4 web archives. In: Remembering and Forgetting in the Digital Age. *Law, Governance and Technology Series.* 2018. Vol. 38. Springer, Cham. Pp. 84–101. DOI: https://doi.org/10.1007/978-3-319-90230-2_6.

13. Toktarova A., Syrlybay D., Myrzakhmetova B., Anuarbekova G., Rakhimbayeva G., Zhylanbaeva B., Suieuova N., Kerimbekov M. Hate Speech Detection in Social Networks using Machine Learning and Deep Learning Methods. *International Journal of Advanced Computer Science and Applications.* 2023. Vol. 14 (5). P. 396. DOI: https://doi.org/10.14569/IJACSA.2023.0140542.

14. Ziwen T., Channing Z. China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy.* 2021. Vol. 5 (1). Pp. 7–25. DOI: https://doi.org/10.69554/NATU8989.

15. Ажнюк Л. В. Лінгвістична експертиза як юридичний інструмент. *Магістеріум. Мовознавчі студії*. 2017. Вип. 66. С. 14.

16. Ажнюк Л., Ажнюк Б. Семантико-текстуальна лінгвістична експертиза усного й писемного мовлення: науково-методичні рекомендації. Київ, 2022. 47 с.

17. Єдиний державний реєстр судових рішень. Офіційний сайт. URL: https://reyestr.court.gov.ua/.

18. Казарян Е. Г. Поняття та особливості мови ворожнечі. *Х Юридичні могилянські читання – 2024 :* матеріали Х всеукраїнської наук.-практ. конф. (м. Миколаїв, 28 квіт. 2024 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2024. С. 23. URL: https://chmnu.edu.ua/wp-content/uploads/Mogilyanski_chitannya_-_2024.pdf.

19. Казарян Е. Г. Роль засобів цифрової криміналістики у розпізнаванні мови ворожнечі у соціальних мережах. *XI Юридичні могилянські читання – 2025* : матеріали XI всеукраїнської наук.-практ. конф. (м. Миколаїв, 24 квіт. 2025 р.). Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2025. С. 60–61. URL: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2794/1/XI%20Юридичні%20Могилянські%20читання.pdf.

20. Казарян Е. Електронні (віртуальні) сліди в розслідуванні умисних убивств із мотивів расової, національної чи релігійної нетерпимості. *Актуальні питання судової експертизи і криміналістики* : зб. мат-лів міжнар. наук.-практ. конф. з нагоди 100-річчя Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» (м. Харків, 10 лист. 2023 р.). Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2023. С. 169.

21. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Istoryko-pravovyi chasopys.* 2017. № 1 (9). С. 141.

22. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2022. № 4 (100). С. 230. DOI: https://doi.org/10.33766/2524-0323.100.226-236.

23. Коваль А. А. Петренко К. Д. Мова ворожнечі у цифровому просторі: особливості розслідування. *Вісник ЛНННІ ім. Дідоренко*. 2025. Вип 3 (111). С. 97. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/80. DOI: https://doi.org/10.32782/2786-9156.111.3.

24. Коваль А. А. Толерантність онлайн: проблеми дотримання прав людини в соціальних мережах та правові шляхи їх вирішення. *Національні інтереси України*. №5 (10). 2025. С. 616. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-609-619.

25. Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 4 https://zakon.rada.gov.ua/laws/show/995004#Text.

26. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

27. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika:* XVIII. 2022. Т. 18. С. 32.

28. Національна поліція України. Офіційний сайт. URL: https://npu.gov.ua/.

29. Офіс Генерального прокурора. Офіційний сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

30. Рекомендація № R (97) 20 Комітету Міністрів державам-членам щодо «мови ненависті». *Офіційний вебпортал Комітету Міністрів Ради Європи.* URL: Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech" – Freedom of Expression.

31. Черняк А. М. Використання спеціальних знань при дослідженні текстів, із закликами до підриву конституційного ладу, порушення територіальної цілісності і недоторканості України. *Вісник кримінального судочинства*. 2023. № 3–4. С. 106. DOI: https://doi.org/10.17721/2413-5372.2022.3-4/101-111.

Information about the authors:

Koval Alla Anatoliivna,
Doctor of Law, Professor,
Head of the Department of Constitutional
and Administrative Law and Procedure
Petro Mohyla Black Sea National University
10, 68 Desantnykiv St., Mykolaiv, 54000, Ukraine

Kazarian Eluchka Hurhenivna,
Doctor of Philosophy in Law,
Senior Lecturer of the Department of Constitutional
and Administrative Law and Procedure
Petro Mohyla Black Sea National University
10, 68 Desantnykiv St., Mykolaiv, 54000, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-9

КРИМІНАЛІСТИЧНІ ЗАСОБИ ОТРИМАННЯ ЗНАЧУЩОЇ ІНФОРМАЦІЇ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У ЦИФРОВУ ЕПОХУ

Курман О. В.

ВСТУП

У сучасних умовах практично не існує сфер суспільного життя, у яких не застосовувалися б електронні засоби комунікації. Будь-яка діяльність, спрямована на збереження ефективності та конкурентоспроможності, об'єктивно потребує активного використання сучасних технічних комунікаторів, що забезпечують майже миттєве отримання, оброблення та передавання значних обсягів інформації.

Сфери державного управління, охорони здоров'я, науки, оборони, правоохоронної діяльності, виробництва та зв'язку зазнали глибокої цифрової трансформації, результатом якої стало широке впровадження електронного документообігу, цифрових методів обробки, зберігання й використання інформації. В Україні реєстри та бази даних органів державної влади й управління вже переведені або перебувають у процесі переведення на електронні носії з розміщенням інформації у локальних мережах або з доступом до неї через глобальну мережу Інтернет. Паралельно з цим стрімко зростає рівень цифрової активності населення: сотні мільйонів користувачів у різних країнах світу мають власні вебресурси або персональні сторінки в соціальних мережах, що формує новий інформаційний простір і нові соціальні зв'язки.

У нашій країні запущено онлайн-сервіс державних послуг «Дія» і проєкти електронної державної реєстрації речових прав на нерухоме майно та їхніх обтяжень; для юридичних і фізичних осіб (підприємців і громадських формувань) – е-Бізнес; для актів цивільного стану – е-ДРАЦС; для цифрової трансформації вищої, фахової передвищої і професійної (професійно-технічної) освіти – е-Університет; для системи управління запасами лікарських засобів і медичних виробів – створення/модернізація Державного реєстру лікарських засобів і Державного реєстру медичних виробів, розвиток застосування електронних рецептів.

Загальновідоме прислів'я про те, що хто володіє інформацією, той володіє світом, характеризує роль інформації у сучасному суспільстві. На нинішньому етапі розвитку суспільства масштаби злочинних посягань на конфіденційні відомості різко зросли. Інформація про результати чужих прикладних і фундаментальних досліджень дає змогу заощадити власні сили й кошти та зосередити увагу на виробництві й маркетингу. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкуренції роблять викрадення чужих таємниць особливо прибутковою, а тому дуже

перспективною справою[1]. Все більше видів інформації у сучасному суспільстві зберігається в електронному вигляді. Такі обставини зумовили широке поширення портативних комп'ютерів, смартфонів, планшетів в усіх галузях діяльності людини. Практично всі сучасні електронні пристрої мають постійне чи періодичне підключення до електронних комунікаційних мереж передачі та отримання інформації.

Така зручність у збиранні, обробці та використанні інформації створює велику спокусу незаконного отримання конфіденційних відомостей про конкретну особу, об'єднання громадян, підприємства, установи з метою використання у подальшому в протиправних цілях[2].

Сьогодні з'являються нові, раніше невідомі способи вчинення злочинів у сфері використання електронно-обчислюваних машин, систем та комп'ютерних мереж і мереж електрозв'язку, де предметом посягання виступає різного роду інформація, що зумовлює необхідність розроблення ефективних методик виявлення й розслідування цих злочинних деліктів.

1. Штучний інтелект у дослідженні цифрових слідів: інноваційні перспективи та проблеми використання

Популярність мережі Інтернет та її суцільне проникнення у повсякденне життя суспільства зумовили формування принципово нового інформаційного середовища. У цьому середовищі практично будь-яка діяльність людини – від перегляду вебсторінок до активної взаємодії в соціальних мережах – супроводжується створенням і накопиченням цифрових слідів. Такі сліди містять інформацію, яка може бути повністю відкритою для необмеженого кола осіб, так і частково або повністю закритою у доступі.

Значну та перспективну роль на сучасному етапі відіграють методики, спрямовані на аналіз цифрового сліду користувачів. За їх допомогою спеціалісти можуть реконструювати послідовність дій злочинців навіть у випадках навмисного знищення доказів або використання засобів анонімізації. Застосовуються методи зворотного аналізу, що включають відновлення видаленої інформації, дослідження історії браузера, системних логів і мережевої активності. Це дає змогу встановлювати не лише автора забороненого контенту, а й осіб, причетних до його поширення або співучасті у цифрових злочинах.

На сучасному етапі розвитку криміналістичної науки відбувається переосмислення тактичних підходів до організації та проведення слідчих (розшукових) дій. Використання новітніх досягнень науки й техніки створює

[1] Курман О.В. Типізація способів учинення злочинних посягань на відомості, що становлять комерційну або банківську таємницю. *Теорія та практика судової експертизи і криміналістики*: збірник наукових праць. Вип. 10 / ред. кол.: М.Л. Цимбал, В.Ю. Шепітько, Л.М. Головченко та ін. Харків: Право, 2010. С. 62.

[2] Курман О.В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. 2017. № 4. С. 245. URL: http://pravoisuspilstvo.org.ua/archive/2017/4_2017/part_1/44.pdf

передумови для підвищення результативності роботи органів досудового розслідування та посилення рівня захисту прав і безпеки громадян[3].

З кожним роком зростають потреби правоохоронних органів в ефективних інструментах виявлення, вилучення, дослідження та використання в доказуванні цифрових доказів. У криміналістичній науці останніх десятиліть цифрова криміналістика є одним із найбільш актуальних напрямів розвитку[4]. Сучасна цифрова криміналістика розвивається в умовах стрімкого технологічного прогресу, що зумовлює радикальні зміни в підходах до розслідування правопорушень.

Сучасна злочинна діяльність дедалі частіше характеризується утворенням значних масивів цифрової інформації, зокрема лог-файлів, електронних повідомлень, графічних і відеоматеріалів, метаданих, а також відомостей, що зберігаються на мобільних та інших електронних пристроях. За наявності такого обсягу й різноманіття цифрових слідів використання традиційних аналітичних підходів не забезпечує належної оперативності та результативності й потребує значних ресурсних витрат. У цьому контексті застосування технологій штучного інтелекту для обробки та аналізу цифрових слідів постає як перспективний науково-практичний напрям, здатний суттєво вплинути на організацію досудового розслідування та процес доказування у кримінальному провадженні.

Водночас на сучасному етапі поняття «цифрові сліди» не відзначається єдністю підходів до його визначення та змістовного наповнення. У межах криміналістичної техніки триває наукова дискусія щодо сутності цифрових слідів, їх характерних ознак, а також можливих підстав для класифікації.

Так, І. Колеснікова наводить визначення цифрових слідів через сукупність їх характерних властивостей. Зокрема: 1) цифрові сліди – це інформація, що міститься на матеріальних цифрових пристроях; 2) для аналізу такої інформації необхідні спеціальні криміналістичні знання із застосуванням комп'ютерних технологій; 3) цифрові сліди як інформаційний ресурс містять відомості про вчинені кримінальні правопорушення. До основних властивостей цифрових слідів, за авторкою, належать: відсутність нерозривного зв'язку з матеріальним носієм; динамічність, тобто здатність до просторового переміщення; можливість їх миттєвого знищення, а також здатність створювати ідентичні копії без втрати змісту[5].

---

[3] Курман О. Правові та практичні аспекти використання поліграфа у кримінальному провадженні України. *Сучасний досвід використання поліграфа у сфері національної безпеки і оборони України в умовах воєнних загроз*: зб. матеріалів панел. дискусії: IX Харків. міжнар. юрид. форум, м. Харків, 26 верес. 2025 р. / [редкол.: А. Гетьман, В. Журавель, В. Шевчук та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики; Нац. акад. прав. наук України; Всеукр. асоц. поліграфологів [та ін.]. Харків: Право, 2025. С. 76. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20575

[4] Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283. URL: https://dspace.univd.edu.ua/items/b174d57a-bf4b-47f9-9211-aeb715b61844

[5] Колеснікова І. А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. № 10. С. 473. URL: http://lsej.org.ua/10_2023/114.pdf

Г. Авдєєва визначає цифрові сліди як матеріальні невидимі сліди, що містять криміналістично значущу інформацію (відомості, дані), зафіксовану в цифровій формі на матеріальних носіях, які можуть бути виявлені, зафіксовані та досліджені із застосуванням відповідних цифрових пристроїв[6].

Є. Демидова подає визначення цифрових слідів через перелік їх ознак, а саме: 1) наявність цифрової форми існування (відсутність традиційної матеріальної форми); 2) виникнення внаслідок взаємодії певного об'єкта з цифровими пристроями, технологіями або інформаційними мережами; 3) локалізація в цифровому просторі (сервері, комп'ютері, смартфоні тощо); 4) можливість їх виявлення та дослідження з використанням відповідного обладнання та/або спеціалізованого програмного забезпечення; 5) здатність до копіювання (виготовлення дублікатів) без втрати якості, у тому числі дистанційно; 6) можливість дистанційного модифікування або знищення[7].

Цифрова трансформація суспільних процесів і способів учинення кримінальних правопорушень супроводжується інтенсивним збільшенням кількості та різновидів цифрових слідів, що об'єктивно вимагає залучення сучасних інтелектуальних технологій, спроможних здійснювати аналіз значних за обсягом і різнорідних інформаційних масивів у стислих часових межах.

У сучасних реаліях в галузі криміналістичної техніки простежується тенденція активних пошуків щодо розроблення та впровадження інноваційних криміналістичних продуктів, спрямованих на оптимізацію розслідування злочинів та судового розгляду. Як зазначається, до таких інноваційних продуктів можна віднести нові розроблені або прилаштовані до потреб слідчої (судової) практики техніко-криміналістичні засоби, сучасні інформаційні технології, електронні бази знань, методи фіксації, аналізу та оцінки доказової інформації та ін[8].

У розв'язанні таких завдань саме ШІ може відіграти ключову роль. Проблематиці використання штучного інтелекту в судовій та правоохоронній діяльності приділяється значна увага з боку науковців-правознавців. Свої наукові праці цій тематиці присвятили такі дослідники, як Бєлова М. В., Бєлов Д. М., Рущак І. В[9]., Карчевський М. В.,

---

[6] Авдєєва Г. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики*. 2018. С. 91. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf

[7] Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. Вип. 85, ч. 4. С. 75. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/12-3.pdf

[8] Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю*: зб. наук. праць. Харків: Право, 2011. Вип. 21. С. 40.

[9] Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично порівняльне правознавство*. 2025. № 1. С. 818-824. URL: https://doi.org/10.24144/2788-6018.2025.01.136

Куковинець Д. О.[10], Негребецький В. В.[11], Плахотнік О. В[12]., Червеко К. О[13]. та інші. З огляду на стрімку динаміку розвитку штучного інтелекту, його активне впровадження у практику діяльності правоохоронних та експертних органів, а також пов'язані з цим виклики та проблеми, цей напрям наукових криміналістичних досліджень потребує постійного вивчення, оновлення та вдосконалення. В. Шевчук справедливо наголошує на необхідності активізації зусиль щодо застосування штучного інтелекту з метою розв'язання практичних завдань як у сфері правозастосування, так і в боротьбі зі злочинністю в умовах війни[14].

Технології штучного інтелекту можуть використовуватися для здійснення автоматизованого виявлення цифрових слідів у різноманітних інформаційних середовищах, зокрема на мобільних пристроях, персональних комп'ютерах, у хмарних сховищах, соціальних мережах і месенджерах. Застосування інтелектуальних алгоритмів пошуку та фільтрації забезпечує можливість визначення потенційно значущих файлів, електронних повідомлень, графічних матеріалів і журналів подій на підставі аналізу ключових слів, часових характеристик, геолокаційних відомостей та особливостей контексту їх використання. Цифрові сліди переважно характеризуються неструктурованістю та представлені у різних інформаційних форматах, зокрема у вигляді текстових документів, мультимедійних матеріалів і системних журналів. Використання алгоритмів машинного навчання й технологій обробки природної мови дає змогу системам штучного інтелекту здійснювати класифікацію таких даних за визначеними ознаками, встановлювати взаємозв'язки між окремими об'єктами (зокрема IP-адресами, обліковими записами та діями користувачів), а також формувати впорядковані інформаційні структури, придатні для подальшого аналітичного опрацювання.

Використання технологій штучного інтелекту, зокрема алгоритмів часової аналітики, створює можливості для реконструкції послідовності дій певної особи, виявлення нетипових або потенційно протиправних форм активності та відтворення причинно-наслідкового зв'язку між окремими подіями, такими як авторизація в системі, копіювання інформаційних ресурсів і подальші спроби

[10] Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 21-31. URL: http://pbz.nlu.edu.ua/issue/view/17882

[11] Негребецький В. В. Використання систем штучного інтелекту у боротьбі зі злочинністю: огляд та перспективи. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. № 1 (9). С. 66-70. URL: DOI: https://doi.org/10.32782/2709-9261-2024-1-9-13

[12] Плахотнік О. В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4. С. 45-57. URL: https://vkslaw.com.ua/index.php/journal/article/view/222

[13] Черевко К. О., Луценко І. Г. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 1. С. 124-133. URL: DOI: https://vca.univd.edu.ua/index.php/vca/article/view/43

[14] Shevchuk V. M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver, Canada). 2023. Pp. 198. URL: https://archive.interconf.center/index.php/2709-4685/issue/view/19-20.05.2023/165

приховування цифрових слідів. Зазначений підхід набуває особливої значущості під час розслідування кримінальних правопорушень у сфері інформаційних технологій, витоків конфіденційної інформації, а також фактів несанкціонованого доступу до інформаційних систем.

Використання технологій комп'ютерного зору в системах штучного інтелекту забезпечує можливість автоматизованого розпізнавання облич, реєстраційних номерів транспортних засобів, окремих об'єктів і моделей поведінки на фото- та відеоматеріалах, отриманих у ході досудового розслідування. Застосування таких інструментів сприяє встановленню місцезнаходження особи, аналізу її дій у певний проміжок часу, зіставленню зовнішніх ознак із відомостями з інших інформаційних джерел, а також виявленню ознак можливого втручання в цифрові відеодані, у тому числі шляхом детекції технологій deepfake.

Окрім цього, штучний інтелект може залучатися до аналізу значних обсягів текстової інформації, зокрема електронного листування, повідомлень у месенджерах і матеріалів, оприлюднених у соціальних мережах, з метою виокремлення ключових смислових тем, встановлення можливих намірів та ідентифікації осіб, причетних до злочинної діяльності. Застосування методів семантичного аналізу дає змогу оцінювати емоційне наповнення повідомлень, виявляти використання умовних або кодованих позначень, а також фіксувати приховані комунікативні загрози

Системи штучного інтелекту можуть бути інтегровані з наявними криміналістичними інформаційними ресурсами, зокрема дактилоскопічними та генотипічними обліками, відеоархівами, реєстрами викрадених транспортних засобів, зброї, мобільних пристроїв та іншими спеціалізованими базами даних, з метою здійснення автоматизованого порівняльного аналізу цифрових слідів із вже накопиченою інформацією. Застосування такого підходу забезпечує скорочення строків ідентифікації особи, сприяє встановленню серійності кримінальних правопорушень, а також створює підґрунтя для формування профілю правопорушника.

Під час використання штучного інтелекту у роботі з цифровими слідами виникає низка проблем і викликів, які можуть істотно вплинути на допустимість, достовірність та ефективність застосування таких технологій у кримінальному судочинстві.

Сучасні системи штучного інтелекту, зокрема побудовані на основі методів глибокого навчання, характеризуються високою результативністю та точністю під час оброблення значних масивів цифрових даних. Разом із тим однією з ключових проблем їх використання залишається недостатній рівень пояснень отриманих результатів, що набуває особливої ваги у контексті кримінального провадження. Обмежена прозорість функціонування алгоритмів унеможливлює належне обґрунтування причин, з яких система дійшла певного висновку або сформувала відповідне рішення, що, своєю чергою, ускладнює перевірку достовірності та обґрунтованості таких висновків і безпосередньо впливає на питання допустимості та належності доказів у судовому розгляді. Додатково відсутність чітко визначених критеріїв і процедур контролю створює ризики зловживань, у тому числі шляхом свідомого коригування параметрів алгоритмів з

метою отримання наперед заданого результату, що суперечить принципам змагальності, об'єктивності та справедливості кримінального процесу.

Незважаючи на значні технічні можливості, застосування систем штучного інтелекту супроводжується низкою обмежень, здатних позначатися на точності й надійності аналізу цифрових слідів у межах кримінального провадження. Одним із ключових ризиків є формування хибнопозитивних або хибнонегативних результатів, що може проявлятися, зокрема, у помилковому тлумаченні змісту текстових повідомлень, неточній ідентифікації облич чи інших цифрових об'єктів. Подібні похибки потенційно спотворюють висновки органів досудового розслідування та істотно впливають на подальшу оцінку доказів під час дослідження в суді.

Окремий блок проблем пов'язаний з обмеженою здатністю систем штучного інтелекту адекватно враховувати комунікативний і ситуаційний контекст повідомлень, особливо у випадках використання неструктурованої лексики, професійного сленгу, іронічних або двозначних висловлювань. За таких умов існує ймовірність суттєвого викривлення змісту аналізованої інформації, що, своєю чергою, підвищує ризик формування помилкових або необґрунтованих висновків.

Додатково системи штучного інтелекту характеризуються вразливістю до цілеспрямованого зовнішнього впливу, зокрема шляхом застосування так званих *adversarial examples* – спеціально модифікованих вхідних даних, які за мінімальних і практично непомітних для людини змін можуть призводити до істотних викривлень результатів аналізу. Наявність таких уразливостей ставить під сумнів надійність використання технологій штучного інтелекту під час роботи з цифровими слідами, особливо в умовах змагальності судового процесу.

Аналіз чинного законодавства України засвідчує відсутність комплексного та системного нормативного регулювання ключових питань застосування систем штучного інтелекту у сфері кримінального провадження. Подібна правова невизначеність спостерігається й у суміжних галузях права, що зумовлює міждисциплінарний характер зазначеної проблематики та потребу у виробленні узгоджених підходів до її вирішення.

По-перше, на законодавчому рівні відсутнє визначення правового статусу результатів, отриманих із використанням систем штучного інтелекту. Така обставина формує правову невизначеність щодо можливості визнання відповідної інформації належними, допустимими, достовірними та достатніми доказами у кримінальному провадженні. Неврегульованість критеріїв оцінки фактично унеможливлює повноцінне процесуальне використання відомостей, сформованих або оброблених із застосуванням технологій штучного інтелекту.

По-друге, чинне законодавство не передбачає уніфікованих процедур перевірки (верифікації) цифрових слідів, які були зібрані, ідентифіковані чи проаналізовані за допомогою автоматизованих систем на основі штучного інтелекту. Це істотно ускладнює оцінку їх достовірності та створює ризики використання доказів, що не відповідають вимогам наукової обґрунтованості, відтворюваності й об'єктивності.

По-третє, законодавчо не врегульовано питання розподілу юридичної відповідальності у випадках помилок або технічних збоїв, що виникають під

час використання систем штучного інтелекту у процесі прийняття рішень. У зв'язку з цим залишається відкритим питання щодо суб'єкта відповідальності за наслідки такого використання – розробника програмного забезпечення, оператора системи, експерта, який застосовував інструменти штучного інтелекту, чи слідчого, який покладався на відповідні результати при ухваленні процесуальних рішень. Подібна невизначеність має безпосередній вплив на забезпечення гарантій справедливого судового розгляду, реалізацію прав сторін кримінального провадження та ефективний захист від можливих технічних або процедурних зловживань.

Використання систем штучного інтелекту у кримінальному провадженні за відсутності належного контролю або чітко визначених процесуальних гарантій може призводити до істотних порушень прав учасників кримінального процесу. Насамперед це стосується ризиків, пов'язаних із дотриманням фундаментальних принципів кримінального судочинства та стандартів справедливого правосуддя. У ситуаціях, коли стороні захисту не забезпечено доступ до інформації про архітектуру алгоритму, параметри його навчання чи методи оброблення цифрових слідів, виникає реальна загроза обмеження права на захист, зокрема можливості ефективного оскарження доказів, покладених в основу обвинувачення.

Додатковим джерелом ризиків є застосування алгоритмів, навчання яких здійснювалося на упереджених або нерепрезентативних масивах даних, що може зумовлювати формування дискримінаційних чи стереотипних висновків. Подібні проблеми вже знаходили відображення у міжнародній правозастосовній практиці, зокрема у випадках, коли системи штучного інтелекту демонстрували статистичну схильність до формування обвинувальних результатів стосовно представників окремих етнічних, соціальних або демографічних груп. Так, у ході журналістських розслідувань було задокументовано щонайменше вісім фактів неправомірних арештів у різних штатах США, спричинених хибними результатами алгоритмів розпізнавання облич, причому переважна більшість постраждалих належала до афроамериканської спільноти, що свідчить про наявність системної алгоритмічної упередженості[15].

Оскільки функціонування систем штучного інтелекту ґрунтується на аналізі наявних масивів даних, використання спотворених, фальсифікованих або отриманих із порушенням вимог законодавства цифрових слідів неминуче зумовлює формування хибних або недостовірних висновків. Водночас можливості сучасних систем штучного інтелекту щодо відмежування автентичних цифрових слідів від штучно створених чи модифікованих залишаються обмеженими, особливо у випадках застосування високотехнологічних методів фальсифікації, у тому числі із залученням тих самих алгоритмів штучного інтелекту. За таких умов виникають суттєві ризики для забезпечення точності, достовірності та процесуальної допустимості доказів, отриманих у результаті автоматизованого аналізу цифрової інформації.

[15] MacMillan D. Arrested by AI: Police ignore standards after facial recognition matches. *The Washington Post.* 13 січня 2025. URL: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ (дата звернення: 20.01.2026).

Використання технологій штучного інтелекту у криміналістичній діяльності становить перспективний напрям розвитку, який розширює можливості підвищення ефективності розкриття та розслідування кримінальних правопорушень, автоматизації типових аналітичних і технічних процедур, прогнозування злочинної активності, а також опрацювання значних за обсягом масивів інформації. Різні варіації штучного інтелекту, зокрема методи машинного й глибокого навчання, обробки природної мови та комп'ютерного зору, вже активно впроваджуються у низці напрямів криміналістичних досліджень[16].

Системи штучного інтелекту створюють можливості для автоматизації процесів виявлення, систематизації та аналітичного тлумачення цифрових слідів із високим рівнем точності. Вони спроможні встановлювати приховані взаємозв'язки між окремими об'єктами, фіксувати аномальні прояви у поведінці осіб, реконструювати послідовність подій і формувати обґрунтовані доказові гіпотези на основі комплексного аналізу цифрової інформації. Окрім цього, технології штучного інтелекту можуть інтегруватися у процедури судово-експертних досліджень, істотно скорочуючи строки опрацювання та інтерпретації цифрових доказів.

Водночас, попри значний потенціал застосування штучного інтелекту у сфері аналізу цифрових слідів, його впровадження супроводжується низкою істотних ризиків і проблем, що зумовлюють необхідність комплексного нормативно-правового регулювання, формування етичних стандартів використання відповідних технологій, а також підвищення рівня цифрової компетентності всіх учасників кримінального провадження.

Упровадження технологій штучного інтелекту в практичну діяльність супроводжується комплексом суттєвих ризиків і проблем, серед яких особливе місце посідають алгоритмічна упередженість, обмежена прозорість процесів ухвалення рішень, етичні та правові виклики, а також наявні технічні обмеження й рівень готовності правничого середовища до використання таких інструментів. З метою мінімізації зазначених ризиків і підвищення результативності застосування штучного інтелекту в криміналістичній практиці необхідним є формування чітких етичних і правових стандартів, забезпечення прозорості та підзвітності алгоритмічних рішень, а також удосконалення якості й репрезентативності навчальних даних.

Доцільним вбачається поетапне та виважене впровадження систем штучного інтелекту у криміналістичну практику за умови збереження визначальної ролі людини у прийнятті остаточних процесуальних рішень і з урахуванням потенційного впливу відповідних технологій на права людини та принципи справедливого судочинства. За відсутності належного нормативного й інституційного врегулювання необґрунтоване та широкомасштабне використання штучного інтелекту у сфері кримінального судочинства здатне поставити під загрозу фундаментальні засади кримінального процесу, що є апріорі неприпустимим.

[16] Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство*. 2025. № 3. Ч.3. С.215. https://app-journal.in.ua/wp-content/uploads/2025/06/33-2.pdf

2. Цифрові сліди мобільних засобів зв'язку у криміналістичній практиці

Розвиток науково-технічного прогресу, використання штучного інтелекту, упровадження сучасних досягнень науки і техніки в практику вчинення кримінальних правопорушень зумовлює необхідність вдосконалення науково-методичного та техніко-криміналістичного забезпечення розслідування злочинів, одним із пріоритетних напрямів якого стає використання спеціальних знань і спеціальної криміналістичної техніки.

Одним із найпоширеніших видів технічних засобів, що використовуються злочинцями під час вчинення правопорушень, є мобільні телефони (смартфони), за допомогою яких узгоджуються та координуються злочинні дії співучасників, висуваються погрози і здійснюється вимагання грошових коштів або майна, підшукують та вербують нових виконавців, визначають дії спільників із підготовки та приховування злочинної діяльності, збирають інформацію щодо майбутніх жертв, фіксують результати своїх дій для звітування, реалізують шахрайські схеми заволодіння чужим майном тощо. Сучасні можливості засобів мобільного зв'язку дають змогу здійснювати дзвінки та обмінюватися повідомленнями за допомогою стільникового зв'язку, проводити фото та відео зйомку, спілкуватися та передавати великі об'єми інформації через месенджери (Telegram, WhatsApp, Viber, Signal тощо), моніторити соціальні мережі та інтернет-простір.

Механізм слідоутворення під час використання засобів мобільного зв'язку має свою специфіку, оскільки утворені ними сліди, маючи інформаційний характер, не відображаються у зовнішній матеріальній обстановці. Використання спеціальних знань під час розслідування кримінальних правопорушень дає змогу не тільки виявити й зафіксувати залишені за допомогою мобільних засобів стільникового зв'язку сліди злочинної діяльності, але й встановити місцезнаходження злочинця або потерпілого, визначити маршрут їхнього переміщення, відновити текстову й мультимедійну інформацію, передану за допомогою мобільного пристрою, з'ясувати приналежність переданих даних конкретній особі.

Сліди, що утворюються під час вчинення злочинів із використанням мобільних засобів зв'язку – це інформація, яка зафіксована в цифрову форматі, міститься в різного роду цифрових пристроях зі створення, оброблення, збереження та передачі цієї інформації, причинно пов'язана з подією кримінального правопорушення, та дає змогу встановити як обставини вчиненого злочину, так і особу злочинця. Іншими словами такі сліди отримали назву цифрових, під якими розуміють дані, що залишаються в цифровому просторі внаслідок використання цифрових пристроїв, технологій та інформаційних мереж, які можуть бути використані в кримінальному провадженні й судочинстві[17].

Інформація (цифрові сліди), яка зберігається у операторів та провайдерів телекомунікацій, відіграє важливу роль у процесі кримінального провадження.

[17] Криміналістика: підручник / В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін.; за ред. В. М. Шевчука. Харків: Право, 2024. С. 396.

Встановлення особи, що користувалася послугами мобільного зв'язку, надає можливість органам досудового розслідування отримати відомості про ймовірного правопорушника, його соціальні зв'язки, а також характер і обставини протиправної діяльності. Будь-які дії злочинця, потерпілого чи інших осіб, які користуються послугами мобільного зв'язку, знаходять відображення на серверах оператора.

Такий процес збирання, аналіз та систематизації інформації отримав назву – білінг. В сучасних телекомунікаційних компаніях білінг – це складний комплекс програм, який дозволяє реалізувати процес збору інформації про використання телекомунікаційних послуг, тарифікацію, виставлення рахунків й обробку платежів споживачів послуг фіксованого і мобільного зв'язку, доступу до мережі Інтернет, інтернет-телефонії[18].

Оператори мобільного зв'язку в процесі надання телекомунікаційних послуг здійснюють безперервну фіксацію технічних параметрів функціонування мобільних пристроїв абонентів шляхом використання реєстрів місцезнаходження та переміщення. У результаті такої діяльності на серверах оператора формується база білінгових даних, яка містить відомості про ідентифікаційні характеристики абонента та параметри з'єднань, зокрема: 1) номер SIM-картки абонента; 2) міжнародний ідентифікаційний номер мобільного обладнання (IMEI); 3) дату, час та тривалість телекомунікаційного з'єднання; 4) номер абонента, який ініціює виклик; 5) номер абонента, з яким встановлюється з'єднання; 6) ім'я абонента, закріплене за відповідним номером у разі його верифікації; 7) вартість наданих послуг зв'язку; 8) ідентифікатор базової станції, через яку здійснено початок з'єднання; 9) ідентифікатор базової станції, через яку завершено з'єднання.

Встановлення місцезнаходження підозрюваного, потерпілого або будь-якої іншої особи може здійснюватися за допомогою можливостей технічних засобів операторів стільникового зв'язку або ж із використанням слідчими спеціалізованої криміналістичної техніки. Як правило, на етапі відкриття кримінального провадження підозрюваний невідомий і, запросивши дані білінгу, слідчий отримує масив даних про здійснені з'єднання абонентів за вказаний період часу в межах відповідної базової станції біля місця вчинення кримінального правопорушення. У подальшому, слідчий, аналізуючи отримані дані, виділяє збіги за датою, місцем і часом, після чого здійснюється перевірка конкретних SIM- та IMEI-номерів.

Зазначені відомості можуть бути отримані слідчим під час проведення такого заходу забезпечення кримінального провадження, як тимчасовий доступ до речей і документів. Відповідна ухвала слідчого судді надсилається оператору мобільного зв'язку, у володінні якого перебуває необхідна інформація, після чого уповноважена службова особа зобов'язана забезпечити тимчасовий доступ до неї з метою вилучення або виготовлення належним чином засвідчених копій. Надалі отриманий масив даних щодо конкретного абонентського номера оператора

[18] Сертифікація білінгових систем в Україні. URL: http://oniis.org/ukr/poslugi/sertifikaciya-obladnannya-zvyazku/sertifikaciya-bilingovih-sistem-v-ukraini (дата звернення: 20.01.2026)

мобільного зв'язку підлягає аналітичному опрацюванню. У разі виникнення потреби в одержанні додаткових відомостей, що мають значення для кримінального провадження, можливе проведення негласних слідчих (розшукових) дій, зокрема зняття інформації з електронних комунікаційних мереж відповідно до статті 263 КПК України або встановлення місцезнаходження радіообладнання (радіоелектронного засобу) згідно зі статтею 268 КПК України[19]. Положеннями статей 159 та 162 КПК України передбачена можливість отримання слідчим або прокурором відомостей про телекомунікаційні з'єднання, що мали місце у минулому (постфактум), зокрема інформації щодо місцезнаходження радіоелектронного засобу у визначений проміжок часу. Відповідно до частини першої статті 165 КПК України особа, яка зазначена в ухвалі слідчого судді або суду про надання тимчасового доступу до речей і документів як їх володілець, зобов'язана забезпечити надання такого доступу до визначених в ухвалі об'єктів особі, зазначеній у відповідному судовому рішенні, або іншій уповноваженій особі, яка діє на підставі доручення слідчого[20].

Відповідно до п. 1 ст. 159 КПК тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення. Відповідно до п. 2 ч.2, 3 ст. 168 КПК тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку не допускається, за винятком випадків, коли надання відповідних об'єктів разом з інформацією, що на них зберігається, є необхідною умовою проведення експертного дослідження, або коли такі об'єкти були отримані внаслідок вчинення кримінального правопорушення чи використовувалися як засіб або знаряддя його вчинення, а також у ситуаціях, коли доступ до них обмежується власником, володільцем чи утримувачем або пов'язаний із необхідністю подолання систем логічного захисту. У разі потреби слідчий або прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих), телекомунікаційних чи інформаційно-телекомунікаційних системах, а також у їх невід'ємних складових частинах. Копіювання такої інформації проводиться із залученням спеціаліста з метою забезпечення належної повноти, точності та збереження цілісності цифрових даних[21].

Оброблення цифрових доказів здійснюється з урахуванням вимог, викладених в ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи

[19] Кузубова Т. О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в України. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 2. С. 118. URL: https://dspace.univd.edu.ua/items/d6ab6f17-2a01-407a-a288-d51d5ee4488b

[20] Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні: метод. рек. / О.В. Таран, О.М. Брисковська, О.С. Тарасенко, А.А. Вознюк та ін. Київ: Нац. акад. внутр. справ, 2021. С. 13. URL: https://elar.naiau.kiev.ua/bitstreams/28ffc35c-c1e5-4583-8e16-2954c8bdd641/download

[21] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651 – VI URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»[22].

Процес ідентифікації складається з пошуку, розпізнавання та документування потенційного цифрового доказу. В процесі ідентифікації працівники правоохоронного органу повинні визначити носій інформації, цифрові дані на якому потрібно зберегти у якості доказу, а також пристрої обробки інформації, які можуть містити потенційні цифрові докази, що стосуються кримінального правопорушення. Збирання передбачає вилучення пристроїв, які можуть містити цифрові докази з метою їх подальшого огляду та проведення експертних досліджень[23].

На стадії вчинення кримінального правопорушення та безпосереднього приховування його слідів і наслідків причетна особа може здійснювати дії, спрямовані на знищення, модифікацію або унеможливлення доступу до цифрової інформації, що зберігається на мобільному пристрої. До таких дій, зокрема, належать видалення електронного листування, фото- й відеоматеріалів, очищення історії вебперегляду, застосування засобів шифрування, а також блокування доступу до відповідних даних на мобільному телефоні.

З метою забезпечення своєчасного та належного вилучення електронно-цифрових слідів у криміналістичній практиці застосовуються спеціалізовані апаратно-програмні комплекси мобільної криміналістики. Для отримання та аналізу інформації з мобільних терміналів підрозділи правоохоронних органів України широко використовують відповідні технічні засоби, зокрема апаратно-програмні комплекси «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC Physical Analyzer». Зокрема, такі комплекси використовують у своїй роботі оперативно-технічні підрозділи Національної поліції України та ДНДЕКЦ МВС України[24] під час проведення: 1) відповідних оперативно-технічних заходів та негласних слідчих (розшукових) дій зі зняття інформації з електронних інформаційних систем; 2) слідчої (розшукової) дії як-то: огляд місцевості, приміщення, речей, документів та комп'ютерних даних (ст. 237 КПК України), для огляду мобільного терміналу (стільникового радіотелефону) та/або SIM-картки, виявлених на місці вчинення кримінального правопорушення;

[22] Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів: ДСТУ ISO/IEC 27037:2017. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC

27037:2012, IDT); Чинний від 2019-01-01. Київ: УкрНДНЦ, 2018. VI, 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

[23] Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у

[23] Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі: науково-методичні рекомендації / розробн. Манжай О.В., Носов В.В., Мальцев В.В., Роговий А.П./ за ред. Бутко Р.Ю. Харків: ХНУВС, 2024. С. 29. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/10ad6bf2-b7d4-45d1-9923-34e9acc0d785/content?trackerId=5e9e04034bf21dff

[24] Кобець М. В. Апаратно-програмний комплекс «Cellebrite UFED» як засіб отримання інформації з мобільних терміналів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану*: матер. міжвідоч. наук.-практ. конференції (м. Київ, 30 берез. 2023 р.). Київ: Нац. акад. внутр. справ. 2023. С. 71. URL: https://elar.navs.edu.ua/items/71ba959b-a48b-468d-a611-cad52e202482

3) обшуку житла чи іншого володіння особи, обшуку особи (ст. 236 КПК України) для доступу до комп'ютерних систем або їх частин, мобільних терміналів (стільникових радіотелефонів) та/або SIM-карток[25].

Зазначені апаратно-програмні комплекси забезпечують можливість пошуку, вилучення та аналізу інформації, що зберігається на мобільних і комп'ютерних пристроях, а також у хмарних сховищах даних (зокрема iCloud, Google, Dropbox), у тому числі у випадках, коли відповідний пристрій перебуває у заблокованому стані. Програмні засоби дозволяють отримувати дані як безпосередньо з мобільних терміналів, так і з їх резервних копій незалежно від особливостей встановленої операційної системи. У результаті застосування такого програмного забезпечення формується повний цифровий образ досліджуваного пристрою, включно з інформацією із зашифрованих застосунків, яка виявляється та, за наявності технічної можливості, розшифровується у максимально повному обсязі й відповідає даним, що містилися на оригінальному пристрої.

Вагомою перевагою зазначених апаратно-програмних комплексів є можливість дослідження мобільних пристроїв, що перебувають у неробочому стані, зокрема внаслідок тривалого впливу води або механічних ушкоджень. Окрім смартфонів на базі операційних систем iOS та Android, програмне забезпечення підтримує також менш поширені платформи, такі як Windows Phone, BlackBerry OS тощо. Пріоритетним напрямом функціонування UFED є виявлення та вилучення інформації з прихованих або видалених джерел, зокрема електронного листування у месенджерах, контактних даних, фотографій і відеозаписів. Крім того, програмні інструменти дозволяють відновлювати та аналізувати геолокаційні дані, що зберігалися на пристрої під час його використання, з метою встановлення маршруту переміщення користувача.

Розкриття та розслідування кримінальних правопорушень, що вчиняються з використанням мобільних засобів зв'язку, вимагає наявності спеціальних знань і навичок у дослідженні інформаційного простору вилученого пристрою. Якщо слідчий приймає рішення здійснити огляд самостійно, він повинен дотримуватися певних криміналістичних рекомендацій.

Слідчий огляд мобільного засобу зв'язку передбачає дві стадії – статичну та динамічну[26]. Проведення слідчої дії починається із загального огляду мобільного пристрою, результати якого підлягають обов'язковій фіксації у протоколі. У ньому, зокрема, зазначаються модель смартфона, його конструктивні особливості (форма, колір, габарити), найменування та наявність ідентифікаційних позначень (логотипів), а також інформація про оснащення пристрою вбудованими фото- чи відеокамерами з лицьового та тильного боку.

[25] Тіхонов С. В., Кобець М. В. Застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень: метод. рекомендації. Київ: Нац. акад. внутр. справ, 2023. С. 6. URL: https://elar.navs.edu.ua/items/eb658e56-3060-413b-9e01-6f797ce3e731

[26] Курман О.В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 533. URL: https://app-journal.in.ua/wp-content/uploads/2023/10/APP_05_2023_FINAL.pdf

Крім того, у протоколі відображається розташування функціональних і сенсорних елементів керування, а також наявність технічних роз'ємів, зокрема micro-USB або Type-C, призначених для підключення зарядних пристроїв, стереонавушників, а також отворів для динаміків і мікрофона.

За наявності технічної можливості та з урахуванням конкретної слідчої ситуації слідчому доцільно залучати спеціаліста й використовувати відповідні техніко-криміналістичні засоби для розблокування мобільного пристрою у випадках, коли на ньому застосовано один із засобів захисту, зокрема буквено-цифровий пароль, PIN-код, графічний ключ, біометричну ідентифікацію за обличчям (Face ID) або інші подібні механізми.

У протоколі огляду слідчий зобов'язаний детально зафіксувати процедуру розблокування мобільного пристрою (смартфона), а також усі подальші дії у чіткій хронологічній послідовності. Після отримання доступу до пристрою здійснюється опис графічних і текстових елементів інтерфейсу, що відображаються у центральному вікні екрана та додаткових системних або прикладних вікнах.

Виявлення криміналістично значущої інформації здійснюється шляхом аналізу вмісту мобільного пристрою, зокрема журналу вхідних і вихідних дзвінків, SMS-повідомлень, електронної та голосової пошти, історії користування вебброузером (у тому числі вмісту каталогів «Вибране», «Журнал», «Cookies», «Temporary Internet Files»), даних месенджерів (WhatsApp, Viber, Telegram тощо), фото- й відеоматеріалів, аудіозаписів диктофона, а також інформації, що міститься в органайзері, з урахуванням технічних особливостей конкретної моделі смартфона.

Під час огляду вмісту мобільного засобу зв'язку спеціаліст за дорученням слідчого здійснює поетапну детальну фотозйомку зображень, що відображаються на екрані мобільного пристрою, з метою фіксації відомостей, які мають значення для кримінального провадження.

У випадках, коли обсяг інформації, що міститься в пам'яті технічного пристрою, є значним, доцільним є застосування методів і прийомів криміналістичного відеозапису для забезпечення повної та наочної фіксації відповідних даних. За таких умов слідчий зобов'язаний здійснювати усний коментар усіх дій і маніпуляцій, спрямованих на одержання конкретних відомостей із мобільного пристрою (смартфона), що забезпечує належну процесуальну фіксацію ходу та результатів огляду.

Водночас слід констатувати наявність низки технічних обмежень і проблем, пов'язаних із застосуванням криміналістичних програмно-технічних комплексів мобільної криміналістики. Одним із основних завдань слідчого за участю спеціаліста є отримання доступу до інформації, що зберігається на захищених мобільних пристроях або перебуває у зашифрованому вигляді. Однак засоби захисту сучасних смартфонів постійно удосконалюються, що, у свою чергу, істотно ускладнює процес їх розблокування та вилучення цифрових даних. У разі впровадження виробниками нових або оновлених протоколів безпеки операційних систем iOS та Android і їх встановлення на мобільні пристрої виникають труднощі з реалізацією повного функціоналу відповідних програмно-апаратних комплексів, а в окремих випадках – і повна

неможливість розшифрування даних. За таких умов від розробників криміналістичних програмно-технічних засобів вимагається постійне оновлення знань щодо характеристик нових моделей пристроїв, особливостей операційних систем та сучасних методів шифрування. Водночас на практиці інструментарій, що пропонується, не завжди є сумісним з останніми поколіннями мобільних пристроїв або з численними варіаціями їх регіональних чи операторських модифікацій.

ВИСНОВКИ

Цифровізація суспільних відносин і масове використання електронних технологій комунікації зумовили формування принципово нового інформаційного середовища, у межах якого майже кожна дія людини залишає цифрові сліди. Особливе місце серед технічних засобів, що використовуються як у повсякденному житті, так і в злочинній діяльності, посідають мобільні телефони (смартфони). Їх багатофункціональність, постійне підключення до мереж електрозв'язку та здатність акумулювати значні обсяги різнорідної інформації роблять ці пристрої одним із ключових джерел криміналістично значущих даних. Саме через мобільні засоби зв'язку здійснюється координація злочинних дій, передавання вказівок, погроз, реалізація шахрайських схем, а також фіксація та приховування результатів протиправної діяльності.

Механізм слідоутворення під час використання мобільних пристроїв має специфічний інформаційний характер і не проявляється у традиційній матеріальній формі. Цифрові сліди локалізуються у внутрішній пам'яті пристроїв, хмарних сховищах, а також у базах даних операторів і провайдерів телекомунікацій. Їх виявлення, фіксація та дослідження можливі виключно за умови застосування спеціальних криміналістичних знань і сучасних техніко-криміналістичних засобів. Аналіз таких слідів дозволяє встановлювати обставини вчинення кримінального правопорушення, ідентифікувати осіб, причетних до нього, відновлювати маршрути переміщення, часову послідовність подій, коло контактів і характер комунікацій.

Важливе місце у процесі доказування займає інформація білінгу, що накопичується на серверах операторів мобільного зв'язку. Відомості про SIM-картки, IMEI-номери, параметри з'єднань і дані базових станцій дають змогу реконструювати події, які відбувалися у конкретний час і в певному місці, а також звузити коло ймовірних підозрюваних. Процесуальні механізми отримання такої інформації, передбачені кримінальним процесуальним законодавством України, створюють необхідні правові умови для її використання як доказу за умови дотримання вимог законності, належності та допустимості.

Водночас стрімке зростання обсягів цифрових даних і їх неструктурований характер істотно ускладнюють застосування традиційних методів аналізу. У цьому контексті штучний інтелект постає як перспективний інструмент оптимізації процесів виявлення, систематизації та інтерпретації цифрових слідів. Використання алгоритмів машинного навчання, обробки природної мови та комп'ютерного зору дозволяє автоматизувати аналіз великих масивів інформації, відновлювати хронологію подій, виявляти приховані взаємозв'язки між об'єктами та формувати обґрунтовані доказові гіпотези. Інтеграція таких

технологій у діяльність слідчих і експертних підрозділів здатна суттєво підвищити ефективність розслідування злочинів, учинених із використанням інформаційних технологій.

У той же час впровадження штучного інтелекту та сучасних апаратно-програмних комплексів мобільної криміналістики супроводжується низкою суттєвих проблем і ризиків. Серед них – складність встановлення причинно-наслідкових зв'язків між вхідними даними та отриманими результатами аналізу, імовірність помилкових результатів, уразливість до технічних атак, а також постійне вдосконалення засобів захисту операційних систем і методів шифрування, що ускладнює доступ до даних. Крім того, відсутність чіткого нормативно-правового врегулювання статусу результатів, отриманих із використанням інтелектуальних технологій, створює ризики порушення прав учасників кримінального провадження та принципів справедливого судочинства.

Узагальнюючи викладене, можна дійти висновку, що ефективне розслідування кримінальних правопорушень у цифровому середовищі можливе лише за умови комплексного поєднання процесуальних механізмів, спеціальних знань, сучасних техніко-криміналістичних засобів і контрольованого використання технологій штучного інтелекту. Подальший розвиток криміналістичної науки в цьому напрямі має бути спрямований на вдосконалення методик роботи з цифровими слідами, адаптацію технічних інструментів до нових технологічних викликів, формування чітких правових і етичних стандартів застосування ШІ та забезпечення балансу між ефективністю розслідування й дотриманням прав і свобод людини.

АНОТАЦІЯ

У науковій роботі досліджено сучасні криміналістичні засоби отримання значущої інформації для розслідування кримінальних правопорушень в умовах цифровізації суспільних відносин. Розкрито сутність і особливості формування цифрових слідів як результату використання інформаційно-комунікаційних технологій у повсякденній та злочинній діяльності. Проаналізовано наукові підходи до визначення поняття, ознак і класифікації цифрових слідів у криміналістиці. Окрему увагу приділено дослідженню ролі мобільних засобів зв'язку як одного з ключових джерел цифрових доказів. Висвітлено механізми слідоутворення під час використання мобільних пристроїв та можливості їх дослідження з застосуванням спеціальних криміналістичних знань і технічних засобів. Розглянуто потенціал використання штучного інтелекту для автоматизованого виявлення, аналізу та інтерпретації цифрових слідів. Проаналізовано основні технічні, правові та етичні проблеми впровадження інтелектуальних технологій у криміналістичну діяльність. Окреслено ризики, пов'язані з достовірністю, допустимістю та законністю результатів, отриманих за допомогою систем штучного інтелекту. Запропоновано напрями вдосконалення криміналістичних методик роботи з цифровими слідами з урахуванням сучасних технологічних викликів.

Література

1. MacMillan D. Arrested by AI: Police ignore standards after facial recognition matches. *The Washington Post.* 13 січня 2025. URL: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ (дата звернення: 20.01.2026).
2. Shevchuk V. M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver, Canada). 2023. Pp. 198–219. URL: https://archive.interconf.center/index.php/2709-4685/issue/view/19-20.05.2023/165
3. Авдєєва Г. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики*. 2018. С. 90–93. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf
4. Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично порівняльне правознавство*. 2025. № 1. С. 818-824. URL: https://doi.org/10.24144/2788-6018.2025.01.136
5. Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні: метод. рек. / О.В. Таран, О.М. Брисковська, О.С. Тарасенко, А.А. Вознюк та ін. Київ: Нац. акад. внутр. справ, 2021. 50 с. URL: https://elar.naiau.kiev.ua/bitstreams/28ffc35c-c1e5-4583-8e16-2954c8bdd641/download
6. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. Вип. 85, ч. 4. С. 71–75. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/12-3.pdf
7. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.; за заг. ред. В. Ю. Шепітька. Харків: Право, 2024. 208 с. URL: https://ivpz.kh.ua/wp-content/uploads/2025/01/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F-%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D1%96%D0%B2-2024.pdf
8. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів: ДСТУ ISO/IEC 27037:2017. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); Чинний від 2019-01-01. Київ: УкрНДНЦ, 2018. VI, 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf
9. Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 21-31. URL: http://pbz.nlu.edu.ua/issue/view/17882
10. Кобець М. В. Апаратно-програмний комплекс «Cellebrite UFED» як засіб отримання інформації з мобільних терміналів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану*: матер. міжвідоч. наук.-практ. конференції (м. Київ, 30 берез. 2023 р.). Київ: Нац. акад. внутр. справ. 2023. С. 70-73. URL: https://elar.navs.edu.ua/items/71ba959b-a48b-468d-a611-cad52e202482

11. Коваленко А. В. Класифікація електронних (цифрових слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. URL: http://plaw.nlu.edu.ua/issue/view/16823

12. Колеснікова І. А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. № 10. С. 472–475. URL: http://lsej.org.ua/10_2023/114.pdf

13. Криміналістика: підручник / В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін.; за ред. В. М. Шевчука. Харків: Право, 2024. 1008 с.

14. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651–VI. URL:https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.01.2026)

15. Кузубова Т. О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в України. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 2. С. 117-123. URL: https://dspace.univd.edu.ua/items/d6ab6f17-2a01-407a-a288-d51d5ee4488b

16. Курман О. В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 532-536. URL: https://app-journal.in.ua/wp-content/uploads/2023/10/APP_05_2023_FINAL.pdf

17. Курман О. Правові та практичні аспекти використання поліграфа у кримінальному провадженні України. *Сучасний досвід використання поліграфа у сфері національної безпеки і оборони України в умовах воєнних загроз*: зб. матеріалів панел. дискусії: IX Харків. міжнар. юрид. форум, м. Харків, 26 верес. 2025 р. / редкол.: А. Гетьман, В. Журавель, В. Шевчук та ін.; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики; Нац. акад. прав. наук України; Всеукр. асоц. поліграфологів [та ін.]. Харків: Право, 2025. С. 76-80. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20575

18. Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. 2017. № 4. С. 245-249. URL: http://pravoisuspilstvo.org.ua/archive/2017/4_2017/part_1/44.pdf

19. Курман О. В. Типізація способів учинення злочинних посягань на відомості, що становлять комерційну або банківську таємницю. *Теорія та практика судової експертизи і криміналістики*: збірник наукових праць. Вип. 10 / ред. кол.: М.Л. Цимбал, В.Ю. Шепітько, Л.М. Головченко та ін. Харків.: Право, 2010. С. 62-68.

20. Латиш К. В. Криміналістичний аналіз кіберінструментів вчинення злочинів. *Проблеми законності*. 2021. Вип. 153. С. 165-172. URL: http://nbuv.gov.ua/UJRN/Pz

21. Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі: науково-методичні рекомендації / розробн. Манжай О.В., Носов В.В., Мальцев В.В., Роговий А.П./ за ред. Бутко Р.Ю. Харків: ХНУВС, 2024. 36 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/10ad6bf2-b7d4-45d1-9923-34e9acc0d785/content?trackerId=5e9e04034bf21dff

22. Негребецький В. В. Використання систем штучного інтелекту у боротьбі зі злочинністю: огляд та перспективи. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. № 1 (9). С. 66-70. URL: DOI: https://doi.org/10.32782/2709-9261-2024-1-9-13

23. Плахотнік О. В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4. С. 45-57. URL: https://vkslaw.com.ua/index.php/journal/article/view/222

24. Сертифікація білінгових систем в Україні. URL: http://oniis.org/ukr/poslugi/sertifikaciya-obladnannya-zvyazku/sertifikaciya-bilingovih-sistem-v-ukraini (дата звернення: 20.01.2026)

25. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283-284. URL: https://dspace.univd.edu.ua/items/b174d57a-bf4b-47f9-9211-aeb715b61844

26. Тіхонов С. В., Кобець М. В. Застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень: метод. рекомендації. Київ : Нац. акад. внутр. справ, 2023. 41 с. URL: https://elar.navs.edu.ua/items/eb658e56-3060-413b-9e01-6f797ce3e731

27. Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики. *Аналітично-порівняльне правознавство.* 2025. № 3. Ч.3. С. 211-215. URL: https://app-journal.in.ua/wp-content/uploads/2025/06/33-2.pdf

28. Черевко К. О., Луценко І. Г. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 1. С. 124-133. URL: DOI: https://vca.univd.edu.ua/index.php/vca/article/view/43

29. Шевчук В. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія* / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. Харків: Право, 2024. С. 83–106. URL: https://ivpz.kh.ua/wp-content/uploads/2025/01/Монорафія-Криміналістів-2024.pdf

30. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. *Військові правопорушення та воєнні злочини: історія, теорія та практика*. Колективна монографія. “Izdevnieciba “Baltija Publishing” (м. Рига, Латвія), 2023. С. 795-822. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/322/8791/18392-1

31. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю*: зб. наук. праць. Харків: Право, 2011. Вип. 21. С. 39-46.

Information about the autho:
Kurman Oleksandr Vasylyovych,
Candidate of Law,
Associate Professor of the Department of Forensic Science
Yaroslav the Wise National Law University
77, Hryhoriya Skovoroda St., Kharkiv, 61024, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-10

СУЧАСНІ ВИКЛИКИ КРИМІНАЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРЗЛОЧИННОСТІ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ ВИМІРИ

Ларченко М. О.

ВСТУП

Стрімкий розвиток цифрових технологій та глобалізація кіберпростору зумовили нові загрози безпеці держав, суспільства та окремих українських громадян. Кіберзлочинність набуває все більшої організованості, а її наслідки можуть мати критичний вплив на функціонування інформаційних систем, фінансового сектору, критичної інфраструктури та навіть національної безпеки. Кримінально-правове регулювання кіберзлочинності стикається з низкою викликів, серед яких: швидка еволюція способів вчинення кіберзлочинів, складність ідентифікації правопорушників, проблеми кваліфікації окремих діянь та їх відмежування від суміжних правопорушень, відсутність єдиних стандартів відповідальності на міжнародному рівні, а також неефективність деяких механізмів правозастосування. Зважаючи на глобальний характер кіберзлочинності, особливої уваги потребує питання міжнародного співробітництва у цій сфері. Незважаючи на існування таких міжнародних правових актів, як Будапештська конвенція про кіберзлочинність, проблема гармонізації законодавства та координації дій держав у боротьбі з кіберзлочинами залишається актуальною. У цьому контексті виникає необхідність комплексного аналізу кримінально-правового регулювання кіберзлочинності, визначення його сучасних викликів на національному та міжнародному рівнях, а також пошуку шляхів удосконалення законодавства та правозастосовної практики.

1. Виникнення передумов проблеми та формулювання проблеми

Дослідження проблеми кіберзлочинності останнім часом постійно проводиться на міжнародному та національному рівнях. Значний внесок у розвиток цієї тематики зробили такі науковці, як Аніщук В. В. та Зицик С. Г., які аналізують методи протидії кіберзлочинам через міжнародну співпрацю[1], а також Степаненко Н. В., Піддубний Д. Д., що досліджують проблематику кримінально-правової кваліфікації атак на критичну інфраструктуру. Зокрема, наголошується, що запобігання та боротьба з кіберзлочинністю вимагає комплексного підходу, що поєднує правове регулювання, технологічні рішення, міжнародне співробітництво та кіберграмотність, йдеться і про необхідність розвитку національного законодавства у сфері кібербезпеки та

[1] Аніщук В. В., Зицик С. Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського Національного Університету.* 2024. Серія ПРАВО. Випуск 83: частина 3, С. 19-23. DOI https://doi.org/10.24144/2307-3322.2024.83.3.2

кіберзлочинності відповідно до міжнародних стандартів[2]. Бараненко Р. В. аналізує особливості застосування спеціальної термінології, аналізуючи наукові праці вітчизняних та зарубіжних дослідників із питань протидії кіберзлочинності[3].

Ряд авторів, зокрема: Авдєєва Г. та Живуцька-Козловська Е., Романюк В. В. та Абламський С. Є., Гарасимів О. І., Марко С. І. та Ряшко О. В. аналізують проблеми використання цифрових доказів у кримінальному судочинстві України та критерії їх допустимості, що є досить серйозною проблемою для судової практики на сучасному етапі. Важливим є також міжнародний досвід у цій сфері, який ще потрібно вивчати та аналізувати[4].

У зарубіжній науці кіберзлочинність вивчають досить глибоко і вже тривалий час. Зокрема, варто згадати роботу Sergiu Cernomoreț та Andrei Nastas, які звертають увагу саме на порівняльний аналіз кіберзлочинності в системі кримінального права та необхідність уніфікації національних правових систем у зазначеній сфері[5]. Актуальним представляється дослідження Murshal Senjaya, де йдеться про кіберзлочинність і кримінальне право в епоху штучного інтелекту. Зокрема, проблеми в правоохоронних органах Індонезії та інших аналізованих автором країн, пов'язані з неправомірним використанням штучного інтелекту, є досить складними, особливо через відсутність конкретних норм, які б регулювали його використання в контексті кіберзлочинності. Існуючі норми часто не охоплюють нові ситуації, що знижує ефективність правозастосування[6]. У підсумку варто згадати Ajoy P. B., який критично аналізуючи ефективність кримінального права в боротьбі з кіберзлочинністю, зазначає, що існує багато факторів, які сприяють неспроможності кримінального права повністю контролювати кіберзлочинність. Ці фактори включають проблеми, пов'язані з анонімністю, юрисдикцією, екстрадицією, правоохоронним механізмом;

---

[2] Степаненко Н. В., Піддубний Д. Д. Сучасні проблеми запобігання і протидії злочинності у сфері інформаційних технологій. *Legal Bulletin.* 2024, 73-81. https://doi.org/10.31732/2708-339X-2024-14-A10

[3] Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ "КПІ" Політологія. Соціологія. Право.* № 1(49) (2021). DOI: https://doi.org/10.20535/2308-5053.2021.1(49).233023

[4] Авдєєва, Г., Живуцька-Козловська, Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*, Вип. 1 (30), 2023. 126-143. https://doi.org/10.32353/khrife.1.2023.07; Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека,* 2 (93), 2024. 140-150. https://doi.org/10.32631/pb.2024.2.13; Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО.* Вип. 75: ч. 2. 2023. 158-162. https://doi.org/10.24144/2307-3322.2022.75.2.25

[5] Sergiu Cernomoreț & Andrei Nastas. Comparative Analysis of Cybercrime in the Criminal Law System. International Academic Publisher. Bucharest, Paris, Calgary 2023. 82 p. URL: https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf

[6] Senjaya, Murshal. Cyber Crime And Criminal Law In The Era Of Artificial Intelligence. International Journal of Law and Society. 1, 2024. 268-276. DOI: https://doi.org/10.62951/ijls.v1i4.210

відсутність даних, що стосуються кіберзлочинності, включаючи неповідомлення про кіберзлочини, труднощі з ідентифікацією, визначенням місцезнаходження та арештом кіберзлочинців, відсутність експертів, проблеми, пов'язані з технологіями, міжнародним правом тощо[7].

Попри значну кількість сучасних українських та закордонних досліджень, ще більше питань залишаються невирішеними. Серед них: 1) недостатня уніфікація кримінально-правових норм щодо відповідальності за кіберзлочини на міжнародному рівні; 2) проблеми ідентифікації злочинців, які діють у цифровому просторі, та особливості збору доказів; 3) відсутність дієвих механізмів співпраці між державами у сфері екстрадиції та спільного розслідування кіберзлочинів; 4) використання криптовалют, анонімних мереж, Darknet(у), що ускладнює виявлення злочинців і відстеження фінансових потоків.

Метою дослідження є комплексний аналіз сучасних викликів кримінально-правового регулювання кіберзлочинності на національному та міжнародному рівнях, зокрема проблем правозастосування щодо кібератак на критичну інфраструктуру, кримінальної відповідальності за розповсюдження шкідливого програмного забезпечення, а також особливостей міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Дослідження спрямоване на виявлення прогалин у чинному законодавстві та правозастосовній практиці, визначення перспектив їх усунення, а також оцінку ефективності міжнародних механізмів протидії кіберзлочинам.

2. Проблеми правозастосування щодо кібератак на критичну інфраструктуру

Критична інфраструктура є однією з найважливіших сфер національної безпеки будь-якої держави, а її захист від кібератак набуває дедалі більшої актуальності. Атаки на енергетичні системи, транспортні мережі, фінансові установи та державні інформаційні ресурси можуть мати катастрофічні наслідки, включаючи порушення функціонування життєво важливих сервісів, економічні збитки та загрозу людським життям. Проте практика правозастосування у сфері боротьби з такими кіберзлочинами стикається з низкою викликів, пов'язаних із міжнародною юрисдикцією, проблемами ідентифікації зловмисників, доказуванням та адекватністю національного законодавства.

Однією з базових проблем є визначення правового статусу кібератак на критичну інфраструктуру. У різних країнах такі злочини можуть кваліфікуватися по-різному: як незаконне втручання в комп'ютерні системи, терористична діяльність або навіть акт кібервійни. В Україні кримінальна відповідальність за кібератаки передбачена Кримінальним кодексом України, зокрема статтями 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»), 361[1] («Створення з метою протиправного

[7] Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis (March 20, 2022). Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2), 2022. 74-79. http://dx.doi.org/10.2139/ssrn.4061947

використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), 361[2] («Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації») та 363[1] («Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»)[8]. Проте визначення «кібератаки» залишається нечітким, що створює труднощі для правозастосовних органів.

Оскільки більшість кібератак здійснюються з-за кордону, правозастосовні органи часто стикаються з труднощами у встановленні та притягненні винних до відповідальності. Ключовими міжнародними інструментами для боротьби з кіберзлочинністю є Будапештська конвенція про кіберзлочинність (2001) та директиви Європейського Союзу у сфері кібербезпеки. Однак ефективність міжнародного співробітництва залежить від рівня взаємної правової допомоги між державами, що може ускладнюватися політичними чинниками та відсутністю єдиних стандартів кримінально-правового переслідування кіберзлочинців. Докладніше в Таблиці 1.

Таблиця 1

Порівняння правових режимів у різних країнах щодо кваліфікації кібератак

Країна	Основні закони та кодекси	Кваліфікація кібератак	Максимальне покарання
Україна	Кримінальний кодекс України (ст. 361, 361-1, 361-2, 363-1)	Незаконне втручання в комп'ютерні системи, поширення шкідливого ПЗ, кібершахрайство	До 10 років позбавлення волі
США	Computer Fraud and Abuse Act (CFAA), Patriot Act	Кіберзлочини кваліфікуються як шахрайство, злом, тероризм або шпигунство	До довічного ув'язнення (якщо спричинені людські жертви)
ЄС (загальні правила)	Директива ЄС 2013/40/EU, GDPR	Несанкціонований доступ, порушення даних, кібершахрайство	Від штрафів до 10 років позбавлення волі
Велика Британія	Computer Misuse Act 1990	Несанкціонований доступ, модифікація даних, DDoS-атаки	До довічного ув'язнення (якщо є серйозні наслідки)

[8] Верховна Рада України. Розділ: Законодавство України. Кримінальний кодекс України. 5 квітня 2001 року, № 2341-III. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 13.03.2025).

Продовження таблиці 1

Німеччина	Strafgesetzbuch (StGB), Telemediengesetz (TMG)	Несанкціонований доступ, порушення конфіденційності, шкідливе ПЗ	До 10 років позбавлення волі
Франція	Code pénal, Loi pour la confiance dans l'économie numérique	Кіберзлочини як комп'ютерне шахрайство або порушення інформаційної безпеки	До 7 років та штрафи до 300 000 євро
Китай	Cybersecurity Law, Criminal Law of PRC	Кібератаки можуть вважатися шпигунством або загрозою держбезпеці	До смертної кари (у випадках державної зради)
Японія	Act on the Prohibition of Unauthorized Computer Access	Несанкціонований доступ, модифікація даних	До 3 років позбавлення волі та штрафи

Ще однією серйозною проблемою є збирання та використання доказів у справах про кібератаки. Виявлення джерела атаки часто є технічно складним завданням, оскільки злочинці використовують анонімізаційні технології, ботнети та викрадені облікові записи. У судовій практиці нерідко виникають питання щодо допустимості цифрових доказів, а також їхньої автентичності та цілісності. Законодавство України містить загальні положення про електронні докази (ст. 99 КПК України «Документи»), а саме: документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження[9], проте потребує подальшої деталізації щодо специфіки доказування кіберзлочинів.

Варто звернути увагу, що в КПК взагалі не йдеться про цифрові докази, бо вони зовсім не тотожні електронним. Якщо під електронними доказами Закон розуміє певним чином розміщену на матеріальному носії цифрову або аналогову інформацію (аудіо чи відео записи, скріншоти переписки тощо), то цифрові докази це зліпки (дампи) оперативної пам'яті комп'ютера, дані аналізу його файлової системи, історія браузера тощо. Аналіз цих об'єктів може виступати предметом технічної експертизи, однак, коли мова йде про кіберзлочини, а також про багато інших категорій кримінальних правопорушень, які вчиняються з використанням комп'ютерів та комп'ютерних

[9] Верховна Рада України. Розділ: Законодавство України. Кримінальний процесуальний кодекс України. 13 квітня 2012 року, № 4651-VI. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 13.03.2025).

мереж, то саме такі цифрові докази мають вирішальну силу, звісно при дотриманні технічних правил їх збирання, зберігання та аналізу. Отримання цифрових доказів здійснюється виключно із дотриманням стандартів цифрової криміналістики та відповідно до міжнародних практик, зокрема, NIST та ISO 27037:2012[10] – єдиний стандарт з цього питання, що офіційно визнаний в Україні (ДСТУ 27037:2012). Лише він нормативно регулює в Україні технічні аспекти збору, зберігання та аналізу цифрових доказів.

Враховуючи вищезазначене, захист критичної інфраструктури від кібератак безумовно вимагає комплексного підходу, що включає вдосконалення національного законодавства, посилення міжнародного співробітництва та розвиток технічних засобів і методів розслідування. Вирішення зазначених проблем можливе шляхом адаптації кримінального та кримінального процесуального законодавства до новітніх викликів у сфері кібербезпеки, а також через активну участь України в міжнародних ініціативах щодо боротьби з кіберзлочинністю.

Ще одним критично важливим аспектом правозастосування щодо кібератак на критичну інфраструктуру є питання відповідальності приватного сектору. У сучасних реаліях значна частина критичної інфраструктури належить або обслуговується приватними компаніями, які не завжди належним чином дотримуються стандартів кібербезпеки. Недостатній рівень захисту інформаційних систем комерційних суб'єктів, які взаємодіють із державними мережами або фінансовими установами, може суттєво посилювати ризики успішності кібератак. У зв'язку з цим деякі країни, зокрема Європейський Союз, запроваджують механізми жорсткішого регулювання кібербезпеки приватного сектору, як-от Директива NIS2, яка встановлює вимоги до суб'єктів критичної інфраструктури щодо управління ризиками кіберзагроз та обов'язкового обміну інформацією про інциденти[11].

Окрім правового аспекту, важливою проблемою залишається питання превентивних заходів та стратегій кіберзахисту. У багатьох випадках кібератаки на критичну інфраструктуру виявляються лише після їх здійснення, що вимагає кардинального перегляду підходів до кібербезпеки на державному рівні. Одним із перспективних напрямів є розбудова національних центрів реагування на кіберінциденти (CERT), які координують діяльність державних і приватних суб'єктів у випадку масштабних атак. Український уряд також активно працює над посиленням кіберзахисту критичної інфраструктури, що знайшло своє відображення у прийнятті Закону України «Про основні засади забезпечення кібербезпеки України»[12] та створенні Національного координаційного центру кібербезпеки.

---

[10] International Standard ISO/IEC 27037. Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

[11] H-X. Директива кібербезпеки NIS2. *Електронний ресурс.* URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua

[12] Верховна Рада України. Розділ: Законодавство України. Закон України «Про основні засади забезпечення кібербезпеки України». 5 жовтня 2017 року № 2163-VIII. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 13.03.2025).

Водночас розвиток міжнародного співробітництва залишається ключовим елементом ефективної боротьби з кібератаками на критичну інфраструктуру. Участь у таких ініціативах, як Глобальний форум із кіберекспертизи (GFCE) чи діяльність у межах партнерства з НАТО (наприклад, у рамках Програми розширених можливостей), дає Україні можливість отримувати оперативну допомогу, обмінюватися розвідданими про нові загрози та вдосконалювати свої методи кіберзахисту.

З огляду на зростаючу кількість кібератак на критичну інфраструктуру, подальший розвиток правозастосування у цій сфері має орієнтуватися на такі ключові напрями: удосконалення кримінального законодавства щодо кіберзлочинів, створення ефективних механізмів притягнення до відповідальності суб'єктів, що нехтують вимогами кібербезпеки, а також активну участь у міжнародних ініціативах з метою посилення глобальної кіберстійкості. Докладніше: рисунок 1.



Рис. 1. Ланцюг кібератак на критичну інфраструктуру

3. Відповідальність за розповсюдження шкідливого програмного забезпечення

Розповсюдження шкідливого програмного забезпечення (ШПЗ) є одним із найбільш небезпечних кіберзлочинів, що завдає значної шкоди як приватним особам, так і державним установам та бізнесу. ШПЗ може використовуватися для крадіжки даних, несанкціонованого доступу до інформаційних систем,

вимагання та навіть для здійснення атак на критичну інфраструктуру. В Україні кримінальна відповідальність за такі дії регламентується статтею 361-1 Кримінального кодексу України, яка передбачає покарання за створення, розповсюдження або збут шкідливих програм.

Однією з основних проблем у боротьбі з розповсюдженням ШПЗ є необхідність доведення умислу правопорушника. Наприклад, розробка програмного забезпечення, яке може бути використане в злочинних цілях, сама по собі не є злочином, якщо особа не мала наміру завдати шкоди. Це створює значні труднощі для правоохоронних органів, особливо з огляду на те, що багато хакерських інструментів мають подвійне використання.

Ще одним викликом є транскордонний характер цього виду кримінальних правопорушень. Шкідливе програмне забезпечення часто поширюється через міжнародні сервери або анонімні платформи, що ускладнює встановлення особи злочинця та його притягнення до відповідальності. Важливу роль у цьому відіграє міжнародна співпраця, зокрема в рамках Будапештської конвенції та діяльності Європолу й Інтерполу.

Правоохоронні органи та кібербезпекові структури використовують різні підходи для боротьби з розповсюдженням ШПЗ, серед яких:

1) використання аналітичних методів та штучного інтелекту для відстеження нових загроз;

2) створення законодавчих механізмів для блокування шкідливого контенту та платформ, що його поширюють;

3) посилення відповідальності за кіберзлочини та вдосконалення правозастосовних процедур.

Таким чином, боротьба з розповсюдженням шкідливого програмного забезпечення вимагає комплексного підходу, що включає як ефективне кримінальне переслідування винних осіб, так і запровадження превентивних заходів, спрямованих на зниження ризику використання ШПЗ. Важливу роль у цьому процесі відіграє міжнародна співпраця, оскільки більшість загроз у кіберпросторі мають глобальний характер.

Також важливо враховувати, що ефективність кримінально-правового регулювання відповідальності за розповсюдження ШПЗ значною мірою залежить від гармонізації національного законодавства з міжнародними стандартами. Зокрема, у межах Європейського Союзу директива 2013/40/ЄС «Про атаки на інформаційні системи» встановлює вимоги до криміналізації незаконного втручання в комп'ютерні системи, включаючи створення та розповсюдження шкідливого програмного забезпечення.

Водночас, практика кримінального переслідування кіберзлочинців свідчить про необхідність запровадження спеціальних слідчих методів, адаптованих до кіберпростору. Наприклад, у деяких країнах застосовуються так звані «контрольовані операції» (controlled delivery), які дозволяють правоохоронцям відстежувати розповсюдження шкідливого програмного забезпечення та виявляти ключових фігурантів кіберзлочинних угруповань.

Окрему проблему становить відповідальність за розповсюдження ШПЗ у випадках, коли його поширення здійснюється через децентралізовані платформи або у мережах даркнету. Через особливості анонімізації,

притягнення до відповідальності таких зловмисників стає надзвичайно складним. Одним із можливих рішень у цій сфері є застосування методів цифрового профілювання кіберзлочинців, що дозволяє ідентифікувати потенційних правопорушників на основі їхніх поведінкових шаблонів у мережі.

На міжнародному рівні варто також враховувати роль приватного сектору у боротьбі з розповсюдженням шкідливого програмного забезпечення. Такі технологічні гіганти, як Microsoft, Google та Amazon, активно співпрацюють із правоохоронними органами у справі блокування зловмисних серверів і видалення контенту, пов'язаного з кіберзлочинною діяльністю. Наприклад, у 2020 році корпорація Microsoft спільно з ФБР та Європолом здійснила успішну операцію з ліквідації ботнету TrickBot, який використовувався для поширення програм-вимагачів.

З огляду на ці виклики, удосконалення кримінально-правового регулювання у сфері розповсюдження ШПЗ потребує комплексного підходу, що включає:

1) удосконалення механізмів співпраці між державами у сфері екстрадиції та збору цифрових доказів;

2) розробку міжнародних стандартів кваліфікації кіберзлочинів для уніфікації підходів до кримінальної відповідальності;

3) використання новітніх технологій, включаючи штучний інтелект, для виявлення та нейтралізації шкідливих програм на ранніх етапах їх розповсюдження.

Таким чином, боротьба з розповсюдженням шкідливого програмного забезпечення виходить за межі традиційних підходів кримінального права і вимагає інтеграції технологічних, правозастосовних та міжнародних інструментів для забезпечення ефективного реагування на загрози у кіберпросторі.

4. Актуальні кейси міжнародного співробітництва у боротьбі з кіберзлочинністю

Злочинність у кіберпросторі давно перестала бути локальним явищем і набула глобального характеру, що вимагає від держав тісної співпраці у сфері розслідувань, обміну інформацією та екстрадиції правопорушників. З огляду на складність встановлення особи злочинця, транскордонний характер атак та анонімність цифрових технологій, боротьба з кіберзлочинністю є значним викликом для правоохоронних органів. Варто також проаналізувати найважливіші кейси міжнародного співробітництва у боротьбі з кіберзлочинами.

1. Операція "Bayonet": ліквідація найбільшого нелегального маркетплейсу AlphaBay

Одним із найбільш значущих прикладів міжнародного співробітництва стало закриття даркнет-маркетплейсу AlphaBay у 2017 році. Ця платформа діяла як глобальний чорний ринок для продажу наркотиків, викрадених даних, шкідливого програмного забезпечення та інших незаконних товарів і послуг. Розслідуванням займалися правоохоронні органи США, Європолу, Канади, Великої Британії, Нідерландів та Таїланду. Ключовим фактором успіху стало залучення технологій аналізу блокчейн-транзакцій та координація між країнами щодо арешту засновника сайту Олександра Казеса. Цей кейс

демонструє ефективність міжнародної співпраці у боротьбі з кіберзлочинами, що використовують криптовалютні платежі[13].

2. Операція "GHOST": затримання учасників кіберзлочинного угруповання REvil

Група REvil, відома атаками програм-вимагачів (ransomware), у 2020 – 2021 роках атакувала низку великих компаній та державних установ, включаючи постачальників критичної інфраструктури. Одним із найгучніших випадків стала атака на компанію Kaseya, яка вплинула на понад 1500 організацій по всьому світу. У відповідь на ці злочини було проведено міжнародну операцію "GHOST", організовану ФБР, Європолом та правоохоронними органами низки європейських держав. Унаслідок спільних дій у 2021 році було заарештовано кількох учасників угруповання, а сервери REvil були виведені з ладу. Операція стала показовою з точки зору координації дій спецслужб та обміну інформацією між різними юрисдикціями[14].

3. Ліквідація ботнету Emotet

Emotet вважався одним із найнебезпечніших ботнетів у світі, використовуваним для розповсюдження банківських троянів та програм-вимагачів. У 2021 році внаслідок міжнародної операції за участі правоохоронних органів США, Німеччини, Великої Британії, Нідерландів, Канади та України вдалося ліквідувати цей ботнет, а також заарештувати причетних осіб. Одним із ключових аспектів успіху операції стала розробка та впровадження механізму дезактивації шкідливого програмного забезпечення на заражених пристроях, що стало прецедентом у світовій практиці боротьби з кіберзлочинами[15].

Попри описані та деякі інші успішні кейси у боротьбі з кіберзлочинністю, міжнародне співробітництво стикається з низкою проблем серед яких:

1) юридичні бар'єри – відмінності у кримінальному законодавстві різних країн, що можуть ускладнювати екстрадицію та притягнення кіберзлочинців до відповідальності;

2) нестача оперативного обміну інформацією – не всі держави мають ефективні механізми взаємодії між правоохоронними органами;

3) використання юрисдикцій з низьким рівнем регулювання – багато хакерських угруповань базуються в країнах, де відсутні суворі закони щодо кіберзлочинності.

Ефективна боротьба з кіберзлочинністю вимагає подальшої інтеграції міжнародних зусиль, розширення повноважень інституцій, таких як Європол, Інтерпол та ФБР, а також вдосконалення механізмів спільного реагування. Приклад операцій "Bayonet", "GHOST" та ліквідації Emotet свідчить

[13] CybelAngel. Home. The Impact of Dark Web Marketplace Takedowns [AlphaBay and Hansa]. September 24, 2024. URL: https://cybelangel.com/alphabay-hansa-two-major-dark-web-marketplaces-shut/

[14] CSO. Home. Security REvil ransomware explained: A widespread extortion operation. 12 Nov 2021. URL: https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html

[15] EUROPOL. Home. Media & Press. World's most dangerous malware EMOTET disrupted through global action. 27 Jan 2021. URL: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

про необхідність комплексного підходу до протидії кіберзлочинам, який включає правозастосовні, технічні та дипломатичні інструменти.

Одним із перспективних напрямів міжнародного співробітництва у боротьбі з кіберзлочинністю є створення єдиних стандартів доказування у кіберсправах, що дозволило б уникнути проблем, пов'язаних із різними підходами до кваліфікації цифрових злочинів у національних правових системах. На сьогодні в рамках Європейського Союзу та ООН активно обговорюється питання розробки глобального механізму збору та визнання цифрових доказів, що стане вагомим кроком до гармонізації слідчих процесів у сфері кібербезпеки.

Крім того, сучасні тенденції міжнародної співпраці свідчать про посилення приватно-державного партнерства у боротьбі з кіберзлочинністю. Такі компанії, як Microsoft, Google, Amazon та інші технологічні гіганти, все частіше беруть участь у розслідуванні глобальних кіберзагроз, зокрема через надання інформації про підозрілі активності, підтримку ініціатив із блокування шкідливих серверів та спільні проєкти з правоохоронними органами.

Окремим викликом залишається регулювання криптовалютних транзакцій, які є основним фінансовим інструментом кіберзлочинців. Незважаючи на розвиток технологій відстеження цифрових активів, таких як Chainalysis або TRM Labs, існує потреба у створенні єдиних міжнародних стандартів контролю за нелегальними криптоопераціями. Деякі держави вже ухвалили відповідні нормативні акти, зокрема у США запроваджені нові вимоги до реєстрації криптовалютних бірж, що допомагають запобігати фінансуванню кіберзлочинності.

Ще одним напрямом міжнародної боротьби з кіберзлочинністю є розробка спільних механізмів реагування на атаки на критичну інфраструктуру. Зокрема, у 2022 році НАТО започаткувало ініціативу Cyber Rapid Reaction Teams, що передбачає можливість швидкого розгортання експертних груп для допомоги країнам-членам у разі масштабних кібератак[16]. Такий підхід може стати зразком для інших міжнародних об'єднань у сфері безпеки, адже він дозволяє не лише оперативно реагувати на загрози, а й напрацьовувати спільні практики цифрової форензіки.

Попри значний прогрес у міжнародному співробітництві, все ще залишаються невирішеними проблеми політичного та юридичного характеру. Багато країн неохоче діляться інформацією про кібератаки, побоюючись, що це може зашкодити їхній національній безпеці або репутації. До того ж, деякі держави використовують кіберзлочинність як інструмент гібридної війни, що ускладнює глобальну координацію у боротьбі з такими загрозами.

З огляду на зазначене, подальша ефективність міжнародного співробітництва у сфері кіберзлочинності залежатиме від удосконалення нормативно-правової бази, зміцнення партнерства між державами та приватним сектором, а також активного впровадження інноваційних технологій для ідентифікації та нейтралізації кіберзлочинних угруповань.

[16] North Atlantic Treaty Organization (NATO). NATO Rapid Reaction Team to fight cyber attack. 13 Mar. 2012. URL: https://www.nato.int/cps/en/natolive/news_85161.htm

ВИСНОВКИ

У сучасних умовах глобальної цифровізації та зростання залежності суспільства від інформаційно-комунікаційних технологій кіберзлочинність стала однією з найбільш актуальних загроз національній та міжнародній безпеці. Кібератаки на критичну інфраструктуру, поширення шкідливого програмного забезпечення та необхідність міжнародного співробітництва у боротьбі з кіберзлочинністю є ключовими викликами, що потребують невідкладної реакції з боку державних органів, правоохоронних структур та міжнародних організацій.

Насамперед, розгляд проблем правозастосування у сфері кібератак на критичну інфраструктуру засвідчив, що чинне законодавство України та міжнародні нормативні акти не завжди відповідають динаміці розвитку кіберзагроз. Наявні правові механізми часто виявляються недостатньо ефективними для забезпечення належного рівня захисту об'єктів критичної інфраструктури, що стають мішенню зловмисників. Аналіз сучасної практики правозастосування демонструє необхідність удосконалення кримінального законодавства, зокрема чіткішого визначення складів злочинів, пов'язаних із кібератаками, розширення повноважень правоохоронних органів у сфері розслідування кіберзлочинів, а також розробки єдиних стандартів кібербезпеки для критичних об'єктів.

Другим важливим аспектом дослідження є кримінально-правова відповідальність за розповсюдження шкідливого програмного забезпечення, яка передбачена Кримінальним кодексом України. Проте аналіз законодавчих норм показав, що існує низка проблем, пов'язаних із доказуванням умислу правопорушників, класифікацією програмного забезпечення як шкідливого та встановленням його реального впливу на інформаційні системи. Крім того, в умовах анонімності та транснаціонального характеру кіберзлочинності існує складність у притягненні винних осіб до відповідальності, особливо якщо вони перебувають поза межами юрисдикції України. У зв'язку з цим актуальним є посилення міжнародної співпраці у сфері кібербезпеки, гармонізація національного законодавства з міжнародними стандартами та створення ефективних механізмів екстрадиції кіберзлочинців.

Окремо було розглянуто актуальні кейси міжнародного співробітництва у боротьбі з кіберзлочинністю, що підтвердило ключову роль спільних зусиль держав у протидії кіберзагрозам. Практика діяльності таких організацій, як Інтерпол, Європол, НАТО та ООН, свідчить про ефективність міжнародних ініціатив, спрямованих на обмін інформацією, проведення спільних розслідувань та розробку глобальних стандартів кібербезпеки. Зокрема, успішні операції з викриття кіберзлочинних угруповань, таких як «Emotet» та «REvil», продемонстрували важливість міжнародної взаємодії та необхідність розширення договірної бази для боротьби з транснаціональною кіберзлочинністю.

Таким чином, дослідження засвідчило, що боротьба з кіберзлочинністю вимагає комплексного підходу, що включає вдосконалення кримінального законодавства, посилення правоохоронних механізмів, забезпечення надійного захисту критичної інфраструктури, а також активну міжнародну співпрацю. Вирішення зазначених проблем потребує не лише законодавчих змін, а й

запровадження інноваційних технічних рішень, підвищення рівня цифрової грамотності населення та створення єдиної глобальної стратегії кібербезпеки. Подальший розвиток цієї сфери має ґрунтуватися на принципах правової визначеності, міжнародної солідарності та технологічної адаптивності, що дозволить ефективно протидіяти кіберзлочинам в Україні.

АНОТАЦІЯ

У статті здійснено комплексний аналіз сучасних викликів кримінально-правового регулювання кіберзлочинності в національному та міжнародному вимірах. Досліджено проблеми правозастосування щодо кібератак на об'єкти критичної інфраструктури, зокрема труднощі кваліфікації таких діянь, особливості збору й використання цифрових доказів, а також недосконаліть окремих положень кримінального та кримінального процесуального законодавства України. Проаналізовано питання кримінальної відповідальності за створення та розповсюдження шкідливого програмного забезпечення, акцентовано увагу на проблемі доведення умислу та подвійного призначення окремих програмних засобів. Окремо розглянуто актуальні кейси міжнародного співробітництва у боротьбі з кіберзлочинністю (ліквідація AlphaBay, REvil, Emotet), які демонструють ефективність координації між державами, міжнародними організаціями та приватним сектором.

Обґрунтовано необхідність удосконалення національного законодавства з урахуванням міжнародних стандартів, гармонізації підходів до криміналізації кіберзлочинів, розширення механізмів міжнародної правової допомоги та впровадження сучасних технологій цифрової форензіки. Зроблено висновок про потребу формування комплексної моделі протидії кіберзлочинності, що поєднує кримінально-правові, процесуальні, організаційні та технологічні інструменти в умовах глобальної цифровізації.

Література

1. Аніщук В. В., Зицик С. Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського Національного Університету. 2024. Серія ПРАВО.* Випуск 83: частина 3, С. 19-23. DOI https://doi.org/10.24144/2307-3322.2024.83.3.2

2. Степаненко Н. В., Піддубний Д. Д. Сучасні проблеми запобігання і протидії злочинності у сфері інформаційних технологій. *Legal Bulletin.* 2024, 73-81. https://doi.org/10.31732/2708-339X-2024-14-A10

3. Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ "КПІ" Політологія. Соціологія. Право.* № 1(49) (2021). DOI: https://doi.org/10.20535/2308-5053.2021.1(49).233023

4. Авдєєва, Г., Живуцька-Козловська, Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*, Вип. 1 (30), 2023. 126-143. https://doi.org/10.32353/khrife.1.2023.07

5. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека,* 2 (93), 2024. 140-150. https://doi.org/10.32631/pb.2024.2.13

6. Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО.* Вип. 75: ч. 2. 2023. 158-162. https://doi.org/10.24144/2307-3322.2022.75.2.25

7. Sergiu Cernomoreț & Andrei Nastas. Comparative Analysis of Cybercrime in the Criminal Law System. International Academic Publisher. Bucharest, Paris, Calgary 2023. 82 p. URL: https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf

8. Senjaya, Murshal. Cyber Crime And Criminal Law In The Era Of Artificial Intelligence. *International Journal of Law and Society.* 1, 2024. 268-276. DOI: https://doi.org/10.62951/ijls.v1i4.210

9. Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis (March 20, 2022). Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2), 2022. 74-79. http://dx.doi.org/10.2139/ssrn.4061947

10. Верховна Рада України. Розділ: Законодавство України. Кримінальний кодекс України. 5 квітня 2001 року, № 2341-III. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 13.03.2025).

11. Верховна Рада України. Розділ: Законодавство України. Кримінальний процесуальний кодекс України. 13 квітня 2012 року, № 4651-VI. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 13.03.2025).

12. International Standard ISO/IEC 27037. Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

13. H-X. Директива кібербезпеки NIS2. *Електронний ресурс.* URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua

14. Верховна Рада України. Розділ: Законодавство України. Закон України «Про основні засади забезпечення кібербезпеки України». 5 жовтня 2017 року № 2163-VIII. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 13.03.2025).

15. CybelAngel. Home. The Impact of Dark Web Marketplace Takedowns [AlphaBay and Hansa]. September 24, 2024. URL: https://cybelangel.com/alphabay-hansa-two-major-dark-web-marketplaces-shut/

16. CSO. Home. Security REvil ransomware explained: A widespread extortion operation. 12 Nov 2021. URL: https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html

17. EUROPOL. Home. Media & Press. World's most dangerous malware EMOTET disrupted through global action. 27 Jan 2021. URL: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

18. North Atlantic Treaty Organization (NATO). NATO Rapid Reaction Team to fight cyber attack. 13 Mar. 2012. URL: https://www.nato.int/cps/en/natolive/news_85161.htm

Information about the author:
Larchenko Maryna Oleksandrivna,
Candidate of Juridical Sciences (Ph. D.), Associate Professor,
Associate Professor at the Department of Cyber Security
and Mathematical Modeling,
Educational and Scientific Institute of Electronics
and Information Technologies,
Chernihiv Polytechnic National University
95, Shevchenko Str., Chernihiv, 14030, Ukraine,
Associate Professor at the Department of
Law and Social and Philosophical Sciences
Faculty of Philology, History and Political and Legal Sciences,
Mykola Gogol Nizhyn State University
2 Grafska Str., Nizhyn, 16600, Ukraine
https://orcid.org/0000-0002-2643-980X

DOI https://doi.org/10.30525/978-9934-26-686-7-11

OSINT TECHNOLOGIES IN LAW ENFORCEMENT: INNOVATIONS AND AREAS OF APPLICATION DURING MARTIAL LAW AND THE COUNTRY'S POST-WAR RECOVERY

Nehrebetskyi V.V.

INTRODUCTION

Modern armed conflicts have radically transformed not only the conduct of hostilities but also the ways in which they are documented and proved in criminal proceedings. The digitalization of communications; the mass availability of mobile devices with cameras, livestreams, and geolocation services; the development of satellite observation; and the emergence of new data-sharing platforms have created an unprecedentedly dense information environment. In such an environment, open sources − social networks, video hosting platforms, web archives, satellite platforms, state registers, and other digital resources − become a fully-fledged basis for building the evidentiary record.

Since the start of the full-scale war, the intensity and diversity of digital traces of war crimes have increased sharply. Videos and photos of the aftermath of shelling, fragments of live broadcasts from the scene, eyewitness accounts on social media, Telegram channels, and arrays of satellite observation have, in near-real time, formed a new evidentiary base for law enforcement agencies. The search for reliable tools to identify those involved in war crimes, to localize the places where they were committed, and to verify causal links naturally directed domestic law enforcement agencies to OSINT as a practice-tested, systematized approach to working with open digital data.

A key advantage of OSINT is the speed and scalability of event capture. This is not only about the 'first alert' from social networks, but also about the ability to build spatio-temporal reconstructions: geolocating frames by distinctive terrain features; comparing them with before/after satellite series; overlaying them with air-raid chronicles or systematic time stamps to narrow the 'time window' to procedurally acceptable limits. Given the limited access to crime scenes in active combat zones, these methods have become a bridge between operational response and subsequent 'classic' investigative and procedural actions.

OSINT has catalyzed interagency interaction and international cooperation. Joint analytical projects, consolidation of verified geolocations in open databases, and the exchange of methodologies and tools with civic initiatives and academic centers have created an 'ecosystem of trust' in which quality standards are gradually being unified[1]. Thus, the turn to OSINT has not been a situational response to the lack of access to scenes, but an element of the structural modernization of law enforcement

[1] OSINT-розвідка у роботі журналістів. URL: https://youcontrol.com.ua/articles/osint-in-journalists-work/

in the digital era, ensuring both promptness and legal viability of evidence during wartime and the post-war period.

The use of modern information technologies, including open-source information gathering, in criminal proceedings has been the focus of academic events and the works of many legal scholars as G. K. Avdeeva, V. S. Batyrgareeva, V. I. Borisov, T. Ya.Gnidets, O. M. Borshchevskaya, S. S. Voznyuk, V. I. Grishko, Yu. I. Dmitrik, I. V. Zhukevich, I. O. Osnova, K. V. Dubonos, N. M. Dyachenko, V. A. Zhuravel, V. P. Zakharov, A. O. Ignatovich, O. Ya. Kovalchuk, R. S. Kozyakov, V. O. Konovalova, T. M. Lemekha, a.m. Lysenko, O. A. Lokhmatov, T. V. Ognevyuk, O. S. Mel-nik, A. O. Moroz, I. V. Oleshko, Yu.V.Osadchaya, O. V. Plahotnik, Yu. S. Razmetaeva, O. V. Rybalsky, V. I. Rudeshko, V. I. Solovyov, L. I. Sopilnik, A.V. Stolitny, I. O. Suprun, E. A. Timoshenko, V. I. Teremetsky, V. V. Topchy, A. O. Fesenko, V. G. Khakhanovsky, L. M. Khmelnichy, R. Yu. Tsarev, V. A. Shvets, V. M. Shevchuk, V. Yu. Shepitko, and others[2].

It should be noted that OSINT technologies for detecting and collecting evidentiary information have been covered in the literature from different angles. However, in our view, it is crucial and timely to comprehensively explore the possibilities of implementing OSINT technologies into the procedural activities of criminal justice bodies, considering their innovative potential, functional capabilities, and application areas specifically under the conditions of war in Ukraine. Therefore, studying the trends and potential of OSINT technologies in the applied aspect for the activities of criminal justice authorities and the security and defense sector of Ukraine in investigating and preventing criminal offenses requires further consideration. Given the war, the use of OSINT in investigative units to increase the effectiveness of investigating war crimes and crimes of aggression is particularly urgent.

Accordingly, examining international experience in using OSINT is relevant and, given the need to improve regulatory frameworks in Ukraine, fully justified.

1. Challenges of Regulating the Use of Digital Evidence Technologies During Wartime

From the outset of the full-scale war against Ukraine, the search for tools to identify the perpetrators of war crimes, the locations of such crimes, and information that had surfaced online led domestic law enforcement to OSINT.

The efforts of the Prosecutor General's Office, the Security Service of Ukraine, the National Police of Ukraine, as well as scholars and human rights defenders aimed at

[2] Трансформація завдань криміналістики в умовах воєнного стану та євроінтеграційних процесів : зб. матеріалів наук.-практ. конф. присвяч. пам'яті д-ра юрид. наук, проф. В.О. Коновалової,м. Харків, 28 берез. 2024 р. Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2024; *Методологічні засади криміналістики: традиції та новації* : зб. матеріалів Криміналістичних читань, присвяч.пам'яті акад. В. О. Коновалової, м. Харків, 28 берез. 2025 р. Нац. юрид. ун-т ім. Ярослава Мудрого,Каф. криміналістики; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В.Сташиса Нац. акад. прав. наук України. Харків: Право, 2025; *Роль OSINT-досліджень у підвищенні рівня національної безпеки України* : матеріали круглого столу (м. Львів,7 травня 2025 р.) Львів: ЛьвДУВС, 2025.

introducing OSINT into the practice of detecting and investigating war crimes deserve positive assessment. On 12–13 January 2026, in cooperation with the Training Center for Prosecutors of Ukraine and the National School of Judges, with the support of the Council of Europe's CyberUA project, a specialized training on the use of open sources (OSINT) and electronic evidence in criminal proceedings − focused on cases concerning war crimes and gross human rights violations − was held[3].

First of all, the requirements for electronic evidence under national criminal procedure law and international standards − particularly the Berkeley Protocol − were discussed. The participants reviewed typical categories of open sources and types of electronic evidence and examined procedures for ensuring the chain of custody for electronic evidence in detail.

In 2020, the Office of the UN High Commissioner for Human Rights and the Human Rights Center at UC Berkeley presented a «practical guide on the effective use of digital open-source information for investigating violations of international criminal, human rights, and humanitarian law» that sets out standards and methodological approaches for the collection, preservation, and analysis of open-source information that may be presented as evidence in criminal proceedings[4]. Unfortunately, Ukraine's Criminal Procedure Code does not provide a separate category of digital evidence. It lacks a definition of «digital evidence» and a detailed procedure for its seizure, examination, recording, and storage. Investigators and judges often face difficulties collecting and assessing digital evidence due to the absence of definitions and procedures in Ukrainian law, which may lead to errors and inadmissibility in court[5].

Therefore, leveraging the experience of leading European countries − engaging specialized research institutions and legal experts − to align current criminal procedure law with the demands of the digital era is essential.

The participants also discussed the role of a specialist in OSINT investigations: from proper acquisition and recording of data to explaining technical aspects to the court (metadata, hash values, file validation, detection of editing, etc.). It was emphasized that proper documentation of specialist involvement during inspection when using OSINT in criminal proceedings is important.

Of particular interest was the block on expedited preservation of data under Articles 16–17 of the Budapest Convention on Cybercrime, which allows electronic data to be preserved prior to obtaining proper procedural access. The network of 24/7 contact points, drafting preservation requests, and using mutual legal assistance mechanisms (MLA) to obtain electronic evidence were also discussed.

---

[3] OSINT та електронні докази: юридичні вимоги та практика застосування у кримінальних провадженнях щодо воєнних злочинів в Україні. 14.01.2026. URL: https://www.coe.int/uk/web/kyiv/-/osint-and-electronic-evidence-legal-requirements-and-practical-application-in-criminal-proceedings-on-war-crimes-in-ukraine

[4] Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

[5] Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США (2023). URL: https://khrife-journal.org/index.php/journal/article/download/564/633.

Practice-oriented trainings were also conducted within the Ministry of Internal Affairs system. In October 2025, investigators and operatives of the National Police of Ukraine were trained to master the skills of collecting and using information from publicly available sources in proving war crimes[6]. As part of implementing the UN–Ukraine framework to prevent and combat conflict-related sexual violence, the MIA Human Rights Monitoring Office organized two two-day offline trainings for investigators and operatives on «Using OSINT to Prove Command Responsibility for International Crimes: Theory and Practice».

OSINT not only enables the collection of evidence under conditions of limited access, but also creates the foundation for building evidentiary records in cases concerning war crimes and crimes against humanity, consistent with national and international investigative standards.

The training was organized by the Human Rights Monitoring Department of the Ministry of Internal Affairs of Ukraine and the National Police of Ukraine with the support of the United Nations Development Programme (UNDP) within the framework of the UNDP project «Joint Programme for Ukraine on conflict-related sexual violence Issues», which is funded by the European Union.

During war, the arsenal of traditional forensic tools and forms of collecting evidence of war crimes in Ukraine is significantly limited due to danger to all participants in investigative actions and the impossibility of direct access to the scene[7], necessitating the use of artificial intelligence technologies. Moreover, the European vector of development of forensics and forensic examination in Ukraine is evidenced by the application of European standards of proof during criminal proceedings[8].

By Presidential Decree No. 273/2023 of 11 May 2023, a Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as part of the Security and Defense Sector for 2023–2027 was approved[9]. «Every element of the state system – law enforcement agencies, first of all – must work so that people really feel safe and secure, so that people really feel justice, so that it is guaranteed at the level of institutions, at the level of the everyday work of those by whom people judge the state. Trust in the state, trust in the state are formed from trust in those who act on behalf of the state. Law enforcement officers, the prosecutor's office system are key

[6] Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: навчання НПУ. 08.10.2025.URL: https://npu.gov.ua/news/vykorystannia-osint-u-dokazuvanni-komandnoi-vidpovidalnosti-za-mizhnarodni-zlochyny-navchannia-npu

[7] Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374. DOI: 10.32782/2524–0374/2022–4/88

[8] Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України.* 2022. № 2. С. 87.

[9] Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

in this. Of course, together with everyone else who works in the state apparatus,» emphasized President Volodymyr Zelenskyy[10].

The document was jointly developed by an interagency group, which included the heads of the Prosecutor General's Office, the Ministry of Internal Affairs, the Ministry of Justice, the Security Service of Ukraine, the State Bureau of Investigation, the National Police, the State Border Service, the Border Guard Service, the State Customs Service, as well as representatives of the Office of the President of Ukraine, the Cabinet of Ministers of Ukraine, international experts from the Council of Europe Office in Ukraine, the EUAM, the EU project «PRAVO-JUSTICE», the Law Enforcement Affairs Department of the US Embassy in Ukraine, and the International Development Law Organization (IDLO).

The main goal of the developers of the Plan was to put the focus of the law enforcement, security and defense sectors on the person, his life, health, honor and dignity, rights and legally protected interests. Every Ukrainian should be sure that he lives in safety, has freedom and can count on the mechanisms of justice.

The plan identifies six strategic priorities that will allow modernizing the security sector and bringing it into line with the standards that Ukraine must achieve on its path to EU membership, including:

1. Effectiveness and efficiency of law enforcement agencies and the prosecutor's office as an integral part of the security and defense sector, within which they ensure the national security of Ukraine, including public safety and order, and combat crime, taking into account strategic goals and in accordance with the standards of human rights and fundamental freedoms, including ensuring gender equality.

2. Consistent criminal policy, the priority of which is the prevention of crime, the inevitability of liability, the protection of the individual, society and the state from criminal offenses, and the protection of the interests of the victim.

3. Efficiency of criminal proceedings in compliance with international standards and the rule of law.

4. A result-oriented management system in accordance with established priorities.

5. Comprehensive digital transformation.

6. Openness, transparency, accountability and independence.

The plan provides for a comprehensive digital transformation, in particular:

1. Implementation of a consolidated phased digital transformation of law enforcement agencies and the prosecutor's office based on strategic management tools that comply with EU best practices.

2. Further introduction of innovative technological achievements into the activities of law enforcement agencies and the prosecutor's office that ensure flexibility of operational processes, IT solutions, digital ability to respond promptly to events and changes and achieve results focused on the interests of society.

3. Phased implementation of an electronic system for managing criminal proceedings through comprehensive replacement and modernization of equipment,

[10] Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku.

ensuring compatibility of IT systems, uninterrupted operation, access of all participants in criminal proceedings and interoperability.

4. Increasing the efficiency of law enforcement agencies and the prosecutor's office by ensuring greater accessibility and completeness of information, development and implementation of services on the Unified State Web Portal of Electronic Services.

5. Implementation of security and personal data protection measures in accordance with EU standards.

6. Improvement and implementation of more secure, flexible, capable and accessible communication systems between all law enforcement agencies and other emergency services (including digital radio: voice communication and broadband data transmission).

7. Implementation of a unified personal authentication system and biometric matching system in all law enforcement agencies and prosecutors' offices, gradually ensuring its compatibility with European systems. Widespread use of artificial intelligence, blockchain, cloud computing and other innovative solutions in pre-trial investigations, as well as for data processing and analytical activities of law enforcement agencies and prosecutors' offices.

8. Updating operational processes using IT systems suitable for data exchange with EU institutions in accordance with EU standards.

9. Granting law enforcement agencies and prosecutors the right to direct shared access to automated information and reference systems, registers and databases, the holder (administrator) of which is other state bodies, to ensure the performance of their functions[11].

2. Using Digital Technologies and Open-Source Data in Investigating War Crimes

In today's realities of war and global threats, all practitioners in the field of international criminal justice must improve their technical understanding of cutting-edge AI technologies and cultivate a deeper, up-to-date understanding of how social networks, geolocations, mobile communications, computer information, and other digital traces and communications are used in conflict zones[12]. Given the aggressor state's actions in Ukraine − mass killings, rapes, looting − the problem of collecting evidence of war crimes is acute and requires greater use of AI technologies in detecting, documenting, and investigating war crimes, crimes against humanity, and genocide.

The investigation and documentation of war crimes in Ukraine is the most important line of work for criminal justice bodies. Decisive factors include professional, high-quality, complete, comprehensive, admissible, timely, and proper

[11] Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

[12] Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності:* мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

documentation of all elements of a war crime. As of 20 January 2026, the Prosecutor General's Office has registered over 216,000 instances of crimes of aggression and war crimes committed during the full-scale invasion, with numerous cases of destruction of residential infrastructure, killings of civilians, looting, and violence documented[13]. The collected evidence will later make it possible not only to prove that these crimes were committed, but also to connect them to specific individuals, bring well-founded charges, and hold perpetrators accountable. Personal accounts of people who suffered violence and inhuman treatment, widely documented and disseminated, draw public attention to the intolerable armed conflict and enable the development of new recommendations and mechanisms for human rights protection.

OSINT plays a major role in documenting gross human rights violations and war crimes. Non-governmental organizations such as Bellingcat[14], Amnesty International, and Human Rights Watch have become pioneers in using open data to investigate events in conflict zones where access for official investigators is limited or impossible. By analyzing satellite imagery, social media videos, and public registers, these organizations have debunked official narratives and provided evidence for international courts.

A milestone that legitimized OSINT as an evidentiary tool was the judgment of the European Court of Human Rights in Ukraine and the Netherlands v. Russia (2022). In this decision, the Court for the first time recognized data obtained from open sources (in particular, Bellingcat's investigation of the downing of flight MH17) as full-fledged and reliable evidence.

The court formulated three key criteria for assessing such evidence:

– the authority and experience of the source (the research team must have recognized competence in the relevant1 field);

– transparency of the methodology (a clear description of how the information was collected, verified and stored);

– consistency with other evidence (coincidence of OSINT data with official investigation results, eyewitness accounts or other materials)[15].

National courts have repeatedly referred to OSINT materials as a means of obtaining information necessary for investigating criminal offenses.Thus, in the Ivano-Frankivsk City Court, OSINT was used to prove guilt in collaboration activities (case No. 344/19008/24). The court referred to the report of the operational officer, which indicated the analysis of information from open sources, in particular the social network «Vkontakte», to establish the fact of cooperation of a person with the occupation authorities. The verdict noted: "…during the implementation of counterintelligence activities, information was obtained regarding the unlawful actions of a citizen of Ukraine PERSON_7… acting to the detriment of sovereignty… went over to the enemy's side under martial law… according to the OSINT analysis of materials about the individual N 4/1-2350 dated 09/29/2022, she

[13] Злочини, вчинені в період повномасштабного вторгнення рф станом на 20.02.26. URL: https://www.gp.gov.ua/

[14] Bellingcat. URL: https://www.bellingcat.com/

[15] Радейко Р. І. Інструментарії OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400–410. DOI: https://doi.org/10.5281/zenodo.15648723

was a cadet of the Luhansk State University of Internal Affairs, worked as a police officer in the response sector of the patrol police at ADDRESS_2" (Verdict dated 05/12/2024 No. 344/19008/24 Ivano-Frankivsk City Court)[16].

2. In the Osnovyanskyi District Court of Kharkiv, the term OSINT was directly used to designate a method of identifying a person who transmitted the coordinates of the Armed Forces of Ukraine to the enemy (case No. 643/6925/24). The verdict states: "…who is registered to the number of the Ukrainian mobile operator NUMBER_Z and belongs to a citizen of Ukraine PERSON_5... whose identity was established using the capabilities of OSINT analytics" (Verdict of the Osnovyanskyi District Court of Kharkiv dated June 10, 2025 in case No. 643/6925/24)[17].

Analysis of these decisions shows that OSINT results are presented in criminal proceedings as OSINT-analysis memos, extracts from open-source intelligence, OSINT dossiers on individuals, and protocols of computer data inspection. In most decisions, references are made not to a document as the source of OSINT data, but to the results or sources gathered through OSINT[18]. This practice arises from the lack of a definition of OSINT as a tool for obtaining information on the circumstances of a criminal offense in current legislation, which, in our view, contradicts the principle of legal certainty in criminal procedure and in the activities of authorized bodies for detecting and investigating criminal offenses.

In today's realities of war and global threats, all practitioners in international criminal justice must improve their technical understanding of emerging artificial intelligence technologies and must cultivate a deeper contemporary understanding of the applications of how social media, geolocation, mobile phone conversations, computer information, and other digital traces and communications are used in war zones[19]. Given the military aggression on the territory of Ukraine and the commission of mass murders, rapes, and looting, the problem of collecting evidence of war crimes is acute today. This requires the activation and expansion of the use of artificial intelligence technologies in the detection, documentation, and investigation of war crimes, crimes against humanity, and genocide.

The use of OSINT technologies in the investigation of war crimes in Ukraine can be useful in many aspects. The main areas in which this technology can be used are as follows:

---

[16] Вирок Івано-Франківського міського суду Івано-Франківської області від 05 грудня 2024 року у справі № 344/19008/24. URL: https://reyestr.court.gov.ua/Review/123535737

[17] Вирок Основ'янського районного суду міста Харкова від 10 червня 2025 року у справі № 643/6925/24. URL: https://reyestr.court.gov.ua/Review/127999232.

[18] Кудінов С. С., Шехавцов Р. М. Правове регулювання використання osint та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126–133. URL: https://doi.org/10.32782/2311-8040/2025-3-14. http://journals.lvduvs.lviv.ua/index.php/law/article/view/1013

[19] Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності:* мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

Satellite imagery analysis. Artificial intelligence can help analyze large volumes of satellite imagery to identify changes in the landscape, including buildings, roads, and infrastructure, that may be linked to war crimes, as well as help identify locations where the bodies of war crimes victims may be buried[20];

Video and photo analysis. Artificial intelligence can be used to analyze large volumes of video and photo materials that were filmed at war crimes sites, which, in turn, can help identify suspects and witnesses, as well as determine whether they depict objects that may contain forensically significant information for investigating such crimes[21];

Audio processing. In telephone recordings and during the processing of audio materials for war crimes investigations, artificial intelligence can help identify voices contained in such media, as well as determine the places where these conversations took place;

Social media analysis[22]. By analyzing social media, AI can help uncover connections between suspects who may be involved in war crimes and identify individuals who may have witnessed or had information about war crimes[23];

analysis of data from medical institutions. Artificial intelligence can help in identifying the bodies of war crime victims, establishing the cause of death, identifying prisoners of war, war criminals and searching for them based on disease data and information about their identification features that help in identifying a specific person[24];

Facial recognition. Artificial intelligence can be used to recognize faces in photos and videos from war crimes scenes. This can help identify suspects involved in committing such crimes and identify witnesses who can provide important information about the war crime event under investigation;

Textual information analysis. Artificial intelligence analysis of textual information (e.g., social media posts and other sources) related to war crimes will

---

[20] Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

[21] Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, – LIGA.net URL: https://tech.liga.net/ua/ukraine/novosti/iskusstvennyy-intellekt-mintsifry-razoblachil-okkupanta-popavshego-v-gospitalv-krivom-roge

[22] Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

[23] Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С.142–146.

[24] Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL:. https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogiluukrayinskih-vijskovih-ta-ponad-460-novih-mogil-foto

help identify suspects and witnesses and uncover forensically significant information about war crimes under investigation[25].

Modern approaches to the investigation of war crimes make it possible to identify sources of digital information that determine the directions of collecting and studying digital traces to obtain information: from mobile devices, phones seized from participants in criminal proceedings; from personal computers of individuals and legal entities; from servers and other information storage devices in organizations and institutions; from radio frequency identifiers, GPS trackers, sensors, stationary and mobile measuring devices using geolocation, video surveillance and positioning systems; from network services that provide voice and video communication between computers via the Internet (ICQ, Skype, WhatsApp, Viber, Telegram, etc.); from banking systems on digital media (HDD, SSD, flash cards, etc.); from cellular operators regarding the detailing of subscriber communication and determining the location of the subscriber using geolocation; from recordings of video surveillance cameras of commercial and government structures; from the cameras and video cameras seized from the participants in the criminal proceedings.

By the same algorithm, OSINT debunks myths about the so-called «special operation» and «invincible» soldiers. Technologies recognize the faces of deceased occupiers and locate their social media profiles; autodialers inform relatives of their deaths. Ukraine's Ministry of Defense has also begun using Clearview AI facial recognition to identify Russian attackers, combat disinformation, and identify the dead and war criminals[26]. In the military realities of a full-scale war on the territory of Ukraine, digital forensics tools significantly assist in the detection, disclosure, and investigation of war crimes.

Geo-OSINT is a subtype of open-source intelligence that specializes in collecting, processing, analyzing, and interpreting geospatial data obtained from open sources. In contemporary forensics, security, intelligence work, and investigative journalism, Geo-OSINT is gaining strategic importance as a tool for obtaining evidence, verifying information, and building situational awareness. Unlike «classic» OSINT, which covers a wide spectrum of open information, Geo-OSINT focuses on data with a geographic reference.

Sources include:

– satellite imagery (Sentinel, Landsat, Maxar);
– digital maps (Google Maps, OpenStreetMap, Bing Maps);
– image/video geotags (EXIF);
– route data (GPS tracks, AIS, ADS-B);
– geolocated social media (Twitter, Instagram, TikTok);
– crowdsourcing platforms (Mapillary, Wikimapia);

[25] Шевчук В.М. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі*: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2024. 208 с. С. 89.

[26] Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі ? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

– open GIS databases [27].

Geo-OSINT consists in identifying spatial relationships among objects, events, and actions based on location, time of capture, and context. For example, combining a satellite image with a geotagged social media video allows one to confirm an event or track the movement of equipment, people, and weapons. Scientifically, Geo-OSINT combines elements of geoinformatics, forensics, digital forensics, information analytics, and law.

With Geo-OSINT, investigators can:

- track routes of suspects and vehicles;
- identify crime scenes;
- establish links among locations, events, and objects;
- reconstruct chronologies from geolocation data;
- monitor changes in terrain using satellite imagery over time[28].

In forensics, Geo-OSINT can:

- verify testimony (e.g., confirming a person's presence at a specific place);
- track criminal groups via their digital footprints in public space;
- create crime maps to analyze hot spots;
- model scenarios in space and time[29].

Geo-OSINT commonly uses:

- satellite visualization services (Sentinel Hub, Google Earth Pro, Zoom Earth);
- geoanalytical platforms (ArcGIS, QGIS, MapInfo);
- tools for extracting coordinates from images (ExifTool, FotoForensics);
- social media monitoring systems with geotag filtering (GeoSocial Footprint, Hootsuite, Maltego)[30].

Geo-OSINT has become popular among military analysts, investigators and detectives, and the State Border Guard Service, particularly in war-crimes investigations. For example, geolocation analysis of social media photos allowed Bellingcat investigators to confirm movements of military equipment during armed conflicts.

---

[27] Батанов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану : дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. С.7.

[28] Кисельов А. О. Тактика спілкування поліцейського з особами. The Top Actual Researches in Modern

Science: Proceedings of the IInd International Scientific and Practical Conference (Ajman, July 28- 29, 2016,

UAE). International Scientific and Practical Conference «World Science». 2016. № 8 (12). P. 23.

[29] Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики: матеріали Всеукр. наук.-практ. конф. : у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро: Дніпроп.держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

[30] Москаленко Я. , Кривошея Д. , Дейкун О, Кисельов А. Гео-OSINT в кримінальному аналізі. Collection of Scientific Papers «SCIENTIA», (May 30, 2025; Glasgow, Scotland, UK). С.89.

3. Ensuring Authenticity and Admissibility of Digital Open-Source Evidence in Criminal Justice

Proper handling of the evidentiary base − detection, collection, documentation, and investigation of war crimes − must be carried out with due regard to international experience and European standards of proof[31]. At the same time, one problem in using OSINT during pre-trial investigation is the risk of human-rights infringements (privacy and data protection). We should not overstate the potential and advantages of these technologies and must pay attention to their drawbacks. OSINT is acceptable in law enforcement and justice only if fundamental rights and rule-of-law principles are strictly respected − human dignity, equality before the law and the court, adversarial process, transparency, proportionality, fairness, and impartiality.

Using open sources in investigating war crimes is accompanied by complex ethical, legal, and procedural challenges that demand a particularly cautious approach. Unlike traditional methods, OSINT relies on data created, disseminated, or collected beyond state procedural control − by private individuals, journalists, volunteers, or even actors pursuing propaganda goals. This increases evidentiary potential but simultaneously creates risks of privacy breaches, exposure of witnesses, dissemination of traumatic content, and the spread of unverified or manipulative materials. For this reason, the Berkeley Protocol emphasizes the need to adhere to professional, methodological, and ethical principles when working with open sources, especially in the context of international crimes.

A single key postulate for the admissibility of open-source data is the protection of the accused's rights and a fair trial (para. 55 of the Berkeley Protocol)[32]. The Protocol is a practical guide developed by UC Berkeley School of Law together with the UN, setting international standards for online investigations into alleged violations of international human rights, humanitarian, and criminal law, and providing guidance on methodologies and procedures for the collection, analysis, and preservation of digital information in a professional, legal, and ethical manner. The Berkeley Protocol was developed with input from individuals with diverse professional perspectives, legal and cultural backgrounds, gender and nationality, and involved over 150 expert consultations and input from key stakeholders, including UN human rights investigators. Building on this collaborative approach, the Berkeley Protocol includes international standards for conducting online investigations into alleged violations of international human rights law, international humanitarian law and criminal law. It also provides guidance on methodologies and procedures for collecting, analyzing and preserving digital information in a professional, legal and ethical manner.

[31] Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. *Використання цифрових технологій у криміналістиці та судовій експертизі :* матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К . Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. С ташиса НАПрН України. Харків: Право, 2024. С. 133–136.

[32] Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

In this context, Articles 6(2) and 8 of the European Convention on Human Rights are fundamental[33]. Одним із ключових етичних вимірів є питання *приватності* та *пропорційності*. One key ethical dimension is privacy and proportionality. An OSINT researcher inevitably deals with data that may contain personal information: faces, voices, locations, household details, behaviors, and social ties. The use of such material must be necessary to achieve a specific procedural purpose, and the intrusion must be proportionate. If identifying a person is not critical, it is appropriate to limit oneself to group or role attribution; if content contains data that may endanger an individual, depersonalization, blurring, or partial redaction should be used. These approaches are reflected in the Berkeley Protocol, which underscores that safeguarding the digital, physical, and psychological security of all involved must prevail over research interests.

An equally important aspect is the *vulnerability of victims and witnesses*. Open-source materials often depict violence, the aftermath of attacks, and the dead or injured. Such content can retraumatize not only victims' relatives but also analysts who process large volumes of imagery. The Protocol therefore calls for ethical filters: limiting access to graphic material, providing psychological support, labeling content, and using procedures that minimize harm. Researchers should refrain from copying and storing unnecessary files lacking evidentiary value to reduce leakage and unauthorized access risks.

Legal aspects include ensuring *authenticity*, *integrity*, and *admissibility*. Evidence must have established provenance, be obtained by a proper subject or in a manner not contrary to law, and remain unchanged from discovery to presentation in court. Documenting the chain of custody − time of receipt, source, technical parameters, software versions, and any transformations − is crucial. The Berkeley Protocol provides a structure for such procedures, and technical transparency is a condition of judicial acceptability.

Authorial context and intent also matter. Social media materials may be created by civilians, military personnel, journalists, or hostile information structures. It is important to assess whether the author had access to the scene, whether third-party rights are violated, and whether the content is part of an influence operation. The fact that material was published by a private person does not preclude its procedural use − provided proper verification and compliance with international standards. However, courts often evaluate not only the content, but also the method of obtaining evidence – therefore, procedural discipline becomes no less important than the content of the material itself.

A separate legal challenge is the problem of *manipulation* and *disinformation.* The digital space is saturated with fakes, edited videos, fake metadata, and content taken out of context. That is why triangulation of independent sources, analysis of the history of content appearance, reverse image search, installation of early copies, and work with primary files are mandatory components of OSINT investigation. The Berkeley Protocol defines procedures for working with digital evidence from

[33] Convention for the Protection of Human Rights and Fundamental Freedoms : Council of Europe Convention of 04.11.1950 : as of 1 August 2021. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

open sources as basic methodological standards that ensure reproducibility and independent verification of the reliability of materials[34].

Ethical dilemmas also arise in public communication of results. OSINT investigations often unfold with interim results being actively disseminated in the media or on social networks. Premature disclosures can hinder official investigations, endanger witnesses, or jeopardize procedural steps. Researchers must balance the public interest in access to information with the interests of justice and adhere to a principle of minimum sufficiency − publishing only what will not harm the proceedings or persons involved. These requirements resonate with the ethical principles for the safe use of digital resources contained in the Berkeley Protocol.

Legal assessment of OSINT materials occurs within international humanitarian and criminal law. To qualify an event as a war crime, one must establish not only the fact of attack or destruction but also the status of the object (civilian or military), proportionality of force, mens rea or gross negligence, and causation. Digital evidence may be necessary but insufficient; it must be aligned with other evidence: witness testimony, expert examinations, crime scene inspections, and official sources. Properly collected and verified OSINT materials, however, can uniquely reconstruct events where direct access is limited or dangerous.

In conclusion, we would like to emphasize that the legal and ethical aspects of using OSINT are not limited to the technical quality of the files. They cover issues of privacy, security, reliability, legal status of the material, balance of intervention, responsibility for the consequences of publication, and methodological transparency. It is precisely adherence to these principles, formulated in the *Berkeley Protocol on Digital Open Source Investigations*, that allows turning digital open sources into a full-fledged evidentiary base in the investigation of war crimes and ensuring the compatibility of the results with international standards of justice.

CONCLUSIONS

Systematic integration of OSINT into war-crimes investigations has demonstrated the ability of open digital sources to ensure rapid event detection, construct spatio-temporal narratives, and produce persuasive analytical findings compatible with procedural standards. Practice has confirmed that it is the combination of various OSINT technologies that gives the highest evidentiary return: imagery, satellite images, geospatial layers, and the content of social networks mutually reinforce each other, making it possible to narrow the «time windows», increase the accuracy of geolocation, and identify the object by unique features.

Correct work with the evidence base, in particular, detection, collection, documentation, investigation of war criminal offenses, must be carried out taking into account international experience and European standards of evidence. Technologies for working with open data impose requirements for ethical prudence on law enforcement officers: protection of privacy, minimization of harm to victims and witnesses, careful work with traumatic content, responsible public

[34] Главюк І.В Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*, 2025. Вип. 91. Т. 4. С. 251-259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35

communication of intermediate results. Given the influence of digital data, it is the balance between probative value and people's safety that should determine the limits of information processing and disclosure.

The Berkeley Protocol emphasizes the need to observe professional, methodological and ethical principles when working with open sources, especially in the context of international crimes. The only key postulate for the admissibility of data from open sources in evidence is the protection of the rights of the accused and a fair trial (clause 55 of the Berkeley Protocol). One of the key ethical dimensions is the issue of privacy and proportionality. The provisions of the Berkeley Protocol emphasize that the protection of the digital, physical and psychological safety of all persons involved must take precedence over research interests.

A separate legal challenge is the problem of manipulation and disinformation. The Berkeley Protocol defines procedures for working with digital evidence from open sources as basic methodological standards that ensure reproducibility and independent verification of the reliability of materials. At the same time, the methodological requirement − triangulation (verification) of sources, work with primary copies, description of tools and software versions, conducting an «audit track» – is an indispensable condition for the admissibility and reliability of digital evidence.

From the standpoint of the strategic development of criminal justice, the priorities are the institutionalization of uniform national protocols for working with digital open sources, the development of an interdepartmental OSINT ecosystem, the training of investigators, prosecutors and judges to work with digital evidence, as well as the integration of tools and procedures compatible with international practice. In such a configuration, OSINT ceases to be an «auxiliary» tool and becomes a full-fledged technology for collecting digital evidence, capable of significantly increasing the effectiveness of the investigation of war crimes in the war and post-war periods and strengthening public confidence in justice.

SUMMARY

The article is devoted to the study of the possibilities of using OSINT technologies for the investigation of war crimes and crimes of aggression in the conditions of modern armed conflicts in the activities of law enforcement agencies of Ukraine. Emphasis is placed on innovative possibilities of technologies for working with open digital sources and methods of their practical use in procedural proof of violations of international humanitarian law. The theoretical and legal principles of OSINT application are revealed and algorithms for working with visual materials, satellite images, geospatial data, social networks and other public digital resources are given. Considerable attention is paid to the peculiarities of recording digital traces during investigative (search) actions, issues of authenticity and admissibility of digital evidence, documentation of the chain of preservation, use of professional approaches to geolocation and chronology of events, as well as methods of identification of involved persons and military equipment. Ethical and legal aspects of technologies for working with open data are separately covered. Emphasis is placed on protecting privacy, minimizing the risks of retraumatization, preventing manipulation, and ensuring compliance with international standards, including the Berkeley Protocol on Digital Open Source Investigations. First of all, such

technologies expand the possibilities of timely notification of offenses, search and identification of criminals. Based on the analysis of global trends in the digital transformation of the activities of criminal justice bodies, a systematic approach to the implementation of the use of OSINT technologies in this direction in the war and post-war periods is proposed. The work pays attention to the issue of consistency of the process with the trends of European integration. The author came to the conclusion that the complex use of digital technologies for working with open data in the investigation of war crimes contributes to increasing the efficiency of law enforcement activities and the judicial process, expands evidentiary possibilities and provides more complete documentation of the circumstances of criminal offenses.

Key words: OSINT, technologization, innovations, war crimes, criminal justice, digital evidence, open sources of information, Budapest Convention on Cybercrime, satellite images, geolocation, chronology, verification, chain of preservation, Berkeley Protocol, propaganda, procedural proof.

References

1. OSINT-розвідка у роботі журналістів. URL: https://youcontrol.com.ua/articles/osint-in-journalists-work/.

2. Трансформація завдань криміналістики в умовах воєнного стану та євроінтеграційних процесів : зб. матеріалів наук.-практ. конф. присвяч. пам'яті д-ра юрид. наук, проф. В.О. Коновалової,м. Харків, 28 берез. 2024 р. / [редкол.: А. П. Гетьман, В. М. Шевчук, Є. Є. Демидова] ; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2024. 148 с. URL: https://ivpz.kh.ua/wp-content/uploads/2024/09/Трансформація-завдань-криміналістики-28.06.2024.pdf

3. Методологічні засади криміналістики: традиції та новації : зб. матеріалів Криміналістичних читань, присвяч.пам'яті акад. В. О. Коновалової, м. Харків, 28 берез. 2025 р. Нац. юрид. ун-т ім. Ярослава Мудрого,Каф. криміналістики; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В.Сташиса Нац. акад. прав. наук України. Харків: Право, 2025. 276 с. URL: https://ivpz.kh.ua/wp-content/uploads/2025/04/Kryminalistychni_chytannia_Konovalova_28.03.2025.pdf.

4. Роль OSINT-досліджень у підвищенні рівня національної безпеки України : матеріали круглого столу (м. Львів, 7 травня 2025 р.) / укладач І. О. Ревак. Львів : ЛьвДУВС, 2025. 249 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8875/1/07_05_2025.pdf.

5. OSINT та електронні докази: юридичні вимоги та практика застосування у кримінальних провадженнях щодо воєнних злочинів в Україні. 14.01.2026. URL: https://www.coe.int/uk/web/kyiv/-/osint-and-electronic-evidence-legal-requirements-and-practical-application-in-criminal-proceedings-on-war-crimes-in-ukraine.

6. Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

7. Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США (2023). URL: https://khrife-journal.org/index.php/journal/article/download/564/633.

8. Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: навчання НПУ. 08.10.2025. URL: https://npu.gov.ua/news/vykorystannia-osint-u-dokazuvanni-komandnoi-vidpovidalnosti-za-mizhnarodni-zlochyny-navchannia-npu.

9. Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374. DOI: 10.32782/2524–0374/2022–4/88.

10. Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України.* 2022. № 2. С. 87-90.

11. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

12. Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku.

13. Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності:* мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

14. Злочини, вчинені в період повномасштабного вторгнення рф станом на 22.12.23. URL: https://www.gp.gov.ua.

15. Bellingcat. URL: https://www.bellingcat.com/

16. Радейко Р. І. Інструментарії OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400–410. DOI: https://doi.org/10.5281/zenodo.15648723.

17. Вирок Івано-Франківського міського суду Івано-Франківської області від 05 грудня 2024 року у справі № 344/19008/24. URL: https://reyestr.court.gov.ua/Review/123535737.

18. Вирок Основ'янського районного суду міста Харкова від 10 червня 2025 року у справі № 643/6925/24. URL: https://reyestr.court.gov.ua/Review/127999232.

19. Кудінов С. С., Шехавцов Р. М. Правове регулювання використання osint та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126–133. DOI: https://doi.org/10.32782/2311-8040/2025-3-14

20. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

21. Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, LIGA.net URL: https://tech.liga.net/ua/ukraine/ novosti/iskusstvennyy-intellekt-mintsifry-razoblachil-okkupanta-popavshego-v-gospitalv-krivom-roge.

22. Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

23. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С. 142–146.

24. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. *Military offences and war crimes: background, theory and practice*: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2023. С. 795-823. URL: http://www.baltijapublishing.lv/omp/ index.php/bp/catalog/download/322/8791/18392-1.

25. Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL:. https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogiluukrayinskih-vijskovih-ta-ponad-460-novih-mogil-foto.

26. *Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі*: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2024. 208 с. С. 89.

27. Батанов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану: дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. 205 с.

28. Кисельов А. О. Тактика спілкування поліцейського з особами. The Top Actual Researches in Modern Science: Proceedings of the IInd International Scientific and Practical Conference (Ajman, July 28- 29, 2016, UAE). International Scientific and Practical Conference «World Science». 2016. № 8 (12). P. 25–28.

29. Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф.: у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро: Дніпроп.держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

30. Москаленко Я. , Кривошея Д. , Дейкун О, Кисельов А. Гео-OSINT в кримінальному аналізі. Collection of Scientific Papers «SCIENTIA», (May 30, 2025; Glasgow, Scotland, UK). С. 85–91.

31. Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. *Використання цифрових технологій у криміналістиці та судовій експертизі:* матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К . Авдєєва]; Нац. акад. прав. наук України ; НДІ вивч.

проблем злочинності ім. акад. В. В. С ташиса НАПрН України. Харків: Право, 2024. С.133–136.

22. Shevchuk, V., Morozova, T., Chornyi, H., Nehrebetskyi, V., and Slobodeniuk, I. Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues / V. Shevchuk та ін. *International Annals of Criminology*. 2025. С. 1–19. URL: https://doi.org/10.1017/cri.2025.10090.

23. Shevchuk, V., Dunaev, O., Tyshchenko, O., Biletska, G., and Nehrebetskyi, V. Innovative Methods in the Identification of Deceased Persons during Armed Conflicts and Disasters: Criminalistic and Forensic Medical Issues / V. Shevchuk et al. *International Annals of Criminology*. 2025. С. 1–20. URL: https://doi.org/10.1017/cri.2025.10094.

24. Гловюк І.В Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*, 2025. Вип. 91. Т. 4. С.251-259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35 URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/37-3.pdf

Information about the author:
Nehrebetskyi Vladyslav Valerevych,
Ph. D. in Law,
Associate Professor at the Department of Criminalistics
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., Kharkiv, 61024, Ukraine,
Researcher at Academician Stashis Scientific Research Institute
for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
49, Hryhoriia Skovorody str., Kharkiv, 61002, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-12

ЕЛЕКТРОННІ ДОКАЗИ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ: КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА ПРОЦЕСУАЛЬНІ ВИМОГИ

Перунова О. М.

ВСТУП

Стрімкий розвиток інформаційних технологій та цифровізація суспільних відносин істотно трансформувала традиційні уявлення про способи фіксації, збереження та передання інформації. Ці процеси безпосередньо вплинули і на сферу цивільного судочинства, зумовивши появу нових форм доказової інформації, зокрема електронних доказів. У сучасних умовах саме електронні носії дедалі частіше стають основним засобом відображення юридично значущих фактів, що виникають у процесі цивільного обороту, комунікації між суб'єктами права, реалізації майнових і немайнових прав та виконання зобов'язань.

Слід підкреслити, що електронні докази вирізняються особливою правовою природою, що відрізняє їх від класичних письмових чи речових доказів. Їх унікальність полягає у нематеріальній формі існування, залежності від технічних засобів відтворення, м можливості швидкого копіювання без втрати змісту, а також у специфічних характеристиках автентичності, цілісності та достовірності. Отже, такі особливості зумовлюють необхідність вироблення спеціальних процесуальних підходів до оцінки електронних доказів та визначення їх належності й доступності у цивільному судочинстві.

Так, необхідність активного використання електронних доказів у цивільному процесі обумовлена не лише технічним прогресом, а й змінами у способах реалізації цивільних прав. Виникають таким чином, так звані електронні правочини, цифрові сервіси, електронне листування, соціальні мережі, хмарні технології та інші форми цифрової взаємодії створюють нову реальність, у якій традиційні засоби доказування не завжди здатні повною мірою відобразити обставини справи. У цьому контексті електронні докази постають не як факультативний, а як необхідний елемент ефективного захисту прав та інтересів учасників цивільного процесу.

Але, слід також зауважити, що запровадження електронних доказів у практику цивільного судочинства супроводжується низкою дискусійних та проблемних питань. Серед них особливе місце по сідає проблема готовності судової системи до повноцінного сприйняття та використання таких доказів. Йдеться як про технічне забезпечення судів, так і про рівень спеціальних знань суддів та інших учасників процесу щодо особливостей електронної інформації, способів її отримання, збереження та перевірки. Недостатня уніфікація судової практики, відсутність сталих підходів до оцінки електронних доказів, а також ризики фальсифікації чи втрати цифрових даних посилюють правову невизначеність у цій сфері. Спірним залишається і питання співвідношення електронних доказів з іншими видами доказів у цивільному процесі, зокрема щодо їх доказової сили з підвищеним рівнем обережності, що може призводити

до необґрунтованого обмеження їх використання або формального підходу до їх оцінки. Така практика свідчить про потребу подальшого наукового осмислення правової природи електронних доказів та вдосконалення процесуальних механізмів їх застосування.

Разом із тим подальше розширення сфери використання електронних доказів у цивільному судочинстві є об'єктивного неминучим. Цифровізація правосуддя, розвиток електронного суду, інтеграція інформаційних систем та поступове формування цифрової правової культури зумовлюють трансформацію доказового процесу. В цих умовах електронні докази набувають не лише допоміжного, а й системо утворюючого значення, стаючи одним із ключових інструментів встановлення істини у цивільних справах.

Таким чином, дослідження унікальності електронних доказів, їх процесуальних вимог, значення та проблем застосування в цивільному судочинстві є вкрай актуальним завданням сучасної цивільної процесуальної науки. Комплексний аналіз цих питань дозволяє не лише окреслити теоретичні засади використання електронних доказів, а й сприяти формуванню ефективної та справедливої судової практики, адаптованої до викликів цифрової епохи.

1. Поняття електронних доказів у цивільному судочинстві

Відповідно до ч. 1 ст. 76 ЦПК України «доказами є будь-які фактичні дані, на підставі яких суд встановлює наявність або відсутність обставин (фактів), що обґрунтовують вимоги і заперечення учасників справи, та інших обставин, які мають значення для вирішення справи»[1].

Слід зазначити, що наука являє собою зміст і розвиток певних явищ, які становлять інтерес у конкретній галузі або напрямі, не винятком є розвиток і застосування практично так званих юридичних фактів (доказів), без яких на сьогодні ми не мислимо розгляду цивільної справи та винесення законного й обґрунтованого судового рішення. Використання таких фактів не тільки набуває великого значення для учасників цивільного процесу, але й має значення для аргументації правосуддя. Оформлюючи кожну цивільну справу, суд у процесуальних актах-документах офіційно фіксує характер і правову природу спору, що є унікальними саме для цього провадження. Таким чином визначається індивідуальний вигляд справи, який відображає особливості її процесуальної форми, змісту й предмета судового розгляду, що, у свою чергу, забезпечує належну правову кваліфікацію й упорядкованість усіх подальших процесуальних дій.

У сучасних умовах ЦПК України закріплює широку класифікацію доказів, що можуть бути використані в процесі розгляду цивільних справ. До таких належать письмові, речові та електронні докази, висновки експертів, а також показання свідків. Згідно з процесуальними приписами обов'язок подання доказів покладено на сторони та інших учасників судового провадження. При цьому доказова інформація повинна спиратися на об'єктивні, достовірні факти, а не припущення. Однією з основоположних вимог цивільного судочинства є

[1] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV.

сумлінність і добросовісність поведінки учасників процесу при поданні доказів, що сприяє забезпеченню їх належності, допустимості та достовірності в межах судового розгляду.

Судові докази – це діалектичне поєднання інформації (змісту) та її процесуальної форми. Інформація, що відображається у доказах, є предметною, оскільки вона стосується обставин цивільної справи. Але пізнати дану інформацію можна тільки через її носія[2].

Незважаючи на всю різноманітність використання різних видів юридичних фактів, нас цікавить застосування саме електронного формату доказової бази, оскільки на сьогоднішній день розгляд і вирішення цивільних справ може відбуватися як у класичному форматі ведення процесуальної форми, так і в форматі електронного суду – Єдиної судової інформаційно-телекомунікаційної системи.

В обох цих варіантах ведення цивільного судочинства суд може використовувати саме юридичні факти у вигляді електронної доказової бази і користуватися нею для винесення судової постанови при вирішенні судового спору.

Слід зазначити, що сучасний розвиток цивільного судочинства неможливо розглядати поза контекстом такого явища, як цифровізація судової системи. Вона постає як стійка тенденція модернізації та формування майбутньої моделі судового розгляду, що зумовлює трансформацію традиційної процесуальної форми. Така трансформація спрямована на поступове впровадження електронних засобів фіксування, обміну та зберігання процесуальної інформації, використання дистанційних форматів участі у провадженні, електронного документообігу, а також застосування засобів комунікації, зокрема електронного листування, текстових чи голосових повідомлень між учасниками процесу.

З урахуванням зазначеного цифровізація постає не лише як технічне оновлення судової діяльності, а як якісна зміна самої культури процесуальної взаємодії, що відкриває нові виміри ефективності, доступності та прозорості правосуддя в умовах інформаційного суспільства.

Отже, підкреслимо, що використання електронних доказів, особливо у форматі дистанційного розгляду справ, суттєво впливає на трансформацію змісту та форми цивільного судочинства. Це зумовлено тим, що електронні докази мають специфічну природу, яка відрізняється від традиційних засобів доказування. Науковці-правознавці, серед яких Ю. С. Павлова, І. В. Вернидубов і С. О. Белікова, О. О. Полуніна й ін., у своїх працях акцентують на особливостях їх правового статусу, способах подання, автентифікації та оцінювання, що підтверджує складність і водночас перспективність їх застосування в сучасному процесуальному середовищі.

Ю. С. Павлова дослідила досвід використання електронних доказів у системі прецедентного та романо-германського права. Вона наголошує, що у країнах прецедентного типу, де відсутні кодифіковані норми, провідну роль відіграє судовий прецедент. Науковиця аналізує системи США, Німеччини,

[2] Андрійцьо В. Д. Докази як об’єкт збору на етапі збирання доказів у цивільному процесі. *Право і суспільство.* 2013. № 4. С. 34.

Франції та Великої Британії, зокрема типологію електронних доказів: документи, створені на комп'ютері, дані, збережені у підключених системах, електронне листування, цифрові записи тощо. Ю. С. Павлова підкреслює, що адаптація такого досвіду до української практики може сприяти підвищенню ефективності цивільного судочинства та забезпеченню належної процесуальної оцінки електронних доказів[3].

Запровадження та розвиток використання електронних доказів у цивільному процесі Франції та Німеччини тісно пов'язані з явищами електронного підпису й електронного документа. Для законодавства США та Великої Британії не характерне пряме визначення поняття електронного доказу як такого, при цьому американська наукова доктрина, як і британська, широко використовує це поняття. Електронний доказ охоплює всі можливі докази та інформацію, яка може бути передана або збережена за допомогою цифрових пристроїв чи програм і які можуть скласти фактичну інформацію про будь-який факт[4].

І. В. Вернидубов і С. О. Белікова вказують на різноманіття видової класифікації електронних доказів і їх ознаки, а саме існування в нематеріальному вигляді; необхідність використання певних технічних засобів для їх застосування в суді; можливість перенесення чи копіювання на різні технічні пристрої без втрати їх сутності; оригінал електронного доказу може бути доданий до матеріалів судової справи в будь-якому виді судочинства[5].

«Особливо важливим фактором для ухвалення судового рішення у справі є відповідність електронних доказів основним чотирьом критеріям: належність, допустимість, достовірність та достатність»[6].

О. О. Полуніна звертає увагу на існування великої ймовірності, «що вже найближчим часом вітчизняне судочинство повністю перейде на електронне доказування, що передбачає абсолютну відмову від особистого спілкування між учасниками процесу і між суддею та учасниками судової справи, що, у свою чергу, призведе до необхідності перегляду сутності та змісту багатьох засад і принципів судового провадження, насамперед принципу безпосередності судового розгляду»[7].

---

[3] Павлова Ю. С. Електронний доказ в цивільному процесі: зарубіжний досвід. *Актуальні проблеми вітчизняної юриспруденції.* 2023. № 2. С. 29–33. DOI: https://doi.org/10.32782/39221466.

[4] Павлова Ю. С. Електронний доказ в цивільному процесі: зарубіжний досвід. С. 32. **Або:** Там само. С. 32.

[5] Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо їх дослідження судом. *European Political and Law Discourse.* 2018. Vol. 5, Iss. 2. P. 299–305.

[6] Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо їх дослідження судом. P. 303. **Або:** Там само. P. 303.

[7] Полуніна О. О. Електронні докази як особливий засіб доказування у цивільному процесі. *Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні* : матеріали Всеукр. наук.-практ. інтернет-конф. ім. Ю. С. Червоного (Одеса, 18 груд. 2020 р.) / за заг. ред. Н. Ю. Голубєвої. Одеса : Фенікс, 2020. С. 44. URL: https://dspace.onua.edu.ua/bitstreams/b255fc75-8f6e-4093-bda2-358afa34faa5/download (дата звернення: 12.12.2023).

Згідно з Керівними принципами Комітету міністрів Ради Європи з електронних доказів у цивільному та адміністративному провадженні від 30.01.2019 приймається широке визначення поняття «електронний доказ» (також відомий як «цифровий доказ»). Він може мати форму тесту, відео, фотографій або звукових записів. Дані можуть походити з різних носіїв або способів доступу, таких як мобільні телефони, вебсторінки, бортові комп'ютери чи GPS-реєстратори, включаючи дані, збережені у сховищах поза контролем сторони. Типовим прикладом електронного доказу є електронні повідомлення (електронна пошта)[8].

Отже, сьогодні електронні докази являють собою значне різноманіття об'єктів із власними технічними характеристиками, що безпосередньо впливає на їх сприйняття та оцінку як судом, так і учасниками процесу. Особливу увагу це питання набуває в контексті дистанційного розгляду справ, де подання та вивчення електронних доказів у цифровому форматі вимагає від суду підвищення обізнаності та суворішого дотримання принципів законності, достовірності, належності та доступності таких доказів. Незважаючи на те, що ст. 100 ЦПК України формально дозволяє сторонам подавати електронні докази до суду, законодавство водночас установлює додаткову вимогу наявності паперової копії, що свідчить про певну обережність законодавця щодо цифрового формату. Відповідно до наведеного особливого значення набуває формування єдиного стандарту оцінювання електронних доказів, який би забезпечував узгодженість та уніфікованість судової практики їх застосування. Запровадження такого підходу сприятиме підвищенню рівня правової визначеності, зменшенню ризику неоднакового тлумачення процесуальних норм і, відповідно, ефективнішому здійсненню правосуддя. Крім того, єдиний стандарт дасть змогу встановити чіткі критерії достовірності, допустимості та належності електронних доказів, що, у свою чергу, зміцнить довіру до судового процесу й забезпечить реалізацію принципу справедливого судового розгляду.

Отже, відсутність чітко окреслених критеріїв оцінки цифрових джерел інформації призводить до фрагментарності судової практики, різночитань щодо доступності скріншотів, листування, електронних копій документів та метаданих. Формально електронні докази є вже інтегрованими у процесуальне судочинство, однак фактичної застосування часто залежить від суб'єктивної оцінки суду, що створює ризики непередбачуваності правозастосування.

Вважаємо, що так званий єдиний стандарт електронних доказів повинен базуватися не лише на формальному визначенні їх процесуального статусу, а й на чітких критеріях автентичності, цілісності та відтворюваності цифрової інформації. Йдеться про нормативно закріплену сукупність вимог до способів фіксації, збереження, подання та перевірки електронних даних. Такий стандарт має включати мінімальний перелік технічних параметрів (наявність метаданих,

[8] Electronic Evidence in Civil and Administrative Proceedings : Guidelines adopted by the Committee of Ministers of the Council of Europe on 30 January 2019 and explanatory memorandum / Council of Europe. Council of Europe, 2019. P. 15. URL: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 (дата звернення: 02.11.2025).

цифрового підпису, хеш-індефікатора, журналу змін), а також процесуальні гарантії їх дослідження в судовому засіданні.

Також, слід зауважити, що уніфікація не повинна зводитися до надмірної формалізації. Електронні докази є технічно варіативними, а тому стандарт має бути технологічно нейтральним і адаптованим. Його завдання – не обмежити розвиток цифрових форм комунікації, а забезпечити передбачуваність оцінки доказів незалежно від платформи чи програмного середовища. Саме баланс між технічною гнучкістю та процесуальною визначеністю здатен гарантувати узгодженість судової практики.

На нашу думку, запровадження такого стандарту можливе через поєднання таких механізмів, а саме: законодавчого уточнення критеріїв допустимості, розроблення методичних рекомендацій для судів та формування усталеної практики вищих судових інстанцій. Особливе значення має узагальнення правових позицій, які формуватимуть презумпції достовірності або, навпаки, критерії сумніву щодо певних видів цифрових доказів. Саме через інституційне закріплення цих підходів можливе досягнення єдності судової практики і можливість застосування у цивільно-процесуальних нормах права.

Наукове впровадження єдиного стандарту електронних доказів у цивільне судочинство України повинно здійснюватися як системна трансформація доказового підходу, а не як фрагментарне технічне уточнення процесуальних норм. Йдеться про формування цілісної концепції доказування в цифрову епоху, яка поєднуватиме *нормативну визначеність, технологічну нейтральність та гарантії справедливого судового розгляду.* Сьогодні, в межах вітчизняної процесуальної доктрини електронне доказування слід розглядати не як сукупність окремих цифрових засобів фіксації інформації, а як самостійний елемент процесуальної форми цивільного судочинства. Відсутність системного стандарту електронних доказів зумовлює фрагментарність судової практики та підвищує рівень дискредитації при оцінці цифрових даних.

На нашу думку, така ознаки електронного доказу, як нормативна визначеність повинна проявлятися у закріпленні чітких критеріїв автентичності, цілісності та відтворюваності електронної інформації, а також у встановленні процесуальних презумпції достовірності певних видів цифрових доказів. Вважаємо, що слід розглядати нормативну визначеність як структурований елемент процесуальної форми цивільного судочинства, що забезпечує передбачуваність судового розгляду та єдність правозастосування.

Технологічна нейтральність, суть цієї ознаки полягає в тому, що процесуальні норми повинні бути сформульовані таким чином, щоб їх дія не залежала від конкретних технічних платформ чи програмних продуктів. Такий підхід забезпечує стабільність процесуальної форми цивільного процесу в умовах постійної цифрової трансформації та унеможливлює нормативну застарілість регулювання.

Також, можна помітити певний взаємозв’язок між електронним доказуванням і гарантіями справедливого судового рішення, зокрема принципами змагальності, рівності сторін і безпосередності дослідження доказів. Аргументовано, що єдиний стандарт електронних доказів має

виступати інструментом реалізації права на справедливий судовий розгляд, а не додатковим бар'єром у доступі до правосуддя.

Отже, запропоновані ознаки електронного доказування створюють теоретичне підґрунтя для формування єдиного стандарту електронних доказів у цивільному судочинстві України, який буде забезпечувати узгодженість судової практики, мінімізує дискреційність оцінки цифрових даних та сприяє модернізації процесуальної форми відповідно до викликів цифрової епохи.

Такий стандарт, вважаємо має бути закріплений на рівні процесуального законодавства через уточнення критеріїв автентичності, цілісності та відтворюваності електронної інформації, із встановленням призумції достовірності для електронних даних, створених із застосуванням кваліфікованих засобів електронної ідентифікації.

Практична реалізація стандарту електронного доказування потребує, вважаємо поєднання трьох рівнів: законодавчого (уточнення положень ЦПК України щодо допустимості та оцінки електронних доказів); методичного (розроблення рекомендацій для судів та учасників процесу) та інституційного (формування єдиних підходів у практиці судової системи України). Саме через усталення правових позицій судової системи можливе створення стабільних орієнтирів для підходів до оцінки цифрових даних. Виникнення єдиного стандарту електронних доказів має розглядатися як елемент модернізації цивільного судочинства України в умовах цифровізації правових відносин. Його метою повинно стати не ускладнення доказового процесу, а забезпечення передбачуваності судових рішень, процесуальної рівності сторін та підвищення довіри до правосуддя. Саме науково обґрунтована модель такого стандарту здатна стати підґрунтям для формування уніфікованої та узгодженої судової практики щодо застосування електронних доказів.

Таким чином, це підкреслює необхідність застосування більш обґрунтованого та системного підходу до оцінки електронних доказів, що передбачає не лише перевірку їх достовірності та належності, а й урахування процесуальної форми, у якій їх подано. Впровадження чітких стандартів у судовій практиці сприятиме узгодженому й законному використанню електронних доказів, забезпечуючи їх надійність і юридичну вагомість. Такий підхід є важливим для забезпечення ефективного цивільного судочинства, гарантування рівних прав учасників процесу та реалізації принципу справедливого й обґрунтованого судового рішення. Його впровадження сприятиме підвищенню довіри до судової системи в умовах цифрової трансформації правосуддя та мінімізує ризики процесуального формалізму або довільного тлумачення доказових критеріїв.

2. Вимоги та особливе значення електронних доказів у цивільному судочинстві

У цивільному судочинстві під час розгляду справ застосовуються конкретні юридичні факти, які дають змогу оцінити зміст і специфіку процесуальної форми для кожної окремої справи. Процесуальні юридичні факти (докази) мають певні якості. Насамперед вони повинні бути зафіксовані у встановленій законодавством процедурно-процесуальній формі, тобто процесуальні

юридичні факти мають правове значення лише в тому разі, якщо вони належним чином оформлені і затверджені. Юридичні факти, які породжують конкретні процесуальні правовідносини, як правило, не одиничні, а виступають у вигляді юридичного складу. Зі свого боку юридичний склад характеризується двоякістю правової природи, він включає в себе матеріально-правовий характер і матеріально охоронюване правовідношення. Ці процесуальні факти повною мірою зазначені в нормах процесуального права.

Саме це зумовлює характер тих вимог, яким повинні відповідати дії учасників цивільного процесу, на яких покладається обов'язок пред'явлення доказів і встановлення об'єктивної істини, тобто на всіх, хто є заінтересованим у вирішенні об'єктивної і законної істини з конкретної цивільної справи.

Тому можна стверджувати, що судове доказування являє собою складну процесуальну діяльність суду й інших учасників цивільного процесу, яка спрямована на встановлення істини з конкретної справи і вирішення спору між сторонами.

Доказування в цивільному судочинстві виконує подвійне функціональне призначення. По-перше, воно забезпечує дотримання процесуальної форми судового розгляду, визначаючи порядок і логіку здійснення процесуальних дій усіма учасниками провадження. По-друге, доказова діяльність має безпосередній вплив на матеріальну складову судового процесу, оскільки саме на основі належно зібраних, перевірених і оцінених доказів суд установлює юридично значущі факти та формує своє обґрунтоване рішення. Процесуальні докази сприймаються сторонами як матеріальна база правової інформації, яка дозволяє реалізувати принципи об'єктивності та всебічності при дослідженні обставин справи. Завдяки цьому судова оцінка доказів і винесення рішення здійснюються в межах закону, забезпечуючи не лише законність, а й справедливість кінцевого результату цивільного процесу.

Відповідно до положень ЦПК України докази оформлені та організовані у вигляді впорядкованої системи, що підпорядкована визначеним нормами вимогам, які регламентують їх допустимість, достовірність і значення. Такий системний підхід забезпечує послідовне і надійне використання доказів, що сприяє належному функціонуванню цивільного судочинства та гарантує прийняття обґрунтованих і законних рішень.

До таких вимог належать належність доказів, доступність і достовірність доказів, стандарти доказування, порядок подання та витребування доказів судом, обов'язок сторін щодо доказування, розподіл цього обов'язку, звільнення від доказування, презумпції та організація доказової діяльності. У контексті сучасного процесуального розвитку особливого значення набувають електронні докази, які можуть включати оригінали електронних документів, роздруківки електронного листування та інтернет-сторінок, відеозаписи, скриншоти повідомлень із мобільних пристроїв, роздруківки з месенджерів (вайбер, телеграм тощо). Важливим є встановлення критеріїв оцінювання таких доказів та витребування їхніх оригіналів для забезпечення законності та надійності процесу.

Отже, безумовно, усі перелічені характеристики доказів мають важливе значення для забезпечення законності та обґрунтованості судового рішення.

Водночас достовірність доказів слід вважати ключовим елементом, що формує правову основу оцінки всієї доказової бази конкретної справи, оскільки вона відображає інтегровану оцінку юридичних фактів і інформації з різних джерел. У світлі зазначених ознак процесуальна форма цивільного судочинства постає не лише як сукупність встановлених законом процедур, а як системний механізм організації та фіксації доказової діяльності. Вона виконує інтегративну функцію – поєднує нормативні приписи, технологічні можливості та ціннісні орієнтири справедливого судочинства в єдину структуровану модель доказування. Саме через процесуальну форму відбувається впорядкування цифрової інформації, її трансформація з технічного масиву даних у юридично значущий доказ.

Також, слід вказати на певний організаційний аспект процесуальної форми, що проявляється у встановленні чіткої послідовності подання та дослідження електронних доказів, визначенні обсягу процесуальних прав і обов'язків сторін, а також процедур перевірки автентичності та цілісності цифрових даних. Фіксаційна функція, у свою чергу, забезпечує документування кожного етапу доказової діяльності – від моменту подання електронного доказу до його оцінки в мотивувальній частині судового рішення. У цифрову епоху ця функція набуває особливого значення, оскільки саме належна фіксація дозволяє відтворити логіку судового дослідження та перевірити обґрунтованість висновків суду.

З урахуванням нормативної визначеності процесуальна форма гарантує передбачуваність процедур і мінімізує ризик довільного підходу до оцінки електронних доказів. Через принцип технологічної нейтральності вона може забезпечувати адаптивність доказового процесу до різноманіття цифрових джерел інформації без порушення його внутрішньої стабільності. А завдяки орієнтації на справедливість судового рішення процесуальна форма перетворюється на інструмент балансу між процесуальною економією та повнотою дослідження доказів.

Отже, процесуальна форма цивільного судочинства в умовах електронного доказування набуває якісно нового змісту. Вона виступає гарантією законності – через чіткість процедур; надійності – через забезпечення перевірюваності та відтворюваності цифрових даних; ефективності – через оптимальну організацію доказового процесу. Саме в цій триєдиній площині розкривається її модернізована роль як структурного каркасу ухвалення судового рішення, що відповідає викликам цифрової трансформації правосуддя.

Зауважимо, що лише в останні роки ЦПК України чітко визначив норми права, які закріплюють положення щодо однієї з ключових характеристик цивільної процесуальної форми при розгляді справ, а саме достовірності та достатності доказів. Так, ст. 79 ЦПК України має назву «Достовірність доказів» і включає лише одне положення: «Достовірними є докази, на підставі яких можна встановити дійсні обставини справи». Стаття 80 ЦПК України містить два положення. Перше: «Достатніми є докази, які у своїй сукупності дають змогу дійти висновку про наявність або відсутність обставин справа, які входять до предмета доказування». І друге: «Питання про достатність доказів для встановлення обставин, що мають значення для справи, суд вирішує

відповідно до свого внутрішнього переконання»[9]. Таким чином, ці норми формалізують процесуальні вимоги до оцінки доказів, підкреслюючи необхідність установлення достовірних фактів справи, і дають суду змогу ухвалювати обґрунтоване рішення на основі оцінки сукупності доказів відповідно до внутрішнього переконання, що є невід'ємною частиною процесуальної форми цивільного судочинства.

Вважаємо, що значна частина зазначених законодавчих положень має практичне значення та здатна забезпечувати належне функціонування цивільного процесу. Водночас положення, яке надає судам можливість вирішувати питання відповідно до свого внутрішнього переконання, потребує більшої конкретизації та правової стандартизації. З одного боку, цей механізм дозволяє суду гнучко оцінювати доказову базу та враховувати всі обставини конкретної справи, що сприяє більш обґрунтованому ухваленню рішення. З іншого боку, відсутність чітких критеріїв може створити ризики непослідовності та суб'єктивності у практиці, що ускладнює уніфіковану оцінку доказів. Тому, на наш погляд, доцільно зробити нормативні орієнтири, які б визначили межі застосування внутрішнього переконання суду, забезпечити баланс між гнучкістю оцінки доказів і дотриманням стандартів процесуальної форми, що, у свою чергу, підвищить правову передбачуваність і ефективність цивільного судочинства.

Водночас, хоча запровадження внутрішнього переконання суду дозволяє оцінювати докази гнучко та приймати рішення з урахуванням усіх обставин конкретної справи, такий механізм має і свої обмеження. Схоже, що застосування цього підходу може викликати певну недовіру та сумніви з боку учасників процесу. Це зумовлено тим, що повнота пізнавальної функції, необхідної для обґрунтованого та законного вирішення справи, у таких випадках не завжди розкривається. Внаслідок цього знижується прозорість і об'єктивність процесу для всіх сторін, а знання, яке формується в ході оцінювання доказів, залишається доступним фактично лише для суду, що обмежує процесуальну участь учасників і впливає на сприйняття справедливості судового розгляду.

Підкреслимо, що в основі цивільного процесу лежить також принцип змагальності сторін, який передбачає їхню активну участь у поданні та доведенні юридичних фактів, необхідних для встановлення істини у справі та визнання правомірності позиції однієї із сторін. У такій площині суд зобов'язаний забезпечити сторонам максимально можливі умови для реалізації їхніх процесуальних прав, зокрема права на подання доказів, їх дослідження та спростування. Водночас суд сам повинен забезпечити повне та всебічне з'ясування всіх характерних обставин справи, що є передумовою ухвалення обґрунтованого й законного рішення, узгодженого з вимогами процесуальної форми цивільного судочинства.

Принцип змагальності в сучасному цивільному судочинстві набуває нового змістового наповнення у зв'язку з активним використанням електронних

[9] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV.

доказів. Якщо традиційна змагальність розумілася як процесуальна рівність сторін у подання та спростуванні доказів, то в умовах цифровізації вона трансформується у більш складну модель взаємодії сторін щодо доступу, автентифікації та технічної перевірки цифрової інформації. Електронний доказ не є статичним носієм відомостей – він має технічні характеристики, метадані, історію змін, що потребує спеціального аналізу. Відтак змагальність сьогодні включає не лише право надати доказ, а й реальну можливість перевірити його цифрову природу.

У такому вигляді принцип змагальності безпосередньо пов'язаний із забезпеченням рівного доступу сторін до електронних джерел інформації та процедур їх дослідження. Якщо одна зі сторін має технічну перевагу – досту до серверів, електронних архивів, корпоративних систем зберігання даних, – виникає ризик порушення процесуального балансу. Саме тому процесуальна форма повинна гарантувати механізми витребування електронних доказів, їх копіювання, збереження та експертної перевірки. Лише за таких умов змагальність набуває реального, а не декларативного характеру.

Крім того, електронні докази актуалізують питання своєчасності їх розкриття. Цифрова інформація може бути змінена або видалена, що створює ризики зловживань. Відповідно, принцип змагальності вимагає встановлення чітких строків і процедур подання електронних доказів. А також можливості їх негайної фіксації. Змагальність у цифровому середовищі – це не лише конкуренція позиції сторін, ай змагальність технічних аргументів щодо достовірності та цілісності даних.

Особливого значення набуває також право сторони ставити під сумнів автентичність електронного доказу, ініціювати експертне дослідження метаданих, перевірку електронного підпису або джерела походження файлу. Таким чином, змагальність розширюється до сфери цифрової верифікації, а суд виступає арбітром не тільки правових, а й технічно обґрунтованих позицій.

Отже, можна підкреслити той факт, що у сучасному цивільному судочинстві принцип змагальності тісно інтегрується з інститутом електронних доказів і набуває багаторівневого характеру. Він охоплює процесуальну рівність у доступі до цифрової інформації, можливість її перевірки та спростування, а також гарантії технічної прозорості доказового процесу. Саме через таке розширене розуміння змагальність стає ключовою передумовою формування справедливого та обґрунтованого судового рішення в умовах цифровізації правосуддя.

Сучасні наукові дослідження доводять, що під достовірністю доказів слід розуміти такий рівень правдивості доказових відомостей, який дає змогу суду з високим ступенем ймовірності бути переконаним в існуванні або неіснуванні фактів чи обставин, які входять до предмета доказування, а також визначити відповідні дані доказами[10].

Вважаємо, що достовірність повинна вказувати на багатоманітність доказової бази, що була застосована при розгляді цивільної справи, вона є тією

[10] Грабовська О. О. Теоретико-правові проблеми доказування у цивільному процесі України : дис. … д-ра юрид. наук : 12.00.03. Київ, 2018. С. 169.

вимогою, яка не допускає припущень, що щось було забуто чи взагалі не переглянуто судом або не була дана можливість учасникам судового процесу надати такий доказ, який у процесі його перегляду, можливо, надасть якусь правову інформацію, що може мати значення для винесення судового рішення і визнання правоти однієї із сторін. Адже лише за умови всебічного, повного та об'єктивного дослідження всіх доказів можливо забезпечити ухвалення справедливого й обґрунтованого судового рішення, яке відображає істину у справі та визначає правоту однієї із сторін.

Цивільна процесуальна форма не повинна мати внутрішніх суперечностей між правовими явищами, вона повинна діяти згідно зі стандартами максимального пізнання істини.

Послідовність стадій цивільного процесу, здійснення процесуальних дій та застосування відповідних норм процесуального права визначає формування процесуальних відносин і має строго нормативний характер. Саме через визначену законом послідовність етапів забезпечується цілісність і впорядкованість судового впровадження. Так, початковою є стадія відкриття провадження у справі, що збігається з пред'явленням позову та прийняттям судом позовної заяви. Наступною стадією виступає провадження у справі до судового розгляду, за якою слідують інші стадії відповідно до процесуального регламенту. Дотримання цієї послідовності є обов'язковим, оскільки зміна порядку або пропуск стадії може порушити встановлений законодавством порядок формування процесуальних відносин і негативно вплинути на забезпечення законності, справедливості та захисту прав учасників цивільного процесу.

Абсолютно очевидним є те, що процесуальна форма цивільного процесу повинна ґрунтуватися на певних складових, серед яких, безперечно, однією з найважливіших сфер процесуальної діяльності є застосування доказування учасниками цивільного розгляду.

Повертаючись до питання визначення формату електронних доказів, відзначимо наявність певної суперечливості у їх оцінюванні судом, зокрема щодо критеріїв, за якими визначається можливість їх прийняття та дослідження в судовому засіданні. Ця проблематика особливо актуалізується у випадках дистанційного розгляду справ, коли подання, долучення та оцінювання доказів відбуваються виключно в електронному форматі, що зумовлює потребу в додаткових гарантіях їх автентичності та достовірності. Відповідно до ч. 4 ст. 100 ЦПК України «учасник справи, який подає копію електронного доказу, повинен зазначити про наявність у нього або іншої особи оригіналу електронного доказу»[11]. Таке положення законодавець запровадив як прояв процесуальної обережності з метою забезпечення автентичності електронних доказів і запобігання можливим маніпуляціям із їх змістом. Вимога щодо наявності оригіналу електронного документа покликана гарантувати суду можливість перевірки справжності поданого доказу в разі виникнення сумнівів щодо його походження чи припущення про зміну первинної інформації. Разом із тим подібний підхід свідчить про певну недовіру до цифрового формату

[11] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV.

доказування, оскільки законодавець продовжує орієнтуватися на матеріальну (паперову) форму як більш надійну та перевірену. Така тенденція демонструє, що українська система цивільного судочинства все ще перебуває на етапі поступової адаптації до повноцінного функціонування в межах цифрового правового середовища, де електронні докази повинні отримати рівнозначну процесуальну силу поряд із традиційними письмовими формами.

З огляду на окреслені обставини варто звернути увагу на потенційну проблему недостовірності електронних доказів і складність перевірки їх автентичності в оригінальній формі. Це пов'язано з тим, що на сучасному етапі законодавство ще не виробило чітких і уніфікованих критеріїв оцінювання таких юридичних фактів, а судова практика перебуває на етапі формування відповідних підходів. У результаті виникає ситуація, коли суд змушений оцінювати електронні докази за аналогією з традиційними формами доказування, що не завжди відображає специфіку їх технічної природи та способів фіксації інформації.

Відсутність єдиного стандарту автентифікації електронних доказів створює суттєві труднощі для правозастосовної практики, адже саме стандарти визначають допустимі межі перевірки достовірності інформації, зафіксованої в цифровій формі. На відміну від письмових або речових доказів електронні носії можуть піддаватися технічним змінам, копіюванню чи редагуванню без очевидних слідів втручання, що ускладнює підтвердження їх первинності. Тому у вітчизняному цивільному процесі виникає потреба в розробленні чітких нормативних приписів і технічних вимог, які б регулювали порядок ідентифікації, подання, зберігання та перевірки електронних доказів. У перспективі це сприятиме забезпеченню більшої правової визначеності, підвищенню рівня довіри до результатів судового розгляду й утвердженню принципу достовірності в цифровому вимірі цивільного судочинства.

Отже, наголосимо, що сучасний етап розвитку цивільного судочинства безпосередньо пов'язаний із впровадженням цифрових технологій та формуванням технічного підґрунтя для електронного функціонування судової системи. Процес цифровізації судочинства зумовив появу нових технічних можливостей для цивільного суду, які законодавство не може ігнорувати, адже вони стали необхідною складовою реалізації принципу доступності правосуддя. Водночас, незважаючи на наявність такого інноваційного підґрунтя, судова практика все ще стикається з низкою проблем, пов'язаних із відсутністю усталених підходів до тлумачення та оцінювання електронних явищ, зокрема щодо визначення критеріїв достовірності електронних доказів. Судова система перебуває в процесі активного адаптаційного етапу, коли їй доводиться одночасно опановувати нові технологічні інструменти та виробляти практичні навички їх застосування в процесі доказування з метою ухвалення законних і обґрунтованих судових рішень.

Поступове впровадження цифрових технологій у процес доказування свідчить про трансформацію традиційних уявлень про засоби доведення та оцінювання доказів у цивільному судочинстві. Електронні докази поступово формують новий рівень правової культури, де *технічна достовірність* поєднується з процесуальною формою, а суд виступає не лише суб'єктом

оцінки фактів, а й арбітром між технологічними можливостями та правовими гарантіями. Відтак питання інтеграції електронних доказів у процесі доказування набуває не лише практичного, а й методологічного значення, адже від правильності їх правового тлумачення залежить ефективність усього механізму цивільного судочинства.

Отже, доказування виступає однією з ключових складових здійснення правосуддя у цивільних справах. Діяльність суду й учасників процесу в цьому контексті має специфічний характер і становить необхідний елемент реалізації процесуальних прав, що врегульовані нормами цивільного законодавства. У межах розгляду кожного спору така діяльність набуває власного процесуального змісту, зумовленого характером справи та наданими доказами. Безперечно, застосування електронних доказів безпосередньо залежить від послідовності та логічності формування доказової бази, що сьогодні охоплює широкий спектр засобів доказування, серед яких особливе місце посідають електронні докази як прояв сучасних тенденцій цифровізації судочинства.

Така правова категорія, як доказування, безперечно, впливає на процесуальну форму і зміст цивільного процесу. Логічність, послідовність, підсумок вирішення цивільної справи залежать від зазначення черговості здійснення дій учасниками судового процесу та врахування таких елементів, як актуальність юридичних фактів та їх своєчасність. Процесуальна форма, яка пронизує судочинство з цивільних справ, є не формальністю, якою можна зневажати, а законодавчо встановленим засобом здійснення правосуддя, тому суворе її дотримання, юридичне обґрунтування, кваліфіковане укладання цивільно-процесуальних документів становить одну з основних умов, яка забезпечує законність і обґрунтованість судових рішень.

Підкреслимо, що положення ЦПК України надають суду й учасникам процесу можливість використовувати всі види доказів, передбачені законом, якщо вони мають значення для розгляду конкретної справи. У зв'язку з наведеним необхідним вбачаємо чітке визначення та розмежування характерних *ознак електронних доказів*, оскільки вони становлять окремий різновид доказової бази, який має власну специфіку та техніко-правові особливості, що відрізняють їх від традиційних форм доказування.

Електронні докази в цивільному процесі становлять окремий різновид доказової бази, що передбачає інформацію в цифровій або електронній формі, яка містить відомості, значущі для встановлення обставин справи. Вони можуть включати електронні документи, мультимедійні файли, вебсторінки, тексти, голосові повідомлення, метадані, бази даних та інші цифрові носії, що зберігаються на різних пристроях. Формат таких доказів визначає спосіб їх подання, фіксації, збереження та подальшої оцінки судом, адже технічні характеристики безпосередньо впливають на їх автентичність і допустимість у процесі. Особливість електронних доказів полягає у їх технічній специфіці та різноманітності форматів, що вимагає застосування відповідних процесуальних правил для забезпечення достовірності та законності доказової діяльності в цивільному судочинстві.

Можемо визначити *характерні особливості* таких доказів, зокрема: вони можуть бути нестійкими, за певних обставин інформація в пам'яті пристрою

може бути змінена або втрачена; їх можна копіювати без втрати якості необмежену кількість разів, і будь-яка наступна копія не буде відрізнятися від оригіналу; вони можуть бути як створені людиною, так і бути результатом функціонування інформаційної системи; вони потребують специфічного порядку збирання, перевірки й оцінювання; вони вільно переміщуються в електронній мережі без технічного носія та не мають нерозривного зв'язку з матеріальним носієм; їх не видно неозброєним оком: вилучити їх подеколи може лише спеціаліст; вони можуть бути підробкою з використанням штучного інтелекту; вони залежать від енергопостачання: у разі розрядки пристрою або недостатності пам'яті система накладає (записує) нову інформацію замість попередньої, а це значить, що й докази можуть бути знищені; комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів; інформація може бути видалена автоматично або може трапитися збій видалення конкретних файлів.

Зауважимо, таким чином, що кожен із зазначених електронних доказів відповідно до своєї характеристики повинен мати дуже вузькі параметри вивчення та визнання їх достовірності при розгляді цивільної справи, і тому вважаємо, що кожен із них у майбутньому все ж таки матиме визнані законодавчо правила прийняття при розгляді цивільної справи.

Так, наприклад, достовірність звуко- та відеозапису потрібно перевіряти за технічними аспектами їх створення, а саме за допомогою якого пристрою їх робили, чи не застосовувався при цьому штучний інтелект, і цю перевірку може провести лише спеціаліст (експерт), який знається на цій справі.

Оцінювання електронних доказів – це розумово-процесуальна діяльність суду й учасників справи, яка направлена на формування остаточного висновку щодо підтвердження або спростування фактів предмета доказування за допомогою електронних доказів. Зміст оцінювання електронного доказу формують індивідуальні (належність, допустимість і достовірність) та системні (достатність і взаємозв'язок доказів) критерії їх оцінювання[12].

Відзначимо, що сучасні цивільні суди все активніше використовують електронні докази в процесі розгляду справ, що є відображенням загальної тенденції цифровізації та технічного прогресу, який охопив і судову систему. Водночас слід враховувати, що таке застосування може породжувати різноманіття, багатогранні та унікальні ситуації під час оцінювання електронних доказів як з боку учасників цивільного процесу, так і під час їх розгляду та прийняття судом. Це вимагає від учасників і суду підвищеної уваги до питань автентичності, достовірності та процесуальної допустимості таких доказів.

Спробуємо зробити, деякі нотатки щодо прийняття окремих різновидів таких електронних фактів:

– електронні докази слід розглядати у форматі лише електронних даних на портативних носіях чи в мережі Інтернет, і тому подача таких доказів не може бути у вигляді скриншотів, інтернет-посилань чи копій, учасники справи

[12] Феннич В. П. Оцінка електронних доказів у цивільному процесі (на прикладах окремих категорій судових справ). *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. Вип. 71. С. 375. DOI: https://doi.org/10.24144/2307-3322.2022.71.63.

повинні бути зацікавленні в доцільності збереження оригіналу таких доказів на відповідних носіях;

– суд може розглядати лише ті електронні докази (листи), які надходять з існуючої електронної пошти і підтверджують належність конкретному учаснику (персоніфікацію) цивільного судочинства;

– скриншоти слід розглядати як допустимі докази, проте слід враховувати, що вони не мають повної автентичності, і тому їх оцінювання судом здійснюється з урахуванням можливих сумнівів щодо достовірності;

– електронні (цифрові) докази є більш вразливими до змін або підробки порівняно з традиційними формами доказів, що підкреслює їх особливу значущість при оцінюванні та прийнятті до розгляду судом;

– цивільні суди повинні користуватися певною системою на майбутнє, яка дасть змогу розпізнати використання штучного інтелекту та підробку електронного доказу (відео-, аудіозапис і т. ін.), це є дуже важливим для достовірності такого доказу.

Отже, використання електронних доказів у цивільному судочинстві сьогодні є досить різноманітним і водночас неоднозначним явищем. Незважаючи на це, їх застосування поступово набирає ваги і стає все більш поширеним серед учасників судових справ, оскільки з'являється можливість фіксувати і подавати інформацію у зручних цифрових форматах, що відповідає сучасним технологічним можливостям.

Водночас слід зважати на складність розпізнання та оцінки електронних доказів. Це пов'язано з тим, що ЦПК України лише формально визнає існування таких доказів, проте конкретні правила їх дослідження, оцінювання та врегулювання спірних питань щодо їх застосування залишаються невизначеними. Така ситуація створює певну невизначеність у правозастосуванні: суд змушений оцінювати електронні докази за загальними процесуальними принципами, водночас враховуючи технічні особливості їх формату, способу збереження та подання. Це підкреслює необхідність подальшого розвитку законодавчих і методичних норм, які б забезпечили уніфіковані підходи до використання електронних доказів, підвищили їх достовірність і правову значущість у процесі ухвалення обґрунтованих судових рішень.

Таким чином, питання застосування електронного формату доказової бази залишається перспективною сферою дослідження серед науковців і практикуючих юристів. Воно відкриває широкі можливості для аналізу процесуальних особливостей та специфіки логічної структури електронних фактів, що використовуються учасниками цивільного судового спору. Значущість електронного доказу сьогодні визначається не лише його матеріальним носієм чи способом фіксації, але й процесуальним змістом, що безпосередньо впливає на правильність, законність і обґрунтованість судового рішення в цивільній справі.

Отже, інтеграція електронних доказів у цивільний процес є не лише сучасною тенденцією, а й необхідністю для забезпечення повноти та достовірності доказової бази, а також реалізації принципу змагальності сторін і процесуальної форми судового розгляду.

ВИСНОВКИ

За результатами проведеного дослідження встановлено, що застосування електронної форми доказової бази в цивільному судочинстві залишається одним із найбільш динамічних і перспективних напрямів сучасних наукових досліджень, що перебуває у фокусі уваги як теоретиків права, так і практичних юристів. Ця сфера відкриває значний потенціал для глибокого осмислення процесуальних характеристик електронних доказів, а також для аналізу їх внутрішньої логічної структури, способів формування, збереження та використання електронних фактів учасниками цивільного процесу.

Так, проведений аналіз підтверджує, що у сучасних умовах значущість електронного доказу не обмежується виключно його технічним носієм чи способом фіксації інформації. Вирішальне значення набуває саме його процесуальний зміст, що визначає допустимість, належність і достовірність такого доказу. Саме ці характеристики безпосередньо впливають на формування внутрішнього переконання суду, а відтак – на забезпечення законності, обґрунтованості та справедливості судового рішення у цивільній справі. Усвідомлення зазначених аспектів зумовлює необхідність подальшого комплексного дослідження електронних доказів як самостійного та складного інституту цивільного процесуального права.

Водночас окреслені особливості електронних доказів не можуть бути належним чином реалізовані поза межами чітко визначеної процесуальної форми цивільного судочинства. Саме процесуальна форма забезпечує нормативну впорядкованість збирання, подання, дослідження та оцінки електронних доказів, надаючи їм статус повноцінного засобу доказування. У цьому контексті електронні докази виступають не лише як інформаційні носії цифрових фактів, а як елементи процесуальної діяльності, що підпорядковуються загальним засадам цивільного процесу, зокрема принципам змагальності, диспозитивності, процесуальної рівності сторін і судового контролю.

Поступове впровадження цифрових технологій у процес доказування свідчить про трансформацію традиційних уявлень про засоби доведення та оцінювання доказів у цивільному судочинстві. Електронні докази поступово формують новий рівень правової культури, де *технічна достовірність* поєднується з процесуальною формою, а суд виступає не лише суб'єктом оцінки фактів, а й арбітром між технологічними можливостями та правовими гарантіями. Відтак питання інтеграції електронних доказів у процесі доказування набуває не лише практичного, а й методологічного значення, адже від правильності їх правового тлумачення залежить ефективність усього механізму цивільного судочинства.

Також, можна дістатися висновку, що практична реалізація стандарту електронного доказування потребує, поєднання трьох рівнів: законодавчого (уточнення положень ЦПК України щодо допустимості та оцінки електронних доказів); методичного (розроблення рекомендацій для судів та учасників процесу) та інституційного (формування єдиних підходів у практиці судової системи України). Саме через усталення правових позицій судової системи можливе створення стабільних орієнтирів для підходів до оцінки цифрових даних. Виникнення єдиного стандарту електронних доказів має розглядатися

як елемент модернізації цивільного судочинства України в умовах цифровізації правових відносин. Його метою повинно стати не ускладнення доказового процесу, а забезпечення передбачуваності судових рішень, процесуальної рівності сторін та підвищення довіри до правосуддя. Саме науково обґрунтована модель такого стандарту здатна стати підґрунтям для формування уніфікованої та узгодженої судової практики щодо застосування електронних доказів.

АНОТАЦІЯ

Розділ монографії присвячено дослідженню правової природи електронних доказів, їх процесуального значення та впливу на формування судового рішення в цивільному судочинстві. Електронні докази вирізняються особливою правовою природою, що відрізняє їх від класичних письмових чи речових доказів. Їх унікальність полягає у нематеріальній формі існування, залежності від технічних засобів відтворення, можливості швидкого копіювання без втрати змісту, а також у специфічних характеристиках автентичності, цілісності та достовірності. Отже, такі особливості зумовлюють необхідність вироблення спеціальних процесуальних підходів до оцінки електронних доказів та визначення їх належності й доступності у цивільному судочинстві.

В результаті наукового осмислення було визначено, що сучасні цивільні суди все активніше використовують електронні докази в процесі розгляду справ, що є відображенням загальної тенденції цифровізації та технічного прогресу, який охопив і судову систему. Також було з'ясовано, що таке застосування може породжувати різноманіття, багатогранні та унікальні ситуації під час оцінювання електронних доказів як з боку учасників цивільного процесу, так і під час їх розгляду та прийняття судом, що вимагає від учасників і суду підвищеної уваги до питань автентичності, достовірності та процесуальної допустимості таких доказів.

Запропоновані, деякі нотатки щодо прийняття окремих різновидів електронних фактів:

– електронні докази слід розглядати у форматі лише електронних даних на портативних носіях чи в мережі Інтернет, і тому подача таких доказів не може бути у вигляді скріншотів, інтернет-посилань чи копій, учасники справи повинні бути зацікавленні в доцільності збереження оригіналу таких доказів на відповідних носіях;

– суд може розглядати лише ті електронні докази (листи), які надходять з існуючої електронної пошти і підтверджують належність конкретному учаснику (персоніфікацію) цивільного судочинства;

– скріншоти слід розглядати як допустимі докази, проте слід враховувати, що вони не мають повної автентичності, і тому їх оцінювання судом здійснюється з урахуванням можливих сумнівів щодо достовірності;

– електронні (цифрові) докази є більш вразливими до змін або підробки порівняно з традиційними формами доказів, що підкреслює їх особливу значущість при оцінюванні та прийнятті до розгляду судом;

– цивільні суди повинні користуватися певною системою на майбутнє, яка дасть змогу розпізнати використання штучного інтелекту та підробку електронного доказу (відео-, аудіозапис і т. ін.), це є дуже важливим для достовірності такого доказу.

Література

1. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV.

2. Андрійцьо В. Д. Докази як об'єкт збору на етапі збирання доказів у цивільному процесі. *Право і суспільство.* 2013. № 4. С. 33-38.

3. Павлова Ю. С. Електронний доказ в цивільному процесі: зарубіжний досвід. *Актуальні проблеми вітчизняної юриспруденції.* 2023. № 2. С. 29–33. DOI: https://doi.org/10.32782/39221466.

4. Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо їх дослідження судом. *European Political and Law Discourse.* 2018. Vol. 5, Iss. 2. P. 299–305.

5. Полуніна О. О. Електронні докази як особливий засіб доказування у цивільному процесі. *Реформування цивільного процесуального права в умовах інтеграційних процесів в Україні* : матеріали Всеукр. наук.-практ. інтернет-конф. ім. Ю. С. Червоного (Одеса, 18 груд. 2020 р.) / за заг. ред. Н. Ю. Голубєвої. Одеса : Фенікс, 2020. С. 42-44. URL: https://dspace.onua.edu.ua/bitstreams/b255fc75-8f6e-4093-bda2-358afa34faa5/download (дата звернення: 02.02.2026).

6. Electronic Evidence in Civil and Administrative Proceedings : Guidelines adopted by the Committee of Ministers of the Council of Europe on 30 January 2019 and explanatory memorandum / Council of Europe. Council of Europe, 2019. P. 15. URL: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 (дата звернення: 02.02.2026).

7. Грабовська О. О. Теоретико-правові проблеми доказування у цивільному процесі України : дис. … д-ра юрид. наук : 12.00.03. Київ, 2018. 563 с.

8. Феннич В. П. Оцінка електронних доказів у цивільному процесі (на прикладах окремих категорій судових справ). *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. Вип. 71. С. 370–375. DOI: https://doi.org/10.24144/2307-3322.2022.71.63.

Information about the author:
Perunova Olena Mukolaivna,
Candidate of Juridical Sciences, Associate Professor,
Associate Professor of the Department of Accounting and Auditing
Kharkiv national automobile and Highway University,
25, Yaroslav Mudryi Street, Kharkiv, 61002, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-13

КОНВЕНЦІЯ РАДИ ЄВРОПИ ПРО КІБЕРЗЛОЧИННІСТЬ ЯК ОСНОВА КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ СУСПІЛЬНИХ ВІДНОСИН У КІБЕРПРОСТОРІ В УКРАЇНИ

Політова А. С.

ВСТУП

Відзначимо, що новинами про кіберзлочини вже нікого не дивують, а така інформація сприймається як звичайна. Правоохоронні органи адаптуються до нових викликів та розвивають нові механізми у сфері кіберзахисту. Захист відбувається на кількох рівнях – як на суто технічному й програмному, так і на рівні законодавства. Країни ЄС та США вже мають відповідну базу знань і процедур, які ефективно працюють у сфері кіберзахисту. Україна так само мало не щодня відповідає все новим і новим викликам і працює над запобіганням таким злочинам[1].

Досліджуючи світові тенденції деякі вчені відзначають, що кількість здійсненних кібератак щорічно зростає, а їх характер дедалі стає складнішим. Фішингові атаки є лідерами серед кіберзлочинів у світі, які демонструють тенденціюдо подальшого збільшення. У 2023р. кількість атак із використанням зловмисного програмного забезпечення становила 6,06 млрд випадків, що свідчить про масштабність проблеми. Глобальні фінансові втрати від кіберзлочинності у 2023 р. склали понад 7,1 трлн дол. США, а до 2029 р. можуть зрости до15,63 трлн дол. США. Основними наслідками для організацій від втрати конфіденційної інформації є: втрата доходу (56,6 %), погіршення репутації (38,9 %) та послаблення конкурентних позицій (35,8 %). Найбільш вразливими залишаються освітній сектор, урядові структури, сектор розваг та фінансові установи. У цих галузях є значна кількість інцидентів із використанням зловмисного програмного забезпечення. США, росія, Франція та Нідерланди є основними країнами-джерелами кібератак, тоді як Канада та Сінгапур демонструють найвищий рівень непокоєння щодо можливих загроз[2]. Окрім того, відповідно до світового рейтингу кіберзлочинності (*World Cybercrime Index*), який був розроблений авторами з Оксфордського університету та Університету Нового Південного Вельсу, найпершою в рейтингу кіберзлочинності стала Росія (58,39 бала), за нею з великим відривом ідуть Україна (36,44 бала), Китай (27,86 бала), США (25,01 бала),

[1] Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. *Mind.ua*. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu (дата звернення: 14.02.2026).

[2] Дикий, А., Савіцький, В., Савчук, С., & Соха, А. (2025). Світові тенденції кіберзлочинності та загрози інформаційній безпеці держав. *Society and Security*, (1(7), 63–74. https://doi.org/10.26642/sas-2025-1(7)-63-74

Нігерія (21,28 бала) та Румунія (14,83 бала). Велика Британія посідає восьме місце у списку (9,01 бала)[3].

Реформа законодавства України, у тому числі й Кримінального кодексу, привертає увагу до питання імплементації у національне законодавство положень міжнародних актів, у тому числі й протидії злочинності. Враховуючи цей аспект, метою нашого дослідження є імплементація положень Конвенції Ради Європи про кіберзлочинність у Кримінальний кодекс України щодо кримінальної відповідальності за кіберзлочини.

1. Конвенція Ради Європи про кіберзлочинність: аналіз окремих положень

І. І. Нагорний вважає, що популярність використання цифрових платформ, перехід до електронного формату документообігу, а також віртуального простору в усіх сферах суспільного життя зумовило виникнення нових форм злочинної поведінки, які називають «кіберзлочини», що за своїм змістом відрізняються від традиційних кримінальних правопорушень за своїм масштабом, способами вчинення та наслідками. Злочини у сфері ІТ вчиняються дистанційно та виходять за межі юрисдикції держав, унаслідок чого національні правові й правоохоронні системи виявляються нездатними до оперативного реагування на нові виклики й загрози [4].

Відзначимо, що перші спроби уніфікувати правові підходи щодо протидії кіберзлочинам у країнах Європи відбувалися під егідою ради Європи. Одне з найбільш ґрунтовних діянь, зорієнтованих на регулювання цієї проблеми, є ухвалення Рекомендацією Європи 23 листопада 2001 р. Конвенції про кіберзлочинність (ратифікована 1 липня 2004 р.).

У преамбулі Конвенції про кіберзлочинність зазначено, що Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами та даними, шляхом установлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва[5].

---

[3] Крайня В. Світовий рейтинг кіберзлочинності очолила Росія. Україна посіла друге місце. *ms.detector.media*. URL: https://ms.detector.media/kiberbezpeka/post/34647/2024-04-11-svitovyy-reytyng-kiberzlochynnosti-ocholyla-rosiya-ukraina-posila-druge-mistse/ (дата звернення: 14 .02.2026).

[4] Нагірний І. П. Еволюція правової протидії злочинам у сфері інформаційних технологій: історичні витоки та сучасні виклики. *Європейський правничий часопис*. 2026. С. 141-147. URL: https://doi.org/10.36919/3041-1149(print).11.2025.141-147 (дата звернення: 14.02.2026).

[5] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

Отже, зупинимося більш детально на загальній характеристиці цієї Конвенції.

Розділ І. Використання термінів Конвенції включає лише одну статтю, де закріплено визначення термінів, що застосовуються, зокрема:

- «Комп'ютерна система» – будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних;

- «Комп'ютерні дані» – будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

- «Постачальник послуг» означає:

і. будь-яку державну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та

іі. будь-яку іншу установу, яка обробляє або зберігає комп'ютерні дані від імені такої комунікаційної послуги або користувачів такої послуги;

- «Дані про рух інформації» – будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги[6].

Саме Розділ ІІ. Заходи, які мають здійснюватися на національному рівні Конвенції має велике значення для нашого дослідження, адже саме положення цього розділу при ратифікації Конвенції повинні бути імплементовані у національне законодавство – Закон України про кримінальну відповідальність та Кримінальний процесуальний кодекс України.

Зупинимося більш детально на основних аспектах Частини 1. Матеріальне кримінальне право Розділ ІІ Конвенції. Проведений аналіз дозволяє відзначити, що ця частина включає п'ять заголовків, а саме:

Заголовок 1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

- ст. 2. Незаконний доступ, тобто навмисний доступ до цілої комп'ютерної системи або її частини без права на це; таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою;

- ст. 3. Нелегальне перехоплення – навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані; таке правопорушення було вчинене з

[6] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою;

- ст. 4. Втручання у дані – навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

- ст. 5. Втручання у систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це;

- ст. 6. Зловживання пристроями – навмисне вчинення, без права на це:

a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином:

i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 вище;

ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5; та

b. володіння предметом, перерахованим у підпунктах a. і або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2–5;

Заголовок 2. Правопорушення, пов'язані з комп'ютерами:

- ст. 7. Підробка, пов'язана з комп'ютерами, тобто навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти;

- ст. 8. Шахрайство, пов'язане з комп'ютерами – навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних,

b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи;

Заголовок 3. Правопорушення, пов'язані зі змістом:

- ст. 9. Правопорушення, пов'язані з дитячою порнографією, тобто навмисне вчинення, без права на це, наступних дій:

a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;

b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;

c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;

d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;

e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації;

Заголовок 4. Правопорушення, пов'язані з порушенням авторських та суміжних прав:

- ст. 10. Правопорушення, пов'язані з порушенням авторських та суміжних прав, яке полягає: «1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем»[7].

Окрім того, у Заголовку 5. Додаткова відповідальність і санкції передбачено:

- ст. 11. Спроба і допомога або співучасть, тобто навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів, перерахованих у статтях 2-10 цієї Конвенції, з метою вчинення такого злочину; навмисну спробу вчинити будь-який зі злочинів, перерахованих у статтях 3-5, 7, 8, 9.1.a та 9.1.c цієї Конвенції;

- ст. 12. Корпоративна відповідальність, тобто юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи.

Окрім того, така фізична особа має займати керівну посаду в рамках юридичної особи, в силу:

a. повноважень представляти цю юридичну особу;

b. повноважень приймати рішення від імені цієї юридичної особи;

c. повноважень здійснювати контроль в рамках цієї юридичної особи[8].

- ст. 13. Санкції і заходи – звернута увага на два аспекти:

По-перше, кримінальні правопорушення, встановлені відповідно до статей 2-11, каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі;

[7] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

[8] Там само.

По-друге, юридичні особи, які несуть відповідальність відповідно до статті 12, каралися ефективними, пропорційними і переконливими кримінальними або некримінальними санкціями або заходами, включаючи грошові санкції.

Таким чином, можна відзначити, що у Частині 1. Матеріальне кримінальне право Конвенції визначено діяння, за повинна наставати кримінальна відповідальність. Окрім того, визначено особливості кримінальної відповідальності у співучасті за такі діяння, покарання для фізичних та юридичних осіб. Також ми погоджуємося з тим, що рівень можливостей, які отримують зловмисники, й тенденція до збільшення кількості злочинів у сфері комп'ютерних інформаційних технологій становлять загрозу не лише демократичним перетворенням та розвитку інформаційного суспільства в Україні, а й національній безпеці загалом[9].

2. Кіберзлочини: поняття та види кримінальних правопорушень

Аналізуючи положення Кримінального кодексу України зауважимо, що поняття «кіберзлочини», «кіберзлочинність», «комп'ютерні кримінальні правопорушення» або «кримінальні правопорушення у сфері інформаційних технологій» не врегульовано. Окрім того, ці дефініції не знайшли однозначного формулювання й у працях вчених, які також пропонуються різні критерії класифікації таких кримінально протиправних діянь.

Так, наприклад, під кіберзлочинністю пропонується розуміти сукупність правопорушень, скоєних у «кіберпросторі» за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж та комп'ютерних даних[10]. Натомість інші вчені стверджує, що кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [11]. І. І. Васильковський відзначає, що кіберзлочинність (або «злочин з використанням комп'ютерних технологій») – це економічний злочин, скоєний з використанням обчислювальної техніки та мережі Інтернет. Приклади кіберзлочинності можуть бути різними: розповсюдження вірусів, незаконне вивантаження інформації, фішинг і фармінг, а також розкрадання особистої інформації (наприклад, реквізитів банківських рахунків). До цієї категорії відносять тільки ті економічні злочини, в яких основним (а не допоміжним або

[9] Dulepa V. P. Criminological characteristics of cybercrime. *Juridical scientific and electronic journal*. 2021. No. 11. P. 592–595. DOI: https://doi.org/10.32782/2524-0374/2021-11/147 (date of access: 17.02.2026).

[10] Shak R. Concepts and Types of Cyber Offenses in Criminal Law. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 44. P. 325–335. DOI: https://doi.org/10.23939/law2024.44.325 (date of access: 14.02.2026).

[11] Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посібн. Харків : Право, 2014. 284 с.

супутнім) інструментом скоєння злочину є комп'ютер, Інтернет або електронні носії інформації та пристрої[12].

Саме тому можна погодитися із С. В. Корзун, яка відзначає, що поняття «кіберзлочинність» має багатовекторне розуміння, що обумовлено його поширеністю в різних сферах суспільних відносин (економічна система, політична система, міжнародні відносини, соціальна сфера), різноманітними наслідками (економічні, соціальні, людські жертви, психологічні та інші) та впливом на національну безпеку (інформаційну, безпеку державного кордону, політичну, економічну, енергетичну, продовольчу та інші)[13].

Що ж нормативного визначення, то, зокрема, у Законі України від 5 жовтня 2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» відзначено, під кіберзлочином (комп'ютерним злочином) слід розуміти суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [14]. Такий підхід законодавця свідчить про використання термінів «кіберзлочини» та «комп'ютерні злочини» як синонімів. Але, як вважає О. І. Денькович, недоліком вказаного законодавчого визначення кіберзлочинності (так само як і визначення злочинності в межах статистичного підходу) є те, що воно відображає НЕ сутність та зміст поняття (тобто сукупність його істотних, необхідних і достатніх ознак), а його обсяг (тобто вказує на об'єкти, як за методологічними підходами доктринальні кримінологічні визначення кіберзлочинності виходять з того, що цей вид злочинності є сукупністю кримінальних правопорушень, їх арифметичною сумою. Різняться вони у тому, які саме кримінальні правопорушення потрібно включати в обсяг цього поняття, тобто якими ознаками характеризується кіберзлочин як одиничний елемент вказаної суми, чим він відрізняється від інших видів кримінальних правопорушень [15].

М. Ю. Яцишин виокремлює такі критерії, які дозволяють вченому узагальнити основні кваліфікаційні ознаки кібернетичних злочинів як основи їх класифікації:

---

[12] Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2 (10-11). С. 276–28.

[13] Корзун С. В. Понятійно-категоріальний апарат державної кримінально-правової політики протидії кіберзлочинам. *Економіка, управління та адміністрування*. 2025. № 1(111). С. 131–145. DOI: https://doi.org/10.26642/ema-2025-1(111)-131-145 (дата звернення: 17.02.2026).

[14] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.02.2026).

[15] Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 17.02.2026).

1. Кіберзлочини, що виникли в результаті створення і поширення ІКТ, та завдають шкоду учасникам кіберпростору шляхом порушення конфіденційності, цілісності та доступності ІКТ. До цього виду злочинних діянь відносяться: незаконний доступ; нелегальне перехоплення; втручання в дані; втручання в систему; зловживання пристроями.

2. Традиційні злочини, вчинені з використанням ІКТ: тероризм; підробка; шахрайство; переслідування, вимагання, порушення права інтелектуальної власності та ін.

3. Кіберзлочини, що пов'язані зі створенням та розповсюдженням нелегального контенту за допомогою ІКТ. До цієї групи злочинних діянь відносимо будь-які цифрові операції із забороненою інформацією, яку становить дитяча порнографія, расистський та ксенофобний матеріал тощо[16].

Але А. В. Боровик та І. М. Копотун вважають, що основною сутнісною ознакою кіберзлочину є те, що це діяння, сама можливість вчинення якого випливає з особливих можливостей інформаційно-телекомунікаційних технологій, які використовуються для завдання шкоди суспільним відносинам[17].

Такі різні підходи щодо визначення ознак кіберзлочинів дозволяють відзначити, що до основними їх властивостями, на нашу думку, є: вчинення діяння у кіберпросторі або із застосуванням інформаційно-комунікаційних технологій; використання специфічних способів реалізації кримінально протиправного наміру (несанкціонованого доступу, втручання в роботу систем, шкідливе програмне забезпечення, маніпулювання даними, соціальна інженерія); спрямованість посягання на інформацію, цифрові ресурси та інфраструктуру; анонімність або псевдоанонімність суб'єкта; транснаціональний організований характер таких кримінальних правопорушень; високий рівень латентності та складність їх виявлення і доказування у кримінальному провадженні.

Окрім того, звернемо увагу й на те, що в основу класифікації кібезлочинів вчені пропонують різні критерії, враховуючи, у тому числі, й положення міжнародного кримінального права. Так, наприклад, Д. Ю. Дрижакова, О. О. Горішній та М. М.Тараненко досліджуючи питання ефективності правових механізмів запобігання кіберзлочинності в Україні відзначають, що відповідно до міжнародних підходів кіберзлочини поділяються на кілька основних категорій:

- злочини проти комп'ютерних систем (наприклад, несанкціонований доступ до інформації, її знищення чи модифікація);
- злочини з використанням інформаційних технологій (шахрайство, розповсюдження шкідливого програмного забезпечення, викрадення персональної інформації);

[16] Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. Т. 53, № 5. С. 92–99. DOI: https://doi.org/10.5281/zenodo.2009191 (дата звернення: 14.02.2026).

[17] Боровик А. В. Кіберзлочини в Україні (кримінально-правово характеристика) : навч. посіб. Луцьк : ВолиньПоліграф, 2019. 304 с.

- злочини, пов'язані з контентом (кібертероризм, розповсюдження незаконної інформації, зокрема пропаганди насильства або дитячої порнографії)[18].

Натомість В. Г. Кундеус пропонує класифікувати за такими видами залежно від об'єкту посягання кіберзлочини (комп'ютерні злочини):

1) Злочини, вчинені у кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами КК України. Такі злочини посягають на різні об'єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права на об'єкти інтелектуальної власності, власність, господарські відносини, права та свободи тощо. Ознакою віднесення цих злочинів до кіберзлочинів є те, що вони вчиняються з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. Наприклад: викрадення реквізитів платіжних карток (фішинг, вішинг, шиммінг, скимінг); незаконні фінансові операції з використанням платіжних карток або їх реквізитів, які не ініційовані або не підтверджені її власником (кардінг); заволодіння коштами через фіктивні Інтернет-магазини, Інтернет-аукціони, сайти та інші засоби телекомунікації (онлайн-шахрайство); порушення авторського права і суміжних прав шляхом незаконного розповсюдження програмних продуктів через комп'ютерні мережі (піратство) тощо.

2) Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що передбачені Розділом XVI КК України. Ознакою віднесення цих злочинів до комп'ютерних є те, що вони посягають на відносини, що виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку[19].

Але є дослідники, які не виокремлюючи критеріїв (підстав) для класифікації кіберзлочинів, просто надають їх перелік. Так, наприклад, Н. В. Савчук наводить рейтинг найбільш суттєвих кіберзлочинів:

- фальшиві рахунки на оплату із Інтернет-магазину (підроблені рахунки, які розсилаються електронною поштою, містять посилання на шкідливі програми);
- фальшиві повідомлення про доставку товару (злочинці часто видають себе за популярні поштові служби та розсилають листи, які під прикриттям повідомлення містять віруси);
- фішинг – заволодіння платіжними особистими даними користувачів шляхом обману на шахрайське їх використання, що пов'язано із електронною комерцією;

[18] Дрижакова Д. Ю., Горішній О. О., Тараненко М. М. Оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні. 2025. URL: https://doi.org/10.5281/zenodo.15074665 (дата звернення: 14.02.2026).

[19] Кундеус, В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 44-45.

- крадіжка особистих даних через фальшиве анкетування (користувачі, які люблять заповнювати різного роду анкети в обмін на різні подарунки, потрапляють до групи ризику);

- компроментування популярних веб-сайтів (кіберзлочинці атакують ті сайти, які відвідує найбільша кількість користувачів);

- відправлення результатів пошукових запитів (користувачам розсилаються посилання на веб-сайти при використанні яких комп'ютер отримує вірус, що призводить значних збитків);

- вірусна реклама;

- небезпечні привітальні листівки;

- підроблені сайти благодійних фондів;

- шахрайство на розпродажу (відвідавши сайт користувачі, клікнушви по банерній рекламі дешевого мобільного телефону, стають жертвами програми – троянський кінь)[20].

У дослідженні «Cyber crime: A review of the evidence» Dr. Mike McGuire (University of Surrey) та Samantha Dowling (Home Office Science) виокремлюють:

- Кіберзалежні злочини – це правопорушення, які можуть бути вчинені лише за допомогою комп'ютера, комп'ютерних мереж або іншої форми ІКТ. Ці діяння включають поширення вірусів та іншого шкідливого програмного забезпечення, хакерство та розподілені атаки типу «відмова в обслуговуванні» (DDoS), тобто перевантаження Інтернет-серверів для виведення з ладу мережевої інфраструктури або веб-сайтів. Кіберзалежні злочини – це, перш за все, діяння, спрямовані проти комп'ютерів або мережевих ресурсів, хоча атаки можуть мати й вторинні наслідки, такі як шахрайство.

- Кіберзлочини – це традиційні злочини, масштаб або охоплення яких збільшуються завдяки використанню комп'ютерів, комп'ютерних мереж або інших ІКТ. На відміну від кіберзалежних злочинів, їх все ще можна вчиняти без використання ІКТ. Такими типами кіберзлочинів є:

шахрайство (включаючи масовий маркетинг, фішингові електронні листи та інші види шахрайства; шахрайство в онлайн-банкінгу та електронній комерції);

крадіжка (включаючи крадіжку особистої інформації та даних, пов'язаних із ідентифікацією);

сексуальні злочини проти дітей (включаючи ґрумінг і створення та/або розповсюдження сексуальних зображень) [21].

Отже, проведений нами аналіз щодо поняття «кіберзлочинів» та видів кримінальних правопорушень, дозволяють зробити висновок, що поняття «кіберправопорушення» відображає широкий спектр суспільно небезпечних діянь, що здійснюються в кіберпросторі за допомогою комп'ютерних систем та мереж. Сучасне розуміння кіберзлочинності становить не лише традиційні

[20] Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. URL: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf (дата звернення: 18.02.2026).

[21] Dr. Mike McGuire, Samantha Dowling. Cyber crime: A review of the evidence / Summary of key findings and implications. Home Office Research Report 75. October 2013. URL: https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf (дата звернення: 18.02.2026).

правопорушення, адаптовані до цифрового середовища, але й злочинні дії, які стали можливими завдяки новітнім технологіям. Ці правопорушення мають різноманітний характер і об'єкт впливу, охоплюючи від порушень інформаційної безпеки до шахрайств та кібератак. Науковці та правозахисники вживають різні терміни для опису цих правопорушень, зокрема «комп'ютерні правопорушення», «кіберправопорушення» та інші, кожен з яких має свою специфіку та значення залежно від контексту. Відмінності у трактуванні цих понять негативно впливають на законодавчі та практичні аспекти протидії кіберправопорушенням [22].

Окрім того, на підставі проведеного аналізу існуючих підходів щодо дефініції «кіберзлочинів», пропонуємо під кіберзлочинами розуміти суспільно небезпечні діяння, що вчиняються у цифровому середовищі або з використанням інформаційно-комунікаційних мереж, хмарних сервісів чи інших елементів кіберпростору, та спрямованих на порушення конфіденційності, цілісності або доступності інформації, цифрових ресурсів і технологічної інфраструктури, а також на завдання майнової чи немайнової шкоди фізичним і юридичним особам, суспільстві або державі. У сучасних проявах кіберзлочинності характеризується активним використанням автоматизованих атак, штучного інтелекту, технологій соціальної інженерії, криптовалюти, уразливого програмного забезпечення, що зумовлює трансформацію як спосіб вчинення таких кримінальних правопорушень, так і механізмів їх протидії.

3. Імплементація положень Конвенції Ради Європи про кіберзлочинність в Кримінальний кодекс України

Як стверджує В. Г. Кундеус, політика в сфері протидії кіберзлочинності здійснюється різноманітними засобами. Найбільш ефективними у системи її протидії залишаються засоби кримінально-правового впливу. Діяльність з протидії кіберзлочинам засобами кримінально-правового впливу ґрунтується на їх криміналізації. Хоча поняття «кіберзлочинність», «кіберзлочини» використовується як у міжнародному, так і у національному законодавстві, Кримінальний кодекс (далі – КК України) не містить визначення поняття кіберзлочину[23].

Аналіз наукових публікацій щодо імплементації положень міжнародно-правових актів щодо протидії кіберзлочинам вказує на те, що дискусійним питанням залишається визначення переліку міжнародно-правових актів, які регулюють це питання. Так, наприклад, О. М. Жеребець стверджує, що центральне місце на національному рівні в механізмі правового регулювання

[22] Shak R. Concepts and Types of Cyber Offenses in Criminal Law. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 44. P. 325–335. DOI: https://doi.org/10.23939/law2024.44.325 (date of access: 14.02.2026).

[23] Кундеус, В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 44-45.

боротьби з такими злочинами займають норми: Європейської Конвенції про взаємну правову допомогу у кримінальних справах 1959 р. (ратифікована із застереженнями і заявами Законом України від 16.01.98 р. № 4498-ВР), Конвенції Ради Європи про кіберзлочинність від 23 листопаду 2001 р. (ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV), Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 р. (ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV), загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору [24]. Натомість інші вказують, що до цих міжнародних актів відносяться: 1) Конвенція про кіберзлочинність Ради Європи, прийнята 21.11.2001 р. та Додатковий протокол від 28.01.2003 р. (далі – Будапештська конвенція); 2) Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р. (далі – Конвенція ЛАД); 3) Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. (далі – Угода ШОС); 4) Конвенція про кібербезпеку і захист персональних даних Африканського Союзу від 27.06.2014 р. (далі – Конвенція АС) [25]. Також М. І. Саєнко, Є. А. Савела та Ю. Ю. Тополянський вважають, що до таких міжнародно-правових актів відносяться: конвенція «Про кіберзлочинність», ратифікована у 2005 р. державами Ради Європи та іншими державами; Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами, 1995 р.; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 р.; Мінімальний список правопорушень у боротьбі з кіберзлочинністю цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 р. [26]. Окрім того, висловлюється й така думка, що найбільш відомим міжнародним документом у цій сфері є Конвенція Ради Європи про кіберзлочинність (так звана Будапештська конвенція, далі – Конвенція), яка стала базовим орієнтиром для багатьох країн світу, зокрема й України. Подальший розвиток цього документа відображено в Додатковому протоколі до Конвенції 2003 р., спрямованому на криміналізацію діянь расистського та ксенофобського характеру, а також у Другому додатковому протоколі 2022 р., який удосконалив механізми міжнародного співробітництва у сфері електронних доказів. Вагомий внесок у формування європейських стандартів кібербезпеки зробили такі акти Європейського Союзу, як Директива 2013/40/ЄС про атаки на інформаційні системи та Директива (ЄС)

[24] Zherebets O. Implementation of state policy in the field of combating cyber crime: legislative aspect. *INFORMATION AND LAW*. 2021. No. 4(39). P. 129–134. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248834 (date of access: 14.02.2026).

[25] Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. Т. 53, № 5. С. 92–99. DOI: https://doi.org/10.5281/zenodo.2009191 (дата звернення: 14.02.2026).

[26] Saenko M. I., Savela E. A., Topolyansky Y. Y. International experience against cyber crime and cyber crime. *Uzhhorod National University Herald. Series: Law*. 2021. No. 64. P. 386–391. DOI: https://doi.org/10.24144/2307-3322.2021.64.71 (date of access: 14.02.2026).

2022/2555 (NIS2 Directive), що визначають межі захисту критичної інформаційної інфраструктури та взаємодії між державами-членами.

Саме тому можна погодитися із Р. В. Захаревичем, який стверджує, що успішна боротьба з кіберзлочинами вимагає від українського законодавства не тільки оперативного реагування на нові виклики, але й запозичення найкращих практик міжнародного права та досвіду провідних країн у сфері кібербезпеки. Імплементація зарубіжного досвіду дозволяє не лише модернізувати національну правову систему, а й гармонізувати її з міжнародними стандартами, що є необхідною умовою для ефективної співпраці в боротьбі з транскордонною кіберзлочинністю[27].

Так, беззаперечно, що в умовах повномасштабного вторгнення Російської Федерації на територію України, важливе значення має саме захист інформаційної безпеки. У Стратегії кібербезпеки України зазначено, що «Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури» [28]. Окрім того, це пов'язано також з необхідністю гармонізації українського законодавства з міжнародними стандартами, зокрема, й адаптацією до вимог Європейського Союзу та Конвенції про кіберзлочинність.

У першому підрозділі нашого дослідження нами проаналізовано окремі положення Конвенції Ради Європи про кіберзлочинність та визначено перелік діянь, за які за національним законодавством повинна бути передбачена відповідальність. Вважаємо, що такий аналіз щодо імплементації положень Конвенції у Кримінальний кодекс України найкраще відобразити у формі Таблиці 1.

Разом з тим, враховуючи положення Конвенції Ради Європи про кіберзлочинність, В. Г. Хахановський та В. Д. Гавловський, до кіберзлочинів також пропонують відносити: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України); посягання на територіальну цілісність і недоторканність України (ст. 110); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132); незаконне розголошення лікарської таємниці (ст. 145); надання неправдивих відомостей до органу ведення Державного

[27] Zakharevych R. V. Implementation of foreign experience into Ukrainian legislation on combating cybercrime. *Analytical and Comparative Jurisprudence*. 2025. Vol. 2, no. 3. P. 372–376. URL: https://doi.org/10.24144/2788-6018.2025.03.2.60 (date of access: 14.02.2026).

[28] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 18.02.2026).

Таблиця 1

Імплементація положень Конвенції Ради Європи про кіберзлочинність у Кримінальний кодекс України

№ з/п	Конвенція Ради Європи про кіберзлочинність	Кримінальний кодекс України
1.	*Стаття 2 – Незаконний доступ* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер*
2.	*Стаття 3 – Нелегальне перехоплення* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації*

3.	*Стаття 4 – Втручання у дані* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це. 2. Сторона може залишити за собою право вимагати, щоб поведінка, описана у пункті 1, завдавала серйозну шкоду.	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації* *Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*
4.	*Стаття 5 – Втручання у систему* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*

Продовження таблиці 1

5.	*Стаття 6 – Зловживання пристроями* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це: a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 вище; ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5; та b. володіння предметом, перерахованим у підпунктах a. і або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів	*Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут*
6.	*Стаття 7 – Підробка, пов'язана з комп'ютерами* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних,	*Стаття 190. Шахрайство* 4. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки

	яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності	
7.	*Стаття 8 – Шахрайство, пов'язане з комп'ютерами* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи	*Стаття 190. Шахрайство* 4. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки
8.	*Стаття 9 – Правопорушення, пов'язані з дитячою порнографією* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій: a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; b. пропонування або надання доступу до дитячої порнографії за допомогою	*Стаття 301. Ввезення, виготовлення, збут і розповсюдження порнографічних предметів* 2. Ті самі дії, вчинені щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру

	комп'ютерних систем; c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації	*Стаття 301-2. Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи* 1. Проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому задіяно неповнолітню особу
9.	*Стаття 10 – Правопорушення, пов'язані з порушенням авторських та суміжних прав* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем. 2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників	*Стаття 176. Порушення авторського права і суміжних прав*

	фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.	

реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (ч. 1 ст. 158); порушення таємниці голосування (ст. 159); порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через Інтернет) (ст. 161); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); розголошення таємниці усиновлення (удочеріння) (ст. 168); порушення недоторканності приватного життя (ст. 182); розголошення комерційної або банківської таємниці (ст. 232); завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259); незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (в частині збуту через Інтернет) (ст. 263); заклики до вчинення дій, що загрожують громадському порядку (ст. 295); ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300); сутенерство або втягнення особи в заняття проституцією (ст. 303); незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307); викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через Інтернет) (ст. 312); викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (в частині збуту через Інтернет) (ст. 313); розголошення державної таємниці (ст. 328); передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330); погроза або насильство щодо працівника правоохоронного органу (ст. 345); погроза або насильство щодо журналіста (ст. 345-1); погроза або насильство щодо державного чи громадського діяча (ч. 1 ст. 346); погроза

або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (ч. 1 ст. 350); незаконне втручання в роботу автоматизованої системи документообігу суду (ч. 1 ст. 376); розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381); розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387); погроза або насильство щодо захисника чи представника особи (ч. 1 ст. 398); розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422); пропаганда війни (ст. 436); виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436-1)[29].

Вважаємо, що деякі з таких кримінально протиправних діянь вчиняються з використанням комп'ютерів або комп'ютерних систем, програмного забезпечення тощо, проте серед цього переліку є також кримінальні правопорушення, в які протягом останніх років було внесено зміни та доповнення або викладено в новій редакції. Окрім того, відповідно до п. 7 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р, передбачено завершення імплементації в законодавство України положень Конвенції про кіберзлочинність щодо імплементація в законодавство України положення Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних з терміном виконання IV квартал 2025 р.[30]. Це вказує на те, що робота в цьому аспектів продовжується.

ВИСНОВКИ

За результати проведеного дослідження щодо Конвенції Ради Європи про кіберзлочинність як основи кримінально-правової охорони суспільних відносин у кіберпросторі в України, можна зробити такі висновки:

1. Конвенція Ради Європи про кіберзлочинність є фундаментальним міжнародним документом, спрямованих на криміналізацію діянь, пов'язаних з із використанням інформаційно-комунікаційних технологій, а також на забезпечення ефективного міжнародного співробітництва у сфері запобігання та протидії кіберзлочинності.

2. Для України Конвенція Ради Європи про кіберзлочинність має велике значення, оскільки: по-перше, визначає міжнародно-правові зобов'язання держави у сфері криміналізації кіберзлочинів та напрями міжнародного співробітництва; по-друге, є фундаментом для удосконалення Закону України про кримінальну відповідальність та адаптації його до європейських стандартів.

[29] Хахановський В. Г., Гавловський В. Д. Interpretation and classification of criminal offenses as cybercrimes. *INFORMATION AND LAW*. 2020. No. 2(33). P. 99–109. DOI: https://doi.org/10.37750/2616-6798.2020.2(33).208101 (date of access: 18.02.2026).

[30] Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядж. Каб. Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-р#Text (дата звернення: 18.02.2026).

3. Сучасні тенденції розвитку кіберзлочинності, зокрема, активне використання штучного інтелекту, ринку криптовалют, хмарних сервісів, автоматизованих кібератак, атак на критичну інфраструктуру, стають поштовхом для удосконалення нормативно-правових актів з питань протидії кіберзлочинності та розширення напрямів міжнародного співробітництва у протидії злочинності. Разом з тим, ефективність такого механізму залежить від імплементації положень Конвенції Ради Європи про кіберзлочинність у національне законодавство, у тому числі й Кримінальний кодекс України.

АНОТАЦІЯ

Актуальність теми пов'язана з тим, що в сучасних умовах кіберзлочинність набула ознак глобального явища, що посягає не лише на майнові права, конфіденційність та інформаційну безпеку окремих осіб, але й на стабільність функціонування державних інституцій, об'єктів критичної інфраструктури, фінансових систем та механізмів публічного управління. Особливої актуальності ці питання набувають для України в умовах збройної агресії та гібридних загроз, коли кібератаки виступають елементом дестабілізації державного управління, інформаційного впливу та підриву національної безпеки.

Звернута увага на Частину 1. Матеріальне кримінальне право Конвенції Ради Європи про кіберзлочинність, де закріплено перелік діянь, за які повинна наставати кримінальна відповідальність. Визначено особливості кримінальної відповідальності у співучасті за такі діяння, види покарань для фізичних та юридичних осіб за Конвенцією Ради Європи про кіберзлочинність. Проаналізовано існуючі підходи до поняття «кіберзлочини», «кіберзлочинність», «комп'ютерні злочини» та запропоновано авторське визначення поняття «кіберзлочинів». Зауважено, що у сучасних проявах кіберзлочинності характеризується активним використанням автоматизованих атак, штучного інтелекту, технологій соціальної інженерії, криптовалюти, уразливого програмного забезпечення, що зумовлює трансформацію як спосіб вчинення таких кримінальних правопорушень, так і механізмів їх протидії. Відзначено, що п. 7 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р, імплементації в законодавство України положень Конвенції про кіберзлочинність продовжується.

Література

1. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. *Mind.ua*. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu (дата звернення: 14.02.2026).

2. Дикий, А., Савіцький, В., Савчук, С., & Соха, А. (2025). Світові тенденції кіберзлочинності та загрози інформаційній безпеці держав. *Society and Security*, (1(7), 63–74. DOI: https://doi.org/10.26642/sas-2025-1(7)-63-74

3. Крайня В. Світовий рейтинг кіберзлочинності очолила Росія. Україна посіла друге місце. *ms.detector.media*. URL: https://ms.detector.media/

kiberbezpeka/post/34647/2024-04-11-svitovyy-reytyng-kiberzlochynnosti-ocholyla-rosiya-ukraina-posila-druge-mistse/ (дата звернення: 14.02.2026).

4. Нагірний І. П. Еволюція правової протидії злочинам у сфері інформаційних технологій: історичні витоки та сучасні виклики. *Європейський правничий часопис*. 2026. С. 141-147. DOI: https://doi.org/10.36919/3041-1149 (print).11.2025.141-147 (дата звернення: 14.02.2026).

5. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

6. Dulepa V. P. Criminological characteristics of cybercrime. *Juridical scientific and electronic journal*. 2021. No. 11. P. 592–595. DOI: https://doi.org/10.32782/2524-0374/2021-11/147 (date of access: 17.02.2026).

7. Shak R. Concepts and Types of Cyber Offenses in Criminal Law. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 44. P. 325–335. DOI: https://doi.org/10.23939/law2024.44.325 (date of access: 14.02.2026).

8. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посібник. Харків : Право, 2014. 284 с.

9. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2 (10-11). С. 276–28.

10. Корзун С. В. Понятійно-категоріальний апарат державної кримінально-правової політики протидії кіберзлочинам. *Економіка, управління та адміністрування*. 2025. № 1(111). С. 131–145. DOI: https://doi.org/10.26642/ema-2025-1(111)-131-145 (дата звернення: 17.02.2026).

11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.02.2026).

12. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 17.02.2026).

13. Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. Т. 53, № 5. С. 92–99. DOI: https://doi.org/10.5281/zenodo.2009191 (дата звернення: 14.02.2026).

14. Боровик А. В. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посібник. Луцьк : ВолиньПоліграф, 2019. 304 с.

15. Дрижакова Д. Ю., Горішній О. О., Тараненко М. М. Оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні. 2025. DOI: https://doi.org/10.5281/zenodo.15074665 (дата звернення: 14.02.2026).

16. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. URL: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf (дата звернення: 18.02.2026).

17. Dr. Mike McGuire, Samantha Dowling. Cyber crime: A review of the evidence / Summary of key findings and implications. Home Office Research Report 75. October 2013. URL: https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf (дата звернення: 18.02.2026).

18. Кундеус, В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 44-45.

19. Zherebets O. Implementation of state policy in the field of combating cyber crime: legislative aspect. *INFORMATION AND LAW*. 2021. No. 4(39). P. 129–134. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248834 (date of access: 14.02.2026).

20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 18.02.2026).

21. Хахановський В. Г., Гавловський В. Д. Interpretation and classification of criminal offenses as cybercrimes. *INFORMATION AND LAW*. 2020. No. 2(33). P. 99–109. DOI: https://doi.org/10.37750/2616-6798.2020.2(33).208101 (date of access: 18.02.2026).

22. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядж. Каб. Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-р#Text (дата звернення: 18.02.2026).

Information about the author:
Politova Anna Serhiivna,
Candidate of Legal Sciences, Associate Professor,
Associate Professor of Department of Law
Mariupol State University
6, Preobrazhenska, Kyiv, Ukraine, 3037, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-14

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В ПРОЦЕСІ РОЗСЛІДУВАННЯ

Ряшко О. В.

ВСТУП

Ми живемо у світі, у якому специфіка сучасної злочинної діяльності призводить до необхідності знаходження особливого підходу щодо об'єкта криміналістичного пізнання. Наразі світова спільнота максимально залучена до інформаційного простору та перетворилася в окрему групу – інформаційне суспільство. Позитивні аспекти цього явища усім прекрасно відомі, але небезпечні його тенденції часом складно спрогнозувати. Серед цих тенденцій виділяються наступні: вплив на людську психіку та масштаб маніпуляцій, який постійно прогресує, використання сучасних інформаційних технологій для можливості проникнення я у приватне життя та в діяльність організацій, використання сучасних технологій для тотального контролю над життям людей, як в окремій державі, так і світової спільноти, поглиблення інформаційної війни між державами, що ворогують і як наслідок, неухильне зростання кіберзлочинів.

Якщо брати до уваги значення, то кіберзлочином виявляється будь-яке протиправне діяння, що здійснюється за допомогою електронних операцій, відповідно метою якого є подолання захисту комп'ютерних систем та даних, які ними обробляються. У ширшому сенсі це явище розглядається як будь-яке протиправне діяння, що вчинене за допомогою або з використанням комп'ютерної системи чи мережі, включаючи й такі злочини, як незаконне зберігання, пропозиція або поширення інформації за допомогою комп'ютерної системи чи мережі.

Важливим є факт, що предметами посягання у кіберпросторі першочергово виступають інформаційні продукти та ресурси. Майно, комп'ютери, комп'ютерні мережі, мережі електрозв'язку, документи виявляються другорядними (вторинними) об'єктами злочину.

Саме інформація, зафіксована в електронній формі, яка здатна задовільнити потреби чи інтереси користувачів кіберпростору і є інформаційним продуктом. Як будь яка інша інформація вона може бути вагомою, враховуючи залучення багатьох осіб для роботи над нею або бути необхідною умовою для виконання конкретного завдання. Цей інформаційний продукт повинен мати законного користувача, що абсолютно логічно пов'язане з певними відомостями щодо персональних даних чи авторського права чи банківської таємниці. Саме характер відомостей, зафіксованих у інформаційному продукті зумовлює його важливість, інтерес та цінність, а також сприяє обранню особою певної лінії злочинної поведінки.

За сучасного розвитку науки і техніки та швидкоплинних можливостей технологій, використання електронних доказів набуває важливого значення щодо доказуванні винуватості чи невинуватості підозрюваного (обви-

нуваченого) – яка становить головну дилему усього кримінального процесу. Зрозуміло, що роль цифрових доказів стрімко зростає і сьогодні переписки, записи з камер відеоспостереження та дані з мобільних пристроїв можуть бути використані для підтвердження або спростування версії сторони обвинувачення.

На відміну від скажімо стало традиційних доказів, електронні мають певні особливості. Сфера їх існування – цифрова, саме тому їх збирання, зчитування, аналіз та оцінка потребують відповідних знань та обладнання. Такі докази є дещо «крихкими», оскільки їх легше підробити, змінити, знищити, фальсифікувати. Саме тому їх використання у кримінальному провадженні стають додатковим тягарем для сторони обвинувачення, коли мова йде про їх відповідність умовам достовірності та допустимості.

1. Роль та місце електронних доказів у розслідуванні кіберзлочинів

Щодо правової природи електронних доказів – не дивлячись на недостатню врегульованість законодавством, це самостійний вид доказів. Коли мова заходить про основні проблеми та питання, що виникають у зв'язку з використанням електронних доказів, першочерговим завданням в ході судового розслідування виявляється необхідність доведення автентичності електронного доказу. Відповідно з цього правила витікає наступне та найголовніше – підтвердження допустимості його отримання та законного залучення до сфери кримінального судочинства. Не менш важливим є забезпечення незмінності та достовірності даних в ході їх збирання, зберігання та використання в кримінальному провадженні. Якщо звернути увагу на способи та механізми перевірки достовірності та належності таких доказів, то найпоширенішими виступають метадані – структурована інформація, яка дозволяє відстежити будь-які його зміни.

Особливе місце відводиться криптографічним методам – застосуванню цифрових підписів, хеш-функцій, електронних сертифікатів для забезпечення автентичності даних. На допомогу органам досудового розслідування приходить й цифрова експертиза – яка дозволяє за допомогою комплексу технічних заходів провести аналіз електронних доказів, включаючи відновлення видалених файлів, аналіз мережевого трафіку та ідентифікацію авторства[1]

Необхідно памятати, що залежно від обставин пристрої можуть бути зібрані як в увімкненому, так і у вимкненому стані. Надзвичайно важливо прийняти міри для запобігання знищення, псування або зміни оригінальних даних. Зрозуміло, що в ході транспортування можуть виникати ситуації, що сприятимуть пошкодженню або спотворенню даних, тому з метою недопущення необхідно використовувати захищене пакування.

Окрім цього, слід максимально забезпечити належні умови для зберігання цифрових носіїв (це і контроль вологості, і захист від магнітних полів) та документувати усі дії, пов'язані з обробленням доказів. З моменту збирання та фіксації доказів до їх представлення в суді, необхідно дотримуватися

[1] Аніщенко О. (2021). Збір і перевірка електронних доказів: проблеми та рішення. *Юридична практика*, 45(2). С. 14.

чіткості та послідовності щодо її документування. Документація повинна містити унікальний ідентифікатор доказу, дату та відомості про осіб, які мали до неї доступ. В першу чергу увага звертається на фіксацію даних, які можуть бути втрачені або є найменливішими за своєю природою, як вміст оперативної пам'яті до прикладу[2].

Основними умовами якісного збирання та аналізу цифрових доказів є ретельність процесу, перевірка та контроль доступу, чіткість процедури та правильність виконання кожного етапу з метою забезпечення подальшого успішного розслідування.

Саме дотримання принципів цілісності, автентичності та відтворюваності є основою застосування цифрової криміналістики, що надає можливості створення умов для максимально об'єктивного та неупередженого аналізу та мінімізує ризики спотворення чи втрати інформації. На жаль, кіберзлочинність, як феномен, постійно прогресує, набуває дедалі складніших форм, тому покращення ефективності методології збирання цифрових доказів є важливим кроком до зміцнення та збереження інформаційної безпеки з метою справедливого судового провадження.

На сьогоднішній день, дедалі в ході розслідування кіберзлочинів при проведенні слідчих (розшукових) дій перед слідчим постає питання щодо збирання, фіксації та використання електронної інформації, як джерела доказів у кримінальному провадженні. В своїй статті І. Г. Каланча зауважує, що під час слідчих (розшукових) дій фіксація доказів з електронних носіїв збирання інформації, що міститься на них, може здійснюватися двома способами: або вилученням носія або інформаційної системи, до якого він входить, або копіюванням інформації, що зберігається на відповідному електронному носії. Щодо вилучення, зрозуміло, що це класичний спосіб збирання доказів у формі матеріальних об'єктів, до яких належать електронні носії та інформаційні системи. Не дивлячись на певні плюси та переваги, неможливо оминути і деякі проблеми, на кшталт неефективності дослідження електронних носіїв після вилучення в разі загрози зупинення критично важливих функцій бізнес-процесів або наявності шифрування тощо. Погоджуємося, що в таких випадках альтернативою виступає збирання інформації, яка міститься в електронному носії шляхом виготовлення копії такої інформації[3].

Зараз ми живемо у світі, де практично щодня відбуваються терористичні акти, війни, що не вчухають, а відповідно зростає кількість кіберзлочинів та інших правопорушень, пов'язаних із військовою агресією. Тому саме цифрові (електронні) докази відіграють ключову роль у їх фіксації. Специфічні риси, якими вони володіють, наділяють їх як плюсами, так і мінусами. Навіть в ході безперервних бойових дій такі докази збираються за допомогою квадрокоптерів, які дозволяють побачити не тільки приміром масштаби руйнувань, але й зафіксувати деталі, не помітні з землі, фіксацією на смартфон за допомогою

[2] Івасишин, Т., Пірог, О. (2025). Порядок збирання цифрових доказів. *Криміналістика і судова експертиза.* Вип. 70. С. 376. DOI: 10.33994/ kndise.2025.70.28.

[3] Каланча І. Г. Копія електронної інформації як доказ у кримінальному про вадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 337.

спеціального додатку, фото- і відеоматеріалами з місць обстрілів або перехопленими електронними комунікаціями окупантів, що є доказами вчинення злочинів проти цивільного населення.

Нематеріальна сутність цифрових даних робить їх надзвичайно крихкими саме в юридичному сенсі. На відміну від фізично існуючих речових доказів, електронна інформація дуже легко піддається різного роду трансформаціям: зміні, знищенню, виправленням, копіюванню, до того ж вкрай складно довести, що ці зміни відбулися внаслідок стороннього втручання[4]

Матеріали, незалежно від того, чи зібрані вони у момент вчинення злочину чи лише зафіксували його наслідки, стають доказами у судовому провадженні при умові підтвердження їх достовірності та допустимості. Коли мова заходить про оцінку таких даних в суді, то будь-які сумніви щодо цілісності, фіксації та зберігання будуть трактуватися на користь обвинуваченого (підсудного). Якщо сторона захисту переконає суд у неналежному зберіганні електронного доказу стороною обвинувачення або наведе доводи щодо сумнівності його автентичності, скоріш за все суд виключить його з процесу доказування, як такий, що не відповідає ознакам допустимості.

Погоджуємося з думкою Ханіна С., що сучасне кримінальне процесуальне законодавство, внаслідок своєї недосконалості фігурально висловлюючись, віддає м'яч на половину поля потенційного маніпулятора, аніж надає ефективні правові інструменти органам досудового розслідування, прокуратури та суду. Автором також дуже вдало підмічено, що цифрові докази, модифіковані через дії контрфорензіки, ускладнюють і сам об'єкт експертизи, оскільки експерт змушений не тільки аналізувати зміст даних, а ще й додатково брати на себе місію дослідника, спочатку відновлюючи та перевіряючи сам доказ, а вже потім роблячи висновки щодо його значення для кримінального провадження. Це досить виснажливо та вимагає від експерта не просто високої кваліфікації, доступу до сучасних інструментів, додаткового часу, але й нерідко і творчого підходу[5].

Кіберзлочинність постійно модернізується, практично щодня кіберзлочинці винаходять нові шахрайські схеми та вдосконалюють свої методи заради власного збагачення за рахунок інших громадян та підприємств по всьому світу з використанням мережі Інтернет. На сьогоднішній день ми не знайдемо конкретного переліку кіберзлочинів, окрім цього правове поле не послуговується і специфічними термінами, на кшталт смішингу, доксингу, фішингу, вішингу. Таке використання могло би допомогти в аналізі та синтезі інформації щодо відповідних тенденцій у кіберпросторі. Загрозливою виглядає тенденція до стрімкого поширення зараження комп'ютерів як окремих користувачів, так і підприємств, установ, організацій за допомогою розсилки електронних листів начебто від імені адміністраторів поштових сервісів, суду, банківських установ чи урядових інституцій.

---

[4] Метелев О.П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* № 1-2. 2023. С. 42 URL: https://vkslaw.com.ua/index.php/journal/ article/view/34.

[5] Ханін С. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. *Юридична газета.* 26 червня 2024. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi dokazi-pid-chas-vikonannya-vimog-st-290-kpk-ukrayini.html.

Складність розслідування полягає ще й в тому, що кіберзлочини дуже часто є міжнародними, а тому не підпадають під єдину національну юрисдикцію, окрім цього непоодинокими є випадки, коли наприклад комп'ютери злочинця та його жертви знаходяться на територіях різних держав[6].

Якщо первинна інформація сприймається будь-якою людиною та є доступною для її розуміння, то для повної картини злочину та обставин його вчинення необхідно залучення експертом спеціальних засобів, спеціалізованих програм, які можуть допомогти розкодувати інформацію, яку намагалися приховати та відтворити її у тих версіях, які висунув слідчий в процесі розслідування.

Саме фахівець може відновити резервні копії системи, логфайли, дампи оперативної пам'яті, дампи мережевих трафіків, інші файли або їх частини (у разі пошкодження), як наявні, так і видалені, а також службову інформацію про ці файли. Після чого саме фахівець здатний проаналізувати сукупність знайдених цифрових слідів і вибудовати таймлайн шляхом структуризації інформації відносно діяльності користувача ЕОМ щодо операцій, які здійснювалися з певними файлами і програмами (встановлення, видалення, зміна), про роботу в локальній мережі або мережі Інтернет[7]

За загальноприйнятим правилом, збирання та використання доказів з відкритих джерел має здійснюватися за протоколом Берклі, яким рекомендовано мінімізувати дані щодо збирання лише необхідно пропорційної інформації, фіксувати щонайменше такі дані, як цільова вебадреса; вихідний код; захоплення всієї вебсторінки або зображення повідомлення крауд-месенджера взастосунку; вбудовані мультимедійні файли; вбудовані метадані; контекстуальні дані; хеш значення; дані про процес збирання інформації. Наприклад, у практиці правоохоронних органів Німеччини, Великобританії та США OSINT-фрагменти можуть входити до складу доказової бази за умови дотримання стандартів chain of custody (ланцюга збереження доказів) та цифрової фіксації із обов'язковим зазначенням джерела, дати та умов отримання[8]

У Сполучених Штатах Америки також використання у кримінальному провадженні цифрових доказів врегульовані правилами федерального доказового права, зокрема це положення про автентифікацію. Американський законодавець використовує напрочуд зрозумілий підхід про необхідність переконати суд у тому, що цифровий об'єкт є саме тим, за що він подається, а не зміненим чи підробленим артефактом. Таке переконання досягається через спеціалізовані експертизи, застосування криптографічних механізмів фіксації, надійних протоколів зберігання об'єкта та суворий контроль доступу до нього[9].

---

[6] Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investigaю*. 2022. Vol. 11, issue 53. P. 268. URL: https://doi.org/10.34069/AI/2022.53.05 (дата звернення: 09.10.2023).

[7] Колеснікова І.А. Цифрові сліди; поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. № 10. 2023. С. 473.

[8] Ліхтанська А. П., Михайлов В. О. (2024) Використання osint в кримінальному праві україни.» *DICTUM FACTUM* 1 (15). С. 110.

[9] Кутепов І.О. Роль цифрових доказів під час розслідування економічних злочинів. *Юридичний науковий електронний журнал.* № 2/2025. С. 629.

Якщо спробувати узагальнити характерні особливості кіберзлочинів, то виявиться, що для переважної більшості осіб, які їх вчиняють притаманна технократична раціональність мислення, яка базується на вмінні виявлення та використання в своїх цілях недостатню обізнаність та прогалини щодо цифрових систем, здібності оминати механізми контролю та створювати певні алгоритми з метою приховування каналів обігу ресурсів. Як влучно зазначає Кутепов І.О. в своїй статті, саме згадана форма раціональності дозволяє таким правопорушникам діяти в межах ретельно сконструйованого кримінального дизайну[10].

Щодо слідчої практики, то найбільш типовими діями є виявлення та збереження цифрових слідів у вигляді комп'ютерних даних. Вимоги ті самі що й відносно інших цифрових доказів. Але й водночас є певна специфіка, обумовлена бінарною природою (послідовність нулів та одиниць), що робить внесені зміни практично непомітними для людського ока. Саме тому, усі процедури щодо ідентифікації комп'ютерних даних у кримінальному провадженні повинні забезпечувати підтвердження їх цілісності та незмінності з істотно вищим рівнем достовірності, ніж це можливо при використанні традиційних методів виявлення цифрових слідів[11]

Якщо брати до уваги класифікацію кіберзлочинів, то за основними критеріями можемо розподілити їх за наступними групами: 1) крадіжка даних (незаконне отримання особистої, фінансової або іншої конфіденційної інформації); 2) фінансові махінації); 3) хакерські атаки; 4) поширення шкідливого програмного забезпечення; 5) кібертероризм[12].

Розслідування кіберзлочинів вимагає чітке розуміння методології та особливостей процесу збирання та аналізу доказової бази. В першу чергу, мова йде про залучення до досудового розслідування фахівців з кібербезпеки та забезпечення їх технічним обладненням. Цифрові докази визначаються як інформація, що є важливою для встановлення обставин кримінального правопорушення, яка зберігається, отримується або передається електронним пристроєм. Цифрові докази можуть існувати в латентному вигляді, на кшталт відбитків пальців, з легкістю перетинати юрисдикційні кордони, чутливість дозволяє змінювати, пошкоджувати або знищувати їх, не докладаючи зайвих зусиль[13].

Електронні сліди також утворюються внаслідок зовнішнього доступу до комп'ютерних систем з метою знищення або копіювання інформації, модифікації баз даних, блокування роботи системи. Такими слідами є видалення з каталогів

---

[10] Кутепов І.О. Кіберзлочинність у фінансовій сфері: предикатна роль, інструменти легалізації та проблематика доказування. *Юридичний науковий електронний журнал*. № 1/2025. С. 775

[11] Караман К.В. Виявлення цифрових слідів: особливості й алгоритм. *Вісник ХНУВС – Bulletin of KhNUIA.* 2025. № 3 (110). С. 145. DOI: https://doi.org/10.32631/v.2025.3.12

[12] Ларченко М.О. Деякі особливості розслідування кіберзлочинів. *Науковий вісник 3/2024 Львівського державного університету внутрішніх справ.* С. 72.

[13] Дунаєва Т.Є. Цифрові дані як доказ скоєння кіберзлочину в розслідуванні кримінальних правопорушень. *Використання цифрової інформації в розслідуванні кримінальних правопорушень: матеріали міжнар. наук.-практ. круглого столу,* м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. С. 104 DOI: https://doi.org/10.31359/978-966-998-460-9.

імен файлів, видалення або додавання окремих записів, фізичне руйнування або розмагнічування носіїв, перейменування каталогів і файлів, зміна розмірів вмісту файлів, зміна атрибутів файлів, поява нових каталогів і файлів, зміна інформації про час останнього доступу до інформації, результати роботи антивірусних і тестових програм тощо. Вони можуть бути виявлені під час експертного дослідження комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду[14].

Нерідко на практиці виникають проблеми саме через нерозуміння між електронним документом та електронним доказом, хоча ці поняття тісно пов'язані, але не є аналогічними. Внаслідок такої неузгодженості на стадії судового провадження трапляються випадки відмови суду приймати до розгляду та дослідження скажімо то саме електронне листування, оскільки, приміром, йому не вистачає обов'язкових реквізитів. Не покращує ситуацію і відсутність чіткої регламентації відповідної процедури перевірки електронного документу перед поданням до суду. Чи то призначення відповідної судової експертизи чи то роздруківка інформації з бази даних? На наш погляд, ефективніше подавати електронні докази в електронній та паперових копіях, тому що такий підхід, однозначно, спрощує процедуру огляду електронних доказів судом.

Погоджуємося з думкою щодо необхідності чіткого визначення електронного доказу в КПК України та, додатково, в підзаконних нормативних актах узгодити порядок роботи з електронними доказами, зокрема окреслити необхідні носії інформації, доказову базу з яких суддя може аналізувати, програмне забезпечення для такого аналізу та обумовлення потреб, за яких виникає така необхідність, інші технічні та технологічні аспекти[15].

Цифрові сліди виникають внаслідок використання цифрових засобів та технологій. Важливим аспектом є те, що використання таких засобів і технологій може бути як безпосереднє, при фізичному, особистому застосуванні (пошук в мережі інтернет певної інформації або завантаження відео- файли в соціальну мережу), так і опосередкованим, коли дані утворюються без фактичного втручання особи (утворення метаданих при здійсненні фотографування певного об'єкту, фіксація камерами відеоспостереження пересування транспортного засобу тощо)[16].

2. Типові слідчі ситуації та характеристика особи кіберзлочинця

Типовими слідчими ситуаціями є ситуації, коли приміром відомості в ЄРДР вносяться в результаті отримання повідомлення особи про кримінальне правопорушення, яке містить інформацію щодо особи можливого злочинця та

[14] Лазебний А. М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10) С. 230. DOI 10.33244/2617-4154.1(10).

[15] В.Г. Хахановський. М.В. Гуцалюк. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* № 1 (31), 2019. С. 16-17. С. 16-17 doi: 10.37025/1992-4437/2019-31-1-13

[16] Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету,* 2024. С. 73. DOI https://doi.org/10.24144/2307-3322.2024.85.4.10

персоналізацію його даних. Таку особу можливо виявити за результатами внутрішньої перевірки під час моніторингу кіберпростору або в ході проведення аудиту.

Процес досудового розслідування буде ефективним у випадку максимального збереження документів, в яких зафіксована робота комп'ютерної мережі, встановлення усіх співучасників злочину та визначення ролі кожного з метою подальшої можливості забезпечення відшкодування цивільного позову. Перед слідчим постають такі типові тактичні завдання, як персоналізація особи злочинця, встановлення його місцеперебування та затримання, встановлення потерпілих осіб, забезпечення збереження віддалених електронних носіїв інформації, у яких зафіксовано роботу злочинця в мережі, накладення арешту на майно з метою відшкодування матеріальних збитків та можливої його конфіскації.

Інша слідча ситуація виникає, коли кримінальне провадження розпочинається на підставі отримання оперативної інформації та місить відомості, що персоналізують особу злочинця (злочинців). Як правило, таке розслідування стосується вчинення тяжких міжнародних кіберзлочинів, що включають розповсюдження дитячої порнографії або насильство, експлуатація та торгівля людьми.

В ході такого розслідування необхідно провести комплекс слідчих (розшукових) дій та негласних слідчих (розшукових) дій, надання доручення оперативному підрозділу на проведення оперативних заходів, спрямованих зокрема для зняття інформації з електронних комунікаційних мереж, з електронних інформаційних систем; особистий огляд затриманих; слідчий огляд вилученого майна; проведення обшуків за місцем проживання, перебування або роботи затриманих осіб.

Кримінальне провадження може бути розпочато в результаті перевірки оперативної інформації, але, на відміну від попередньої сприятливої слідчої ситуації, без жодних відомостей про особу злочинця. Така ситуація є характерною, коли мова йде про незаконну діяльність організованої злочинної групи, що пов'язана із заволодінням майном шляхом незаконних операцій з використанням електронно-обчислювальної техніки. В такому випадку на початок досудового розслідування слідчий володіє інформацією про потерпілих, йому відомий спосіб та механізм вчинення злочину, але практично нічого не відомо про безпосередніх замовників, виконавців чи спонсорів злочинних діянь.

Як правило, це багатоепізодні кримінальні провадження, нерідко виникають підстави для їх об'єднання в одне, тому основним завданням виступає скрупульозне документування усіх епізодів, встановлення суб'єктного складу щодо кожного з епізодів злочинної діяльності, визначення ролі кожного з учасників та встановлення механізмів легалізації незаконно отриманих доходів. З усіх слідчих ситуацій ця виглядає найскладнішою, оскільки, саме при її відпрацюванні слідчий змушений максимально реалізовувати весь арсенал тактичних операцій, в першу чергу спрямованих на подолання засобів конспірації, які використовують учасники мережевої злочинної групи.

Звернемо свою увагу на встановлення мотивів вчинення кіберзлочинів. Перше місце належить мотивації корисливій, оскільки дійсно чорний ринок даних, які викрадаються та простота їх монетизації сприяють постійній активізації цього мотиву, який надає можливість для швидкого фінансового збагачення. Політичні та інші ідеологічні мотиви народили так званий хактивізм – використання комп'ютерів, комп'ютерних мереж для просування політичних ідей, в тому числі й втручання у виборчі процеси країн через використання технологій фреймингу, сугестії, чорного піару. Метою хактивістів є приміром зрив діяльності організації, з якими вони перебувають в опозиції або навпаки, просування своїх власних політичних ідей шляхом злому.

Мотиві ігрові, які притаманні особам, що розглядають злом як виклик особистий, чи інтелектуальний, чи технічний. Такі особи намагаються доводити свою значимість, підвищувати авторитет у своєму колі спілкування або ж роблять це заради розваги, оскільки знаходяться в пошуку задоволення гострих відчуттів. Злочинець, що вчиняє кіберзлочин, фактично завжди прирівнюється до активного користувача комп'ютера. Фаховий рівень варіюється від користувача, упевненого користувача, досвідченого користувача до профі. Критеріями такої диференціації, в першу чергу, слугують кількість програм, які опанував користувач; ступінь опанування ним кожної з програм; рівень професійної самооцінки та бажання постійного самовдосконалення.

Абсолютно згідні з думкою, що така диференціація цілком підходить теорії, але є дещо формальною на практиці саме з позицій формулювання типових версій про особу злочинця. Наприклад, той самий професійний рівень не в змозі у повній мірі відобразити весь комплекс ознак злочинця, які він задіяє у процесі детермінації механізму злочину. Тут і психологічні особливості, і конкретна роль, якщо мова йде про злочинне угрупування, і його місце-знаходження в сенсі географічному, і соціальна мобільність[17].

Кіберзлочинці поділяються на так званих «одиночок», які працюють самостійно та переслідують матеріальну вигоду чи виявляють особисту зацікавленість до злому технологій; кіберзлочинні угруповання – це організовані групи, які об'єднують свої знання та ресурси для досягнення конкретних злочинних цілей; хакери, діяльність яких спонсоруються державою і які діють за підтримки або з дозволу держави, з метою шпигунства або завдання шкоди іншим країнам; і насамкінець, інсайдери – це працівники компаній або організацій, які можуть зловживати своїм доступом до конфіденційних даних[18].

Саме тому, банківські установи, ІТ-компанії, фірми охорони й технічного обслуговування, добираючи персонал, проводять тестування з метою визначення рівня професіональності, а також психотипу майбутнього

[17] [Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. С. 100. (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM).

[18] Найченко А.М. Кіберзлочинність та оцінка судом електронних (цифрових) доказів в кримінальному провадженні. *Журнал «Наукові інновації та передові технології.* № 12 (40). 2024. С. 538

працівника. Результати такого роду тестувань можуть бути досить цінними для працівників кіберполіції під час первинної перевірки інформації та слідчого з позицій визначення кола підозрюваних в установі-жертві[19].

ВИСНОВКИ

На сьогоднішній день саме Інтернет відкриває надзвичайно великі можливості для спілкування, обміну інформацією будь-якого характеру та потенційною самореалізацією у багатьох сферах. Відповідно до цих можливостей, ми стали свідками та учасниками виникнення та функціонування абсолютно нового типу суспільних відносин – відносин у кіберпросторі, які вивели світову спільноту на зовсім інший рівень царину державного управління, наукові дослідження, мистецькі здобутки та економічні досягнення. Кожна монета має дві сторони, інша сторона інтернет-середовища лякає та жахає масштабами криміногенного характеру, від порушення авторських прав до розповсюдження та збуту творів, що пропагують культ насильства та жорстокості, порнографічних предметів, наркотичних засобів, вчинення вимагань та шахрайств.

Проблемним моментом в ході розслідування кіберзлочинів можна назвати відсутність можливості дослідження електронних доказів, які зберігаються на віддалених серверах. Звичайно є можливість дослідження їх паперових аналогів. Маємо надію, що можливість дослідження таких доказів виведе досудове розслідування кіберзлочинів на абсолютно інший, якісно новий рівень.

Іншою проблемою, на наш погляд, виступає відсутність єдиної методики трактування одних і тих самих фактів сторонами кримінального провадження. Ми пов'язуємо це з використанням різних методів і процедур розслідування кіберзлочинів різними спеціалістами та експертними установами. Доцільно би було запровадити єдиний стандарт щодо методики, аналізу та синтезу інформації, принципів безпосереднього дослідження та оцінки в ході розслідування кіберзлочинів з метою недопущення помилкових висновків та неефективного використання ресурсів. Саме оцінка доказової інформації виявляє усі недоліки, які мають місце як в процесі збирання, так і в недостатньо якісному аналізу цифрових доказів на стадії досудового розслідування.

Константуємо факт, що при характеристиці особи комп'ютерного злочинця, необхідно враховувати, що в електронну злочинність втягнуто надзвичайно широке коло осіб, яке варіюється від висококваліфікованих спеціалістів до дилетантів. До того ж правопорушники мають різний соціальний статус та різний рівень освіти. Зловмисники постійно вдосконалюють свої методи в обхід заходів безпеки, що надзвичайно ускладнює роботу органів досудового розслідування. Як правило, особам, що вчиняють кіберзлочини притаманний високий рівень інтелекту, професіоналізм, постійне залучення до новинок у сфері комп'ютерних технологій.

[19] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст] : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса :ТЕС, 2020. С. 118

Цілком логічно, що більшість таких осіб знають декілька мов програмування, мають значний досвід роботи на комп'ютері, як правило раніше до кримінальної відповідальності не притягувалися, наділені розвиненим формально-логічним мисленням, використовують специфічну лексику, так званий компютерний сленг. Нерідко суб'єктом злочину є «білокомірцеві злочинці», які вчиняють злочини, пов'язані безпосередньо з їх службовою діяльністю, шляхом використання доступу до певних комп'ютерних інформаційних систем та електронних баз даних[20].

АНОТАЦІЯ

У статті досліджуються особливості збирання, перевірки та оцінки електронних доказів до розслідування кіберзлочинів. Наголошується на загрозі злочинності у кіберпросторі як основному чиннику негативного впливу, пов'язаними з багатьма сферами життя. Виокремлено й проаналізовано чинники, які ускладнюють процес досудового розслідування, зокрема обмежені можливості фіксації обстановки вчинення кіберзлочину та слідової картини. Визначено необхідність в подальшому розвитку забезпечення ефективності сфери кібербезпеки із врахуванням практики європейських партнерів, зокрема адаптації національного законодавства до міжнародних стандартів.

Література

1. Аніщенко О. (2021). Збір і перевірка електронних доказів: проблеми та рішення. *Юридична практика*, 45(2), 12–19.

2. Івасишин, Т., Пірог, О. (2025). Порядок збирання цифрових доказів. *Кримінал істика і судова експертиза.* Вип. 70. С. 371–381. DOI: 10.33994/ kndise. 2025.70.28.

3. Каланча І. Г. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 336-339. DOI https://doi.org/10.32782/2524-0374/2021-8/77

4. Метелев О.П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* № 1-2. 2023. С. 42-53 URL: https://vkslaw.com.ua/index.php/journal/ article/view/34.

5. Ханін С. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. *Юридична газета.* 26 червня 2024. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi dokazi-pid-chas-vikonannya-vimog-st-290-kpk-ukrayini.html.

6. Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investigaю*. 2022. Vol. 11, issue 53. P. 259–269. URL: https://doi.org/10.34069/AI/2022.53.05 (дата звернення: 09.10.2023).

[20] Максимчук Ю. В. Особливості розслідування кіберзлочинів та протидії їх вчинення / Ю. В. Максимчук / Грані права: XXI століття : матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 19 травня 2018 р.) У 2-х т. Т. 2 / за ред. Г. О. Ульянової ; уклад.: Ю. Д. Батан, М. В. Сиротко [та ін.] – Одеса : Видавничий дім «Гельветика», 2018. – С. 379-381.

7. Колеснікова І.А. Цифрові сліди; поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. №10. 2023. С. 472-474 DOI https://doi.org/10.32782/2524-0374/2023-10/114

8. Ліхтанська А. П., Михайлов В. О. (2024) Використання osint в кримінальному праві україни.» *DICTUM FACTUM* 1 (15). С. 105-111. DOI.ORG/10.32703/2663-6352-2024-1-15-105-111

9. Кутепов І.О. Роль цифрових доказів під час розслідування економічних злочинів. *Юридичний науковий електронний журнал.* № 2/2025. С. 626-630. DOI https://doi.org/10.32782/2524-0374/2025-2/151

10. Кутепов І.О. Кіберзлочинність у фінансовій сфері: предикатна роль, інструменти легалізації та проблематика доказування. *Юридичний науковий електронний журнал*. № 1/2025. С. 774-778. DOI https://doi.org/10.32782/2524-0374/2025-1/184

11. Караман К.В. Виявлення цифрових слідів: особливості й алгоритм. *Вісник ХНУВС – Bulletin of KhNUIA.* 2025. № 3 (110). С. 141-150. С. 145 DOI: https://doi.org/10.32631/v.2025.3.12

12. Ларченко М.О. Деякі особливості розслідування кіберзлочинів. *Науковий вісник 3/2024 Львівського державного університету внутрішніх справ.* С.70-77. DOI: https://doi.org/10.32782/2311-8040/2024-3-9

13. Дунаєва Т.Є. Цифрові дані як доказ скоєння кіберзлочину в розслідуванні кримінальних правопорушень. Використання цифрової інформації в розслідуванні кримінальних правопорушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. 104 с. DOI: https://doi.org/10.31359/978-966-998-460-9.

14. Лазебний А. М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10) С. 226-233. DOI 10.33244/2617-4154.1(10).

15. В.Г. Хахановський. М.В. Гуцалюк. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* № 1 (31), 2019. С. 13-19. С. 16-17 DOI: 10.37025/1992-4437/2019-31-1-13

16. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету*, 2024. С. 71-75. DOI https://doi.org/10.24144/2307-3322.2024.85.4.10

17. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. 298 с. (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM).

18. Найченко А.М. Кіберзлочинність та оцінка судом електронних (цифрових) доказів в кримінальному провадженні. *Журнал «Наукові інновації та передові технології.* № 12 (40). 2024.535544. DOI https://doi.org/10.52058/2786-5274-2024-12(40)-535-544

19. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст] : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с. Режим доступу: https://doi.org/10.32837/11300.13264

20. Максимчук Ю. В. Особливості розслідування кіберзлочинів та протидії їх вчинення / Ю. В. Максимчук / Грані права: XXI століття : матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 19 травня 2018 р.) У 2-х т. Т. 2 / за ред. Г. О. Ульянової ; уклад.: Ю. Д. Батан, М. В. Сиротко [та ін.] – Одеса : Видавничий дім «Гельветика», 2018. С. 379-381. http://hdl.handle.net/11300/10643

Information about the author:
Ryashko Olena Vasylivna,
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminal Procedure and Criminology,
Lviv State University of Internal Affairs,
Ukraine, Lviv, Candidate of Law,
26, Horodotska St., Lviv, 79007 Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-15

МІЖНАРОДНИЙ МЕХАНІЗМ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сироїд Т. Л.

ВСТУП

Кіберзлочинність – це глобальне явище, що стосується всіх держав, і воно так само безмежне, як і сам Інтернет. Поверхня атаки продовжує зростати в міру того, як суспільство стає більш цифровим, і все більше громадян, підприємств, державних служб і пристроїв підключаються до Інтернету.

Складні злочинні мережі діють у всьому світі, координуючи складні атаки за лічені хвилини. Держави та їх правоохоронні органи повинні йти в ногу з новими технологіями, розуміти можливості, які вони відкривають для злочинців, і те, як їх можна використовувати в якості інструментів для боротьби з кіберзлочинністю[1].

Згідно з оцінкою загроз організованої злочинності в Інтернеті (IOCTA), кіберзлочинність стає все більш агресивною та конфронтаційною. Це можна побачити в різних формах кіберзлочинності, включаючи злочини у сфері високих технологій, витік даних та сексуальне насильство.

Кіберзлочинністю є будь-яка злочинна активність у віртуальному просторі (кіберпросторі). У деяких кіберзлочинах здійснюються прямі атаки на комп'ютери або інші пристрої для виведення їх з ладу. В інших кіберзлочинах комп'ютери використовуються правопорушниками для поширення шкідливих програмних кодів, отримання незаконної інформації, розкрадання особистих даних з метою шахрайства. Отже, кіберзлочини – це злочини, вчинені в кіберпросторі (з використанням мережі Інтернет чи іншої комп'ютерної мережі), як компонент злочину. Широкий спектр можливостей, які намагаються використати кіберзлочинці, вражає. До таких злочинів належать: використання ботнетів – мереж пристроїв, заражених шкідливими програмами без відома їх користувачів – для передачі вірусів, які незаконно отримують віддалений контроль над пристроями, крадуть паролі та відключають антивірусний захист; створення «чорних ходів» на скомпрометованих пристроях для крадіжки грошей та даних або віддалений доступ до пристроїв для створення ботнетів; створення онлайн-форумів обміну хакерським досвідом; абузостійкий хостинг та створення противірусних сервісів; відмивання традиційних та віртуальних валют; здійснення онлайн-шахрайства, наприклад через системи онлайн-платежів, кардинг та соціальну інженерію; різні форми сексуальної експлуатації дітей в Інтернеті, включаючи поширення в Інтернеті матеріалів про сексуальне насильство над дітьми та прямі трансляції такого насильства; онлайн-хостинг

[1] Cybercrime. URL: https://www.interpol.int/Crimes/Cybercrime (дата звернення: 20.02.2026).

операцій з продажу зброї, фальшивих паспортів, підроблених та клонованих кредитних карток, наркотиків, а також хакерські послуги.[2]

Встановлення ефективних норм, що регулюють поведінку в місці, яке всі відвідують, але яке нікому не належить, – дуже важке завдання. Однак наявність норм необхідна для забезпечення максимального рівня свободи і зниження ризиків, пов'язаних з перебуванням у кіберпросторі. Враховуючи ту обставину, що технології розвиваються швидше, ніж норми, що регулюють їх застосування, необхідно постійно знаходити шляхи вирішення нових завдань, частіше пов'язаних із такими сферами, як захист даних, транскордонний доступ правоохоронних служб до даних і обмін інформацією між державами-членами та приватними структурами.

1. Міжнародно-правова основа протидії кіберзлочинності

Питання правового регулювання інформаційного простору, захисту осіб у кіберпросторі, протидії злочинам, які вчиняються з використанням можливостей кіберпростору тощо є обговорюваними як на універсальному, так і на регіональному міжнародному рівнях. Зокрема, у межах Організації Об'єднаних Націй (далі – ООН, Організація) вони є центром уваги головних органів організації, інституцій, спеціалізованих структур, установ, форумів, які діють під її егідою (Генеральна Асамблея, Економічна і Соціальна Рада, Комісія із запобігання злочинності і кримінального правосуддя, Конгреси ООН із запобігання злочинності і кримінального правосуддя, Міжнародний союз електрозв'язку (МСЕ), Організація Об'єднаних Націй із питань освіти, науки і культури (ЮНЕСКО), Конференція ООН із торгівлі і розвитку (ЮНКТАД), Програма розвитку Організації Об'єднаних Націй (ПРООН), Управління ООН із наркотиків і злочинності (ЮНОДК), Міжнародна організація кримінальної поліції (Інтерпол) тощо, які акцентують увагу на тому, що кіберзлочинність є одним із нових політичних питань у сфері запобігання злочинності і кримінального правосуддя, яке потребує розроблення шляхів і засобів його вирішення.

Слід зазначити, що ООН ще в 1994 році опублікувала Керівництво із запобігання злочинності, пов'язаної із застосуванням комп'ютерів, і боротьби з нею, в якому зазначалось, що «потенційна сфера охоплення комп'ютерної злочинності така ж широка, як і сфера охоплення міжнародних телекомунікаційних систем». Хоча в Керівництві слово «Інтернет» згадується одноразово, а термін «кіберзлочинність» взагалі не використовується, висновки, які воно містить, є далекоглядними. Основну увагу приділено поняттю «комп'ютерний злочин», формулюванню терміна «кіберзлочинність»[3].

Рішучість щодо прийняття заходів задля того, щоб усі могли користуватися благами нових технологій, особливо інформаційних і комунікаційних, відповідно до рекомендацій, зазначених у Декларації міністрів на сесії

[2] Cybercrime. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (дата звернення:10.02.2026).

[3] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication. 1994). URL: https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF (дата звернення:11.02.2026).

ЕКОСОР 2000 р., була висловлена Декларацією тисячоліття ООН 2000 р. (ст. 20)[4], підтверджена Цілями сталого розвитку ООН (Ціль 9).[5]

Знаковою подією стало прийняття у 2024 році першого всеохоплюючого глобального договору про кіберзлочинність – Конвенції Організації Об'єднаних Націй проти кіберзлочинності (резолюція Генеральної Асамблеї ООН 79/243).[6] Договір об'єднує держави-учасниці спільною метою: запобігання та боротьба з кіберзлочинністю, зокрема шляхом зміцнення міжнародної співпраці, а також сприяння технічній допомозі та розбудові потенціалу, зокрема для країн, що розвиваються. Містить норми щодо криміналізації найпоширеніших форм кіберзлочинності. Розділ Конвенції про криміналізацію вимагає, щоб держави-учасниці створили комплексну систему, спрямовану на злочини, скоєні через системи інформаційно-комунікаційних технологій (далі – ІКТ). Це включає криміналізацію «кіберзалежних злочинів» (широко відомих як «незаконний хакерський злом»), які спрямовані на конфіденційність, цілісність і доступність електронних даних та систем ІКТ, а також «злочинів, що сприяють кіберзлочинності», які є традиційними злочинами, масштаби, швидкість та обсяг яких значно зросли через неправильне використання систем ІКТ. Розділ про юрисдикцію встановлює чіткі та гнучкі правила, що запобігають злочинцям використовувати прогалини в юрисдикції для уникнення покарання, водночас окреслюючи правові сфери, які можуть регулювати держави-учасниці. Конвенція покладає на сторони надавати допомогу іншим державам-учасницям у кримінальних розслідуваннях, коли докази або підозрювані знаходяться на їхній території. Ця співпраця включає екстрадицію, взаємну допомогу у пошуку та збереженні даних, а також взаємну правову допомогу для сприяння збору та обміну доказами. Розділ про процесуальні заходи та правоохоронну діяльність надає державам-учасницям можливість вирішувати питання, пов'язані із забезпеченням електронних доказів, адаптуючи традиційні засоби та методи розслідування до середовища ІКТ. Ці заходи дозволяють ефективно збирати електронні докази, одночасно захищаючи права людини та підтримуючи як національні кримінальні провадження, так і міжнародну співпрацю. Договір покладає на правоохоронців зобов'язання під час розслідування та переслідування кіберзлочинів за допомогою цих процесуальних заходів поважати основні права людини. Розділ про міжнародну співпрацю встановлює глобальну систему, яка дозволяє сторонам договору допомагати одна одній у розслідуваннях, кримінальному переслідуванні, поверненні активів та судових провадженнях через кордони. Розділ про профілактичні заходи розроблений для сприяння

[4] Resolution adopted by the General Assembly [without reference to a Main Committee (A/55/L.2)] 55/2. United Nations Millennium Declaration. URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_55_2.pdf (дата звернення:09.02.2026).

[5] THE 17 GOALS. URL: https://sdgs.un.org/goals (дата звернення:08.02.2026).

[6] 79/243. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. URL: https://docs.un.org/en/A/RES/79/243 (дата звернення 11.02.2026).

зменшенню та управлінню ризиками і загрозами кіберзлочинності. Він передбачає низку профілактичних заходів та акцентує на залученні й активній участі у цьому процесі всіх зацікавлених сторін – урядів, приватного сектору, наукових кіл, організацій громадянського суспільства та громадськості в цілому. Розділ про технічну допомогу та обмін інформацією встановлює широкі заходи щодо технічної допомоги, нарощування потенціалу та обміну інформацією між державами-учасницями, приділяючи особливу увагу потребам країн, що розвиваються. Договір засновує Конференцію держав-учасниць, яка служить основним механізмом нагляду за впровадженням Конвенції та покращенням потенціалу і співпраці між державами-учасницями для досягнення цілей Конвенції.

На міжнародному регіональному знаковим документом є Конвенція про кіберзлочинність 2001 р. Ради Європи (далі – Конвенція (ETS № 185)),[7] яка стала першим міжнародним договором про злочини, що вчиняються через Інтернет та інші комп'ютерні мережі, особливо щодо порушень авторських прав, комп'ютерного шахрайства, дитячої порнографії та порушень мережної безпеки. Вона також містить низку функцій та процедур, таких як пошук комп'ютерних мереж та перехоплення. Основну мету договору викладено у преамбулі і вона полягає у проведенні загальної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, особливо шляхом ухвалення відповідного законодавства та розвитку міжнародного співробітництва.

Конвенцію спрямовано головним чином на гармонізацію елементів внутрішнього кримінального матеріального права щодо правопорушень та пов'язаних із ними положень у сфері кіберзлочинності; надання внутрішньо-державним органам кримінально-процесуальних повноважень, необхідних для розслідування та судового переслідування таких злочинів, а також інших злочинів, вчинених за допомогою комп'ютерної системи або пов'язаних із використанням електронних доказів та інших злочинів; встановлення швидкого та ефективного режиму міжнародного співробітництва.

Застосовуючи Конвенцію (ETS № 185), сторони дотримуються обов'язків урядів захищати людей від злочинів, вчинених онлайн або офлайн шляхом ефективного кримінального розслідування та судового переслідування. Деякі сторони Конвенції вважають, що вони пов'язані міжнародним зобов'язанням надавати засоби захисту від злочинів, вчинених за допомогою комп'ютерної системи (див.: К. У. проти Фінляндії, Європейський суд з прав людини (скарга № 2872/02, судове рішення від 2 березня 2009 р.)[8], з посиланням на процедури та повноваження для кримінальних розслідувань або розглядів, які сторони повинні встановити відповідно до Конвенції. Конвенцію відкрито для приєднання державами, які не є членами Ради Європи.

Конвенція про кіберзлочинність є впливовою міжнародною угодою, що регулює питання порушення закону через Інтернет або інші інформаційні мережі.

[7] Convention on Cybercrime. URL: ttps://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/convention_on_cybercrime_html/Budapest_Convention_on_Cybercrime.pdf (дата звернення:11.02.2026).

[8] Case of K.U. v. Finland (Application no. 2872/02). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-89964%22] (дата звернення:12.02.2026).

Вона вимагає від сторін модернізувати і гармонізувати своє кримінальне законодавство проти дій хакерів та інших порушень безпеки, включаючи порушення авторських прав, шахрайство за допомогою комп'ютера, дитячу порнографію та іншу протиправну кібердіяльність. Договір також передбачає процесуальні повноваження, що охоплюють обшук комп'ютерних мереж і перехоплення комунікацій у контексті боротьби з кіберзлочинністю; створює можливості для ефективного міжнародного співробітництва. Конвенція не є інструментом забезпечення захисту персональних даних, вона криміналізує діяльність, яка може порушувати право суб'єкта на захист особисти даних. Конвенція також зобов'язує договірні сторони передбачити при виконанні Конвенції адекватний рівень захисту прав і свобод людини, у тому числі прав, гарантованих Конвенцією про захист прав людини і основоположних свобод 1950 р., як право на захист персональних даних.

Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (ETS № 189) 2003 р.[9], розширює сферу дії Конвенції про кіберзлочинність, включаючи її суттєві, процедурні та присвячені міжнародному співробітництву положення, охоплюючи також правопорушення, пов'язані з расистською та ксенофобською пропагандою. Таким чином, крім гармонізації суттєвих правових аспектів такої поведінки, Протокол спрямовано на розширення можливостей сторін щодо використання коштів і напрямків міжнародного співробітництва, передбачених Конвенцією (ETS № 185) у цій галузі.

Другий Додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття електронних доказів 2022 р. (CETS 224)[10] спрямовано на подальше зміцнення співпраці у боротьбі з кіберзлочинністю та розширення можливостей органів кримінального правосуддя щодо збирання доказів в електронній формі про кримінальний злочин для цілей конкретних кримінальних розслідувань або розглядів за допомогою додаткових інструментів, що стосуються більш ефективної взаємодії та інших форм співробітництва між компетентними органами; співробітництво у надзвичайних ситуаціях (тобто у ситуаціях, коли існує значний та безпосередній ризик для життя або безпеки будь-якої фізичної особи); та пряме співробітництво між компетентними органами і постачальниками послуг та іншими суб'єктами, які володіють відповідною інформацією або контролюють її.

Негативною ознакою сьогодення стало використання ІКТ у вчиненні терористичних злочинів[11]. У 2015 році Парламентська асамблея Ради Європи (ПАРЄ) прийняла рекомендацію № 2070 щодо зміцнення співробітництва

[9] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. URL: https://rm.coe.int/168008160f (дата звернення:14.02.2026).

[10] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab (дата звернення:14.02.2026).

[11] Сироїд Т. Л., Гавриленко О. А. Внесок Ради Європи у забезпечення інформаційної безпеки та протидію кіберзлочинності. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2020. Вип. 61, т. 2. С. 149–154. DOI https://doi.org/10.32782/2307-3322.61-2.33

у боротьбі з кібертероризмом та іншими масовими атаками в мережі Інтернет[12]. Рекомендація підкреслює роль Ради Європи у вирішенні глобального виклику, пов'язаного з безпекою комп'ютерних мереж у зв'язку з появою кібертероризму та інших масових атак, що діють на/через комп'ютерні системи, являючи собою серйозну загрозу національній безпеці, громадській безпеці та добробуту країн.

Кіберзлочинність також є одним із пріоритетів Європейського Союзу (далі – ЄС, Союз) у боротьбі з серйозною та організованою злочинністю в рамках EMPACT 2022–2025. Кіберзлочинність – проблема, що зростає, для таких країн, як держави-члени ЄС, у більшості яких добре розвинено Інтернет-інфраструктуру і платіжні системи знаходяться в режимі онлайн. Але не лише фінансові дані, а й дані загалом є ключовою мішенню для кіберзлочинців. Кількість та частота витоків даних зростають, що, своєю чергою, призводить до збільшення кількості випадків шахрайства та вимагання.

ЄС докладає суттєвих зусиль до розробки й узгодження законодавства щодо кіберзлочинності, яке діє на території держав-членів, серд таких нормативів слід зазначити: Директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких як електронна торгівля на внутрішньому ринку (в редакції від 17.02.2024); Повідомлення Європейського парламенту, Ради та Комітету регіонів: Загальна політика боротьби з кіберзлочинністю (COM(2007) 267 final); Директива 2011/93/ЄС Європейського парламенту та Ради про боротьбу із сексуальним насильством та сексуальною експлуатацією дітей та дитячою порнографією, яка замінює Рамкове рішення Ради 2004/68/ЈНА (в редакції від 17.12.2011); Повідомлення Комісії Раді та Європейському парламенту: Боротьба зі злочинністю в наш цифровий вік: створення Європейського центру кіберзлочинності (COM(2012) 140 final); Директива 2013/40/ЄС Європейського парламенту та Ради про атаки на інформаційні системи, яка замінює Рамкове рішення Ради 2005/222/ЈНА; Рішення (CFSP) 2019/797 – обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам (в редакції від 14.05.2025); Регламент (ЄС) 2019/796 – обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам (в редакції від 14.05.2025); Регламент (ЄС) 2019/881 Європейського парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, що скасовує Регламент (ЄС) № 526/2013 (Закон про кібербезпеку) (Текст, що стосується ЄЕЗ) (в редакції від 04.02.2025); Регламент (ЄС) 2021/1149 про створення Фонду внутрішньої безпеки (спрямований на забезпечення високого рівня безпеки в Європейському Союзі, зокрема шляхом запобігання та протидії тероризму і радикалізації, серйозній і організованій злочинності та кіберзлочинності); Регламент (ЄС) 2021/887 про створення Європейського промислового, технологічного та науково-дослідного центру кібербезпеки

[12] Increasing co-operation against cyberterrorism and other largescale attacks on the Internet. URL: http://www.europeanrights.eu/public/atti/2070_ing.pdf (дата звернення: 13.02.2026).

та мережі національних координаційних центрів,; Директива (ЄС) 2024/1385 про боротьбу з насильством щодо жінок та домашнім насильством, яка спрямована на введення цільових мінімальних правил щодо прав цієї групи жертв злочинів і криміналізації найбільш важких форм насилля стосовно жінок і кібернасилля; Регламент (ЄС) 2024/2847 (в редакції від 20.11.2024), який встановлює горизонтальні вимоги до кібербезпеки для продуктів із цифровими елементами; Регламент (ЄС) 2024/1689, що встановлює гармонізовані правила щодо штучного інтелекту.

Перш за все слід зазначити, що прийняті ЄС акти мають за мету унормувати діяльність, пов'язану з використанням ІКТ у різних сферах відносин. Так, Директива 2000/31/ЄС[13] встановлює стандартні правила ЄС із різних питань, пов'язаних з електронною торгівлею. Вона спрямована на сприяння належному функціонуванню внутрішнього ринку шляхом забезпечення вільного переміщення послуг інформаційного суспільства між державами-членами. Документ наближає деякі національні положення про послуги інформаційного суспільства, що стосуються: внутрішнього ринку, постачальників послуг, комерційного зв'язку, електронних контрактів, відповідальності посередників, кодексів поведінки, позасудового врегулювання спорів, судових позовів та співробітництва між державами-членами. Директива доповнює законодавство Союзу, що застосовується до послуг інформаційного суспільства, без шкоди для рівня захисту, зокрема, громадської охорони здоров'я та інтересів споживачів, встановленого актами Союзу та національним законодавством, що їх реалізує, тією мірою, якою це не обмежує свободу надання послуг інформаційного суспільства.

Директиву 2013/40/ЄС[14] спрямовано на боротьбу з кіберзлочинністю та забезпечення інформаційної безпеки завдяки суворішому державному законодавству, суворішим кримінальним покаранням та більш тісній співпраці між надмірними податками. Директива запроваджує нові правила, що гармонізують криміналізацію та покарання за низку правопорушень, спрямованих проти інформаційних систем. Ці правила включають заборону використання ботнетів – шкідливого програмного забезпечення, призначеного для віддаленого управління мережею комп'ютерів. Основними видами кримінальних злочинів, що охоплюються Директивою, є атаки на інформаційні системи, починаючи від атак типу «відмова в обслуговуванні», призначених для виведення із ладу сервера, і закінчуючи перехопленням даних та атаками ботнетів. Директива зобов'язує держави-члени криміналізувати означені правопорушення; розширювати співпрацю правоохоронних органів. Директива передбачає зближення систем кримінального законодавства країн ЄС та розширення співробітництва

[13] Consolidated text: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000L0031-20240217 (дата звернення:12.02.2026).

[14] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng (дата звернення: 12.02.2026).

між судовими органами щодо незаконного доступу до інформаційних систем, незаконного втручання у систему, незаконного втручання в дані, незаконного перехоплення. Документ містить норми щодо запровадження ефективних, пропорційних та стримуючих санкцій. Покладає зобов'язання на держави-члени щодо вжиття необхідних заходів для забезпечення того, щоб такі діяння, як незаконний доступ до інформаційних систем, незаконне втручання у систему, незаконне втручання в дані, незаконне перехоплення, засоби, що використовуються для вчинення правопорушень, а також підбурювання, пособництво та підбурювання і спроба скоєння означених злочинів (статті 3–8), каралися ефективними, пропорційними і кримінальними покараннями.

Рішення (CFSP) 2019/797[15] та Регламент (ЄС) 2019/796[16], запроваджують структуру, яка дозволяє ЄС вводити санкції для стримування та реагування на кібератаки, які становлять зовнішню загрозу для ЄС чи країн ЄС. Такі протиправні дії включають атаки, що стосуються інформаційних систем, а також: критичної інфраструктури, необхідної для життєдіяльності суспільства чи здоров'я громадян, безпеки, захисту та економічного чи соціального благополуччя; послуг, необхідних для основної соціальної та економічної діяльності, зокрема енергетика, транспорт, банківська справа; фінансів, охорони здоров'я, питної води, цифрової інфраструктури; найважливіших державних функцій, зокрема оборони, управління та функціонування інститутів, публічних виборів, економічної та громадянської інфраструктури, внутрішньої безпеки і зовнішніх зв'язків, включаючи дипломатичні місії; зберігання чи обробка секретної інформації; або урядових аварійно-рятувальних загонів. Ці кібератаки включають атаки на країни, які не є членами ЄС, або міжнародні організації, коли дії вважаються необхідними для досягнення спільних цілей зовнішньої та безпекової політики ЄС.

Означені нормативи дозволяють ЄС накладати санкції на осіб чи організації, які відповідальні за кібератаки чи спроби кібератак, надають фінансову, технічну чи матеріальну підтримку таким атакам, чи беруть участь у них в інший спосіб. Санкції можуть також застосовуватись до пов'язаних з ними осіб або організацій. Обмежувальні заходи включають заборону на в'їзд до ЄС та заморожування активів. На країни ЄС покладено зобов'язання щодо встановлення мір покарання за ці правопорушення.

Регламентом (ЄС) 2024/2847[17] встановлено горизонтальні вимоги щодо кібербезпеки для продуктів із цифровими елементами. Документ визначає правила допуску на ринок продуктів із цифровими елементами для забезпечення кібербезпеки таких продуктів; основні вимоги до кібербезпеки

[15] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng (дата звернення: 12.02.2026).

[16] Там само.

[17] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (дата звернення: 12.02.2026).

для проектування, розробки та виробництва продуктів, а також зобов'язання для економічних операторів щодо кібербезпеки цієї продукції; основні вимоги до кібербезпеки для процесів обробки вразливостей, застосовних виробниками, і пов'язані з ними зобов'язання; правила нагляду за ринком, включаючи моніторинг і забезпечення дотримання вимог.

Регламент (ЄС) 2024/1689[18] встановлює гармонізовані правила розміщення на ринку, введення в експлуатацію та використання систем штучного інтелекту (ШІ) в ЄС. Він забороняє певні практики та запроваджує особливі вимоги для систем ШІ з високим ризиком, а також зобов'язання для операторів таких систем; включає гармонізовані правила прозорості для певних систем ШІ, гармонізовані правила розміщення на ринку моделей ШІ загального призначення, правила моніторингу ринку, нагляду за ринком, управління та забезпечення дотримання; запроваджує заходи, спрямовані на підтримку інновацій. Метою Регламенту є покращення функціонування єдиного ринку ЄС та сприяння впровадженню орієнтованого на людину та надійного ШІ, забезпечуючи при цьому високий рівень захисту здоров'я, безпеки та основних прав, закріплених Хартією ЄС про основні права, від негативного впливу систем ШІ в ЄС.

Директива (ЄС) 2024/1385 про боротьбу з насильством щодо жінок та домашнім насильством[19] визначає в якості кримінальних правопорушень кіберпереслідування (ст. 6), кібердомагання (ст. 7) та кіберпідбурювання до насильства чи ненависті (с. 8) тощо.

Організація з безпеки і співробітництва в Європі (далі – ОБСЄ) також відіграє важливу роль у підвищенні кібер- / ІКТ-безпеки, зокрема за рахунок зниження ризиків конфліктів між державами, що виникають унаслідок використання ІКТ. Ключовим завданням щодо цього є введення в дію відповідних вказівок ООН з боку груп урядових експертів на регіональному рівні.

Багато держав інвестують у наступальні та оборонні можливості ІКТ, додаючи складний вимір міждержавним відносинам. Такі можливості можуть змінюватись від розвідувальних та інформаційних операцій до порушення критично важливих мереж і служб або можливостей управління та командування.

Унікальні характеристики ІКТ значно збільшили ймовірність неправильного сприйняття, прорахунків та навіть напруженості між державами, коли вони стикаються з питаннями намірів, атрибуції, правил та норм. У відповідь держави-учасниці ОБСЄ працюють над заходами зміцнення довіри (далі – ЗД) для зниження ризиків конфліктів, що виникають унаслідок використання ІКТ. Вони покликані зробити кіберпростір більш передбачуваним і пропонують конкретні інструменти та механізми, щоб уникнути непорозумінь, зокрема такі: механізм об'єднання держав для консультацій з приводу можливих інцидентів у сфері

[18] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 12.02.2026).

[19] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. URL: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення:12.02.2026).

кібер- / ІКТ-безпеки з метою зниження напруженості, що зростає; платформу для обміну думками, національною політикою та підходами в галузі безпеки і сфері кібер/ІКТ, що дозволяє державам краще «читати» наміри одна одної в кіберпросторі; конкретні напрямки роботи, наприклад захист критично важливої інфраструктури з використанням ІКТ, що дозволяють державам-учасницям колективно підвищувати кіберстійкість у регіоні ОБСЄ на благо всіх.

На додаток до ЗД безпеки, кібер / ІКТ, ОБСЄ та її інститути також зосереджені на протидії загрозам безпеці кібер/ІКТ з боку недержавних суб'єктів, таких як організована злочинність і терористи. Ключовий акцент тут робиться на заохоченні адекватних і своєчасних заходів у відповідь з боку національних органів влади на ці мінливі загрози, починаючи від більш якісної судової експертизи і закінчуючи інноваційними підходами, що дозволяють запобігти перетворенню ІКТ на тактичних помічників терористів.

Заходи з правової протидії кіберзлочинності запроваджуються і на рівні Ліги арабських держав, в межах якої прийнято Арабську конвенцію про боротьбу зі злочинами, пов'язаними з технологіями, яку спрямовано на покращання співпраці між арабськими державами в боротьбі з правопорушеннями у сфері інформаційних технологій для захисту безпеки та інтересів арабських держав, а також безпеки їхніх спільнот і окремих осіб (2010 р.). Договір містить визначення злочинів, пов'язаних із використанням інформаційних технологій, процесуальні положення та механізми правової і судової співпраці між державами-учасницями у цій сфері[20].

Африканський союз докладає зусиль щодо розробки правової основи у протидії кіберзлочинності, яка має тенденції до зростання в регіоні. Це підтверджується статистичними даними, згідно яких африканський континент демонструє один із найшвидших темпів зростання проникнення Інтернету у світі, а цифрове підключення майже потроїлося за останні п'ять років. У той самий період як уряди, так і приватні структури в Африці стикаються зі зростаючою тенденцією кібератак, що відповідає тому, що було зафіксовано також на глобальному рівні. Масштабні крадіжки персональних даних, комп'ютерні втручання, цькування, переслідування та інші форми кібернасилля або сексуального насильства щодо дітей в Інтернеті є нападами на права людини. Мова ненависті, ксенофобія та расизм сприяють радикалізації, що призводить до насильницького екстремізму. Атаки на комп'ютери та дезінформація, що використовуються на виборах і передвиборчих кампаніях, є атаками на функціонування фундаментальних інституцій та політичну стабільність. Щоденні атаки на критичну інформаційну інфраструктуру впливають на національну безпеку, економічні та інші національні інтереси, а також на міжнародний мир і стабільність[21].

[20] Arab Convention on Combating Information Technology Offences. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/arab_convention_on_combating_information_technology_offences__html/Arab_Convention_on_Combating_Information_Technology_Offences.pdf (дата звернення:12.02.2026).

[21] African Forum on cybercrime. URL: https://au.int/fr/node/34897 (дата звернення: 13.02.2026).

Серед правових актів слід вказати Конвенцію Африканського Союзу про кібербезпеку та захист особистих даних (2014 р.), яку спрямовано на створення законодавчої бази для забезпечення кібербезпеки та захисту персональних даних. Договір покладає на держави-учасниці зобов'язання щодо розробки національної політики кібербезпеки та відповідного інституційного механізму управління; розробки законодавства та створення інститутів у сфері протидії кіберзлочинності; забезпечення моніторингу та реагування на інциденти і попередження; здійснення національної і транскордонної координації та глобальної співпраці[22].

У межах АС розроблено Стратегію AFRIPOL щодо боротьби з кіберзлочинністю 2020-2024 рр.[23]. Вона є гнучким документом, який підлягає періодичному перегляду з метою забезпечення його актуальності, подальшого реагування на нові загрози у динамічному середовищі, в якому діють сили безпеки, та відповідність очікуванням держав-членів. Документ, головним чином, має на меті розробити дорожню карту боротьби з кіберзлочинністю, тобто основні напрямки дій для розробки заходів контролю за злочинами, спрямованими на комп'ютери та інформаційні системи, у спробах отримати несанкціонований доступ до пристроїв або запобігти доступу законних користувачів до цих пристроїв (часто за допомогою шкідливого програмного забезпечення).

Стратегія зосереджена на чотирьох напрямках дій зі спільною метою допомогти державам розробити узгоджені методології контролю та таким чином забезпечити плідний обмін інформацією. Ці напрямки полягають у наступному: зміцнення можливостей центральної групи AFRIPOL з боротьби з кіберзлочинністю, а також команд держав-членів, шляхом надання ресурсів та механізмів для збору доказів, необхідних для цифрових розслідувань; спеціалізована підготовка фахівців у боротьбі з кіберзлочинністю; розробка гармонійного та узгодженого регулювання, а також широка співпраця між державами-членами Африканського Союзу; забезпечення постійної оцінки загроз щодо кіберзлочинності на рівні суспільства/членства.

Ключовою частиною інтеграційних пріоритетів АС є Стратегія цифрової трансформації АС на 2020–30 рр.[24] Ктім того, Порядок денний 2063[25] – довгостроковий план розвитку Африканського Союзу, який відповідає глобальній рамковій програмі Цілей сталого розвитку ООН, зазначає науку, технології, інновації та охорону здоров'я як ключові цілі, що є пріоритетами для трансформації Африки.

---

[22] African Union Convention on Cyber Security and Personal Data Protection. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/african_union_convention_on_cyber_security_and_personal_data_protection__html/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата звернення: 11.02.2026).

[23] AFRIPOL Cybercrime Strategy. URL: https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/ (дата звернення: 13.02.2026).

[24] The Digital Transformation Strategy for Africa (2020-2030). URL: https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.p (дата звернення: 13.02.2026).

[25] Documents Agenda 2063. URL: https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf (дата звернення: 13.02.2026).

2. Міжнародна інституційна основа протидії кіберзлочинності

Найбільший обсяг роботи у справі боротьби з міжнародною злочинністю на інституційному універсальному рівні здійснюється в межах Міжнародної організації кримінальної поліції (Інтерпол).[26] Невід'ємною складовою діяльності Інтерполу є протидія комп'ютерній злочинності, на нього покладено функцію збирання, обробки й аналізу інформації, яка поступає з мережі Інтернет із метою надання допомоги у виявленні протиправних діянь, вчинення яких полегшується завдяки Інтернету. Крім того, Цільовою групою по здійсненню контртерористичних операцій створено Робочу групу по боротьбі з використанням Інтернету в терористичних цілях. До завдань якої віднесено: виявлення і об'єднання зусиль зацікавлених сторін і партнерів з метою обміну інформацією, а також визначення можливих шляхів протидії цій загрозі на національному, регіональному і глобальному рівнях; вивчення питання щодо ролі ООН у координації дій держав-членів.

Зважаючи на ту особливість, що негативною ознакою сьогодення стало використання ІКТ у скоєнні терористичних злочинів, безперечно, значну роль в організаційній співпраці протидії злочинності відіграє Контртерористичний комітет (КТК) (резолюція Ради Безпеки ООН 1373 (2001))[27], створений з метою сприяння зміцненню потенціалу держав-членів ООН щодо запобігання терористичним актам як на національному, так і на міжрегіональному рівні. Резолюція 1373 (2001) закликає держави-члени здійснити низку заходів, спрямованих на зміцнення їхніх правових та інституційних можливостей у галузі боротьби з тероризмом, у тому числі криміналізувати фінансування тероризму; невідкладно заблокувати будь-які засоби, пов'язані з особами, причетними до терористичних актів; не надавати ні в якій формі фінансову підтримку терористичним групам; здійснювати обмін інформацією з іншими урядами щодо будь-яких груп, які вчиняють чи які планують здійснити терористичні акти; співпрацювати з іншими урядами в розслідуванні, виявленні, арешті, видачі та переслідуванні осіб, причетних до таких актів тощо.

Спеціалізована установа ООН Міжнародний союз електрозв'язку (далі – МСЕ) сприяє інноваціям у сфері інформаційно-комунікаційних технологій, а також у питаннях кіберзлочинності. Для прийняття конкретних заходів, спрямованих на обмеження комп'ютерних загроз, МСЕ розробив Глобальну програму кібербезпеки, яка забезпечує рамки для координації зусиль щодо задоволення юридичних, технічних, організаційних і навчальних потреб у всьому світі. Програма визначила основні принципи, цілі та стратегії розробки моделей законодавства у сфері боротьби з кіберзлочинністю та базується на п'яти стратегічних принципах, а саме: правові заходи; технічні та

[26] Constitution of the International CriminaL Police Organization-INTERPOL. URL: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents (дата звернення: 10.02.2026).

[27] Resolution 1373 (2001). URL: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (дата звернення: 12.02.2026).

процедурні заходи; організаційні структури; створення потенціалу; міжнародне співробітництво (с. 506)[28].

У межах регіональних міжнародних організацій також функціонує низка структур, інституцій та агенств що сприяють підвищенню кібербезпеки, серед яких слід вказати Європейське поліцейське агентство (Європол), правовим підґрунтям функціонування якого є Регламент (ЄС) 2016/794 (в редакції від 28.06.2022). Серед завдань Європолу, означених статею 88 Договору про функціонування Європейського Союзу (ДФЄС), віднесено такі: підтримка та зміцнення діяльності поліцейських органів та інших правоохоронних служб держав-членів, їхньої взаємної співпраці щодо запобігання та протидії тяжким злочинам, що впливають на дві або більше держав-членів, тероризму та тим формам злочинів, що впливають на спільні інтереси, охоплені політикою ЄС[29], зокрема ... комп'ютерній злочинності, виготовленню контрафактної і піратської продукції тощо.

Регламент (ЄС) 2016/794 уповноважив Європол на виконання таких задач: збирання, збереження, обробка, аналіз інформації і даних, а також обмін інформацією і даними; безвідкладне повідомлення компетентним органам держав-членів через спеціальний відділ про факти, які їх зачіпають, і сповіщення про зв'язок, який констатовано між злочинами; сприяння розслідуванням у державах-членах, особливо шляхом передачі національним відділам усієї необхідної інформації з цього приводу; звернення до компетентних органів відповідних держав-членів із запитами про порушення, проведення та координацію розслідувань і висунення пропозицій щодо створення сумісних слідчих бригад у визначених справах; надання державам-членам інформації та допомоги в аналізі при проведенні масштабних заходів («зустрічі у верхах», міжнародні спортивні змагання) тощо[30].

Заслуговують на увагу практичні інноваційні підходи Європолу щодо запобігання кіберзлочинам, серед яких слід вказати програму «Кіберзахисники», яка має за мету підвищення обізнаності про кіберзлочини[31].

Агентство Європейського союзу з кібербезпеки (ENISA) займається досягненням високого загального рівня кібербезпеки в Європі (створене в 2004 р.

---

[28] Сироїд Т.Л. Міжнародно-правове регулювання сфери інформаційно-комунікаційних технологій і протидія кіберзлочинності // Сучасні проблеми міжнародного права. Liber Amicorum до 60-річчя проф. М. В. Буроменского: моногр. / авт. кол.; за ред. В. М. Репецького, В. В. Гутника. Львів; Одеса: Фенікс, 2017. 564 с. С. 495-521. ISBN 978-966-928-118-0

[29] Consolidated version of the Treaty on the Functioning of the European Union. URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng (дата звернення:10.02.2026).

[30] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. https://eur-lex.europa.eu/eli/reg/2016/794/oj/eng (дата звернення: 13.02.2026).

[31] Cyber Defenders. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/cyber-defenders (дата звернення: 13.02.2026).

та посилене Регламентом (ЄС) 2019/881 (в редакції 04.02.2025)[32]. ENISA робить свій внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг та процесів ІКТ за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами й органами ЄС та допомагає Європі підготуватися до кібервикликів у майбутньому. За допомогою обміну знаннями, нарощування потенціалу та підвищення обізнаності Агентство працює разом зі своїми ключовими зацікавленими сторонами над зміцненням довіри до підключеної економіки, підвищенням стійкості інфраструктури ЄС та, зрештою, для забезпечення цифрової безпеки європейського суспільства і громадян.

З 2013 року функціонує Європейський центр боротьби з кіберзлочинністю (ЕС3)[33] – підрозділ Європолу покликаного відігравати провідну роль у боротьбі з кіберзлочинністю на території ЄС. ЕС3 займається створенням оперативних і аналітичних потужностей, необхідних для забезпечення швидкого реагування на кіберзлочини, а також організацією взаємодії офіційних відомств ЄС і країн-членів з міжнародними партнерами. Мандат ЕС3 охоплює такі сфери відповідальності: боротьба зі злочинами, які вчиняються організованими злочинними групами та тягнуть за собою отримання незаконних доходів в особливо великих розмірах (шахрайство з кредитними картками або банківськими операціями); боротьба зі злочинами, що завдають серйозної шкоди жертві, зокрема розбещення малолітніх; боротьба з діями, спрямованими на спричинення шкоди або виведення з ладу інфраструктури та інформаційних систем ЄС. ЕС3 також відповідальний за збір та обробку даних, надання інформаційної, технічної та криміналістичної підтримки відповідним підрозділам правоохоронних органів країн – членів ЄС, координацію спільних розслідувань, навчання й підготовку фахівців (у співпраці із CEPOL). Центр сприяє проведенню необхідних досліджень і створенню програмного забезпечення, опікується оцінкою й аналізом наявних і потенційних загроз, складанням прогнозів і випуском завчасних попереджень. Сфера його діяльності також охоплює надання допомоги суддям і прокурорам[34].

Щороку ЕС3 публікує оцінку загрози організованої злочинності в Інтернеті (IOCTA) – флагманський стратегічний звіт про ключові результати, нові загрози та події в кіберзлочинності. IOCTA демонструє, наскільки широкою і різноманітною є кіберзлочинність і як ЕС3 є ключовою частиною Європолу та відповідних заходів ЄС. ЕС3 використовує тристоронній підхід до боротьби з кіберзлочинністю: криміналістика, стратегія та операції. Ці заходи також

[32] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (дата звернення: 13.02.2026).

[33] Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012DC0140 (дата звернення: 12.02.2026).

[34] European Cybercrime Centre URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення:12.02.2026).

підтримуються Групою кіберрозвідки (CIT), аналітики якої збирають та обробляють інформацію, пов'язану з кіберзлочинністю, з державних, приватних та відкритих джерел і визначають загрози та моделі, що виникають.

Сумісно з ЕС3 працює Спільна цільова група боротьби з кіберзлочинністю (J-CAT) (створена у 2014 р.), яка надає допомогу у протидії кіберзлочинності всередині та за межами ЄС. Цільова група має за мету стимулювати та координувати дії, засновані на інтелекті, з ключовими загрозами та цілями кіберзлочинності, полегшуючи спільну ідентифікацію, встановлення пріоритетів, підготовку та початок транскордонних розслідувань та операцій з боку своїх партнерів. Її компетенція J-CAT охоплює: високотехнологічні злочини (зокрема шкідливе програмне забезпечення, вторгнення); сприяння вчиненню злочинів (куленепробивний хостинг, контр-антивірусні послуги, лізинг та оренда інфраструктури, відмивання грошей, включаючи віртуальні валюти); онлайн-шахрайство (онлайн-платіжні системи, кардинг, соціальна інженерія).[35]

Кіберзлочинність – це зростаюча та швидкорозвинена сфера злочинності, яка становить значну частку загальної роботи Євроюсту – Агентства Європейського Союзу з питань співробітництва у сфері кримінального правосуддя, – це унікальний центр де національні судові органи тісно співпрацюють у боротьбі з серйозною організованою транскордонною злочинністю. Роль Євроюсту полягає в тому, щоб допомогти зробити Європу безпечнішим місцем шляхом координації роботи національних органів влади-держав-членів ЄС, а також третіх держав – у розслідуванні та переслідуванні транснаціональної злочинності[36]. Євроюст підтримує національні органи влади у співпраці та використанні доступних інструментів транскордонного розслідування кіберзлочинності та пов'язаної з нею злочинності.

Європейська судова мережа з питань кіберзлочинності (EJCN)[37], створена у 2016 році для сприяння контактам між фахівцями, які спеціалізуються на протидії викликам, що виникають у зв'язку з кіберзлочинністю, кібер-злочинністю та розслідуваннями в кіберпросторі, а також для підвищення ефективності розслідувань і кримінального переслідування. EJCN посилює співпрацю між компетентними судовими органами, забезпечуючи обмін досвідом, передовим досвідом та іншими відповідними знаннями щодо розслідування та кримінального переслідування кіберзлочинності.

Євроюст є ключовим партнером EJCN, особливо в ситуаціях, коли Мережа має справу з численними викликами, пов'язаними з дійсно безкордонним характером кіберзлочинності. Крім того, Євроюст проводить регулярні зустрічі Мережі та підтримує обмін інформацією між членами EJCN та іншими

[35] Joint Cybercrime Action Taskforce. URL: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (дата звернення:08.02.2026).

[36] Consolidated text: Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA. URL: https://eur-lex.europa.eu/eli/reg/2018/1727/2025-11-04/eng (дата звернення: 13.02.2026).

[37] European Judicial Cybercrime Network. URL: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network (дата звернення: 12.02.2026).

зацікавленими сторонами, які відіграють роль у забезпеченні верховенства права в кіберпросторі.

Серед регіональних структур слід зазначити Механізм співробітництва поліції Африканського Союзу (AFRIPOL) – це технічна установа АС, яка має за завдання зміцнювати та гармонізувати можливості правоохоронних органів у державах-членах. Його місія полягає в підтримці африканських поліцейських служб у запобіганні та боротьбі з транснаціональною організованою злочинністю, тероризмом, кіберзлочинністю та іншими новими загрозами континентальній безпеці.

На виконання свого мандату AFRIPOL надає комплексний спектр механізмів підтримки, серед яких: очне та онлайн-навчання, включаючи спеціалізовані курси через спеціалізовану платформу електронного навчання; навчання тренерів для забезпечення національної стійкості навичок; проведення семінарів для обміну досвідом та передовим досвідом між державами-членами; доступ до судово-медичних та слідчих інструментів; підтримка спільних операцій та транскордонних розслідувань; сприяння державно-приватному партнерству для вдосконалення стратегій запобігання злочинності; сприяння співпраці через безпечну систему зв'язку та спільні бази даних; стажування та можливості отримання стипендій для розвитку майбутніх лідерів правоохоронних органів[38].

Контртерористичний центр Африканського Союзу (AUCTC) – спеціалізована установа, створена для зміцнення потенціалу держав-членів АС у сфері реагування на боротьбу з тероризмом та насильницьким екстремізмом. Працюючи у тісній співпраці з регіональними економічними співтовариствами і регіональними механізмами, AUCTC надає технічну, оперативну та стратегічну підтримку. Він розробляє інструменти та програми для запобігання, аналізу та ефективного реагування на терористичні загрози на африканському континенті[39].

ВИСНОВОК

Підсумовуючи вищеозначене слід констатувати, що кіберзлочини є складними не лише за своїми юридичними ознаками, але й тому, що вони часто мають транснаціональний характер, тобто це діяння, ініціювання, запобігання чи наслідки яких зачіпають більш ніж одну країну, і вони мають багатонаціональний характер. Крім того, вони є видом професійної діяльності організованих злочинних груп. Кіберзлочини охоплюють широкий спектр об'єктів посягання. Вони послаблюють економіку держав, впливаючи (прямо та опосередковано) на економічні витрати урядів і тягнуть за собою кримінальну діяльність, яка може загрожувати стабільності держав, особливо у випадку поєднання з транснаціональною злочинністю, включаючи відмивання грошей, контрабанду зброї, торгівлю наркотичними речовинами. Крім того, вони посягають на права і свободи людини (крадіжка особистих даних фізичних осіб, насилля щодо неповнолітніх, насилля стосовно жінок).

[38] About AFRIPOL. URL: https://afripol.africa-union.org/about (дата звернення: 13.02.2026).

[39] African Union Counter Terrorism Centre. ABOUT US. URL: https://caert.org.dz/about-us/мм(дата звернення: 13.02.2026).

Подолання цього негативного явища потребує сумісних активних дій з боку держав і міжнародного співтовариства та вирішення спільних проблем, серед яких: 1. Втрата даних: електронні дані є ключем до успішних розслідувань у всіх сферах кіберзлочинності, але можливості отримання таких даних значно обмежені. 2. Втрата місцезнаходження: останні тенденції призвели до ситуації, коли правоохоронні органи більше не можуть встановити фізичне місцезнаходження злочинця, злочинну інфраструктуру чи електронні докази. 3. Проблеми, пов'язані з національними правовими рамками: відмінності у національних правових базах держав. 4. Перешкоди для міжнародної співпраці: у міжнародному контексті не існує спільної правової бази для прискореного обміну доказами (як і для їх збереження). Існує також очевидна потреба в кращому механізмі транскордонної комунікації та швидкого обміну інформацією. 5. Проблеми державно-приватного партнерства: співпраця з приватним сектором є життєво важливою для боротьби з кіберзлочинністю, проте стандартизованих правил взаємодії немає, і таким чином розслідування можуть бути ускладнені[40].

Міжнародне співтовариство докладає зусиль щодо розробки правової основи протидії кіберзлочиннності та криміналізації протиправних дій про що свідчать акти, прийняті на рівні ООН та регіональних міжнародних організацій (РЄ, ЄС, ОБСЄ, ЛАД, АС), згідно з якими кіберзлочини віднесено до окремого виду міжнародних правопорушень. Важливим є імплементація існуючих міжнародних норм у національне законодавство; криміналізація кіберзлочинів; посилення співпраці держав з міжнародними спеціалізованими інституційними органами (структурами, агентствами) універсального і регіонального характеру задля попередження розповсюдження злочинів та притягнення до відповідальності винних осіб.

АНОТАЦІЯ

Стаття присвячена дослідженню міжнародно-правової та інституційної складової протидії кіберзлочинності. Проаналізовано положення міжнародних універсальних актів, акцентовано увагу на першому глобальному договорі про кіберзлочинність – Конвенції Організації Об'єднаних Націй проти кіберзлочинності (резолюція Генеральної Асамблї ООН 79/243). Розкрито сутність та особливості актів, прийнятих на рівні Ради Європи (Конвенція про кіберзлочинність 2001 р та додаткові протоколи до Конвенції, рекомендації тощо), Європейського Союзу (установчі акти, директиви, рішення, регламенти, повідомлення), Африканського Союзу (договірні та стратегічні акти); означено роль ОБСЄ у підвищенні кібер- / ІКТ-безпеки тощо. Зосереджено увагу на діяльності органів, інституцій, агентств, створених на міжнародному універсальному рівні (Міжнародна організація кримінальної поліції (Інтерпол), Контртерористичний комітет ООН, Міжнародний союз електрозв'язку тощо) та на регіональному рівні (Європейське поліцейське агентство (Європол),

[40] Common challenges in combating cybercrime As identified by Eurojust and Europol June 2019. URL: https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf (дата звернення: 13.02.2026).

Агентство Європейського Союзу з питань співробітництва у сфері кримінального правосуддя (Євроюст), Агентство Європейського союзу з кібербезпеки, Європейський центр боротьби з кіберзлочинністю, Механізм поліцейського співробітництва Африканського Союзу (AFRIPOL), Контр-терористичний центр Африканського Союзу (AUCTC) тощо) та їх ролі у протидії кіберзлочинності. Зроблено відповідні висновки і рекомендації.

Ключові слова: безпекові виклики, електронна торгівля, злочини, імплементація, криміналізація, міжнародні інституції, міжнародне співробітництво, особисті дані, права людини, Цілі сталого розвитку, штучний інтелект.

Література

1. About AFRIPOL. URL: https://afripol.africa-union.org/about (дата звернення: 13.02.2026).
2. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. URL: https://rm.coe.int/168008160f (дата звернення: 14.02.2026).
3. African Forum on cybercrime. URL: https://au.int/fr/node/34897 (дата звернення: 13.02.2026).
4. African Union Counter Terrorism Centre. ABOUT US. https://caert.org.dz/about-us/мм (дата звернення: 13.02.2026).
5. African Union Convention on Cyber Security and Personal Data Protection. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/african_union_convention_on_cyber_security_and_personal_data_protection__html/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата звернення:11.02.2026).
6. AFRIPOL Cybercrime Strategy. URL: https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/ (дата звернення: 13.02.2026).
7. Arab Convention on Combating Information Technology Offences. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/arab_convention_on_combating_information_technology_offences__html/Arab_Convention_on_Combating_Information_Technology_Offences.pdf (дата звернення:12.02.2026).
8. Case of K.U. v. Finland (Application no. 2872/02). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-89964%22] (дата зверненн:12.02.2026).
9. Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012DC0140 (дата звернення: 12.02.2026).
10. Common challenges in combating cybercrime As identified by Eurojust and Europol June 2019. URL: https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf (дата звернення: 13.02.2026).
11. Consolidated text: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services,

in particular electronic commerce, in the Internal Market (Directive on electronic commerce). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000L0031-20240217 (дата звернення:12.02.2026).

12. Convention on Cybercrime. URL: ttps://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/convention_on_cybercrime_html/Budapest_Convention_on_Cybercrime.pdf (дата звернення:11.02.2026).

13. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng (дата звернення: 12.02.2026).

14. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/eli/reg/2019/796/oj/eng (дата звернення: 12.02.2026).

15. Consolidated version of the Treaty on the Functioning of the European Union. URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng (дата звернення: 10.02.2026).

16. Consolidated text: Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA. URL: https://eur-lex.europa.eu/eli/reg/2018/1727/2025-11-04/eng (дата звернення: 13.02.2026).

17. Constitution of the International CriminaL Police Organization-INTERPOL. URL: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents (дата звернення: 10.02.2026).

18. Cyber Defenders. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/cyber-defenders (дата звернення: 13.02.2026).

19. Cybercrime. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (дата звернення: 10.02.2026).

20. Cybercrime. URL: https://www.interpol.int/Crimes/Cybercrime (дата звернення: 10.02.2026).

21. Сироїд Т. Л., Гавриленко О. А. Внесок Ради Європи у забезпечення інформаційної безпеки та протидію кіберзлочинності. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2020. Вип. 61, т. 2. С. 149–154. DOI https://doi.org/ 10.32782/2307-3322.61-2.33

22. Сироїд Т.Л. Міжнародно-правове регулювання сфери інформаційно-комунікаційних технологій і протидія кіберзлочинності // Сучасні проблеми міжнародного права. Liber Amicorum до 60-річчя проф. М. В. Буроменского: моногр. / авт. кол.; за ред. В. М. Репецького, В. В. Гутника. Львів; Одеса: Фенікс, 2017. 564 с. С. 495-521. ISBN 978-966-928-118-0

23. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення: 12.02.2026).

24. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng (дата звернення:12.02.2026).

25. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. URL: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення:12.02.2026).

26. Documents Agenda 2063. URL: https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf (дата звернення: 13.02.2026).

27. European Cybercrime Centre URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення:12.02.2026).

28. European Judicial Cybercrime Network. URL: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network (дата звернення: 12.02.2026).

29. Increasing co-operation against cyberterrorism and other largescale attacks on the Internet. URL: http://www.europeanrights.eu/public/atti/2070_ing.pdf (дата звернення:13.02.2026).

30. Joint Cybercrime Action Taskforce. URL: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (дата звернення:08.02.2026).

31. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (дата звернення: 12.02.2026).

32. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 12.02.2026).

33. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. https://eur-lex.europa.eu/eli/reg/2016/794/oj/eng (дата звернення: 13.02.2026).

34. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (дата звернення: 13.02.2026).

35. Resolution adopted by the General Assembly [without reference to a Main Committee (A/55/L.2)] 55/2. United Nations Millennium Declaration. URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_55_2.pdf (дата звернення:09.02.2026).

36. Resolution 1373 (2001). URL: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (дата звернення: 12.02.2026).

37. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab (дата звернення:14.02.2026).

38. The Digital Transformation Strategy for Africa (2020-2030). URL: https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.p (дата звернення: 13.02.2026).

39. THE 17 GOALS. URL: https://sdgs.un.org/goals (дата звернення: 08.02.2026).

40. 79/243. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. URL: https://docs.un.org/en/A/RES/79/243 (дата звернення 11.02.2026).

41. UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication. 1994). URL: https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF (дата звернення:11.02.2026).

Information about the author:
Syroid Tetiana Leonidivna,
DSc(Law), Professor,
Head of the Department of International and European Law
V.N. KarazinKharkivNational University Kharkiv,
4, Svobody square, Kharkiv, 61022, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-16

CONSTITUTIONAL AND LEGAL GUARANTEES OF MEDIA FREEDOM AND JOURNALISTIC ACTIVITY IN THE DIGITAL ENVIRONMENT: THE PRACTICE OF THE ECTHR IN THE CONTEXT OF CYBER OFFENCES

Slinko T. M., Slinko K. M.

INTRODUCTION

Freedom of expression and media freedom constitute fundamental values of modern constitutionalism and an essential prerequisite for the functioning of a democratic society governed by the rule of law. The possibility to freely disseminate information, express opinions, and participate in public debate ensures transparency in the activities of public authorities, facilitates public oversight, and promotes the development of civil society. For this reason, guarantees of freedom of speech and journalistic activity occupy a central place in the constitutional systems of democratic states.

In the contemporary era, characterized by rapid technological development and the digitalization of social relations, the traditional understanding of media activity and its legal regulation is undergoing significant transformation. Information and communication technologies, online media platforms, and social networks have greatly expanded opportunities for the dissemination of information and the exercise of freedom of expression. At the same time, the digital environment has created new legal challenges related to cyber offences, the spread of unlawful content, digital surveillance, and potential interference with journalistic activity.

These developments require a reconsideration of existing constitutional and legal mechanisms aimed at ensuring the protection of media freedom and the professional activities of journalists. It becomes increasingly important to develop legal guarantees capable of maintaining an appropriate balance between freedom of expression and other legitimate interests, including national security, public order, the protection of reputation and privacy, and the prevention of crime. In this regard, international legal standards and judicial practice play a particularly important role in shaping modern approaches to the protection of freedom of speech.

A key role in the formation of contemporary standards for the protection of freedom of expression is played by the European Court of Human Rights. Through the interpretation of Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, the Court has developed a comprehensive system of legal principles that determine the permissible limits of state interference in the sphere of freedom of expression and media activity. According to the Court's established approach, any restriction on freedom of expression must be prescribed by law, pursue a legitimate aim, and be necessary in a democratic society.

The relevance of these issues has increased significantly in the context of digital transformation. Modern journalists actively use electronic communication tools, digital platforms, and cloud technologies for collecting, processing, and

disseminating information. At the same time, investigations of cyber offences often involve access to electronic devices, digital accounts, and information systems, which may potentially lead to the disclosure of journalistic sources or interference with professional activities. In such circumstances, the need to ensure a proper balance between the interests of criminal justice and guarantees of freedom of expression becomes particularly important.

For Ukraine, the issue of ensuring effective constitutional and legal guarantees of media freedom has acquired special significance in the context of digital transformation and ongoing armed aggression. The Constitution of Ukraine enshrines freedom of thought and speech, the right to information, and the prohibition of censorship as fundamental elements of the democratic constitutional order. At the same time, the national legal system continues to develop mechanisms aimed at protecting journalists and ensuring the functioning of independent media, particularly under conditions of wartime and information threats.

In this context, the study of constitutional and legal guarantees of media freedom requires a comprehensive analysis of both national legislation and the practice of international judicial institutions. The jurisprudence of the European Court of Human Rights plays a particularly important role in shaping modern legal standards for the protection of freedom of expression and journalistic activity.

The purpose of this article is to analyze the constitutional and legal guarantees of media freedom and journalistic activity in the digital environment, as well as to examine the case law of the European Court of Human Rights concerning freedom of expression in the context of cyber offences. Particular attention is devoted to the role of ECtHR jurisprudence in establishing modern legal standards for the protection of journalists and the media in the digital era.

1. Media Freedom as a Fundamental Value of Constitutionalism in the Conditions of the Digital Society

The digital transformation of social relations necessitates a reconsideration of the content and mechanisms for the implementation of constitutional and legal guarantees of media freedom and journalistic activity. In this context, particular importance is attached to the analysis of the practice of the European Court of Human Rights as an institution that establishes binding standards for member states regarding the interpretation and application of the right to freedom of expression in the digital environment, particularly in the context of the growing number of cyber offences.

The axiological foundation of these guarantees consists of the fundamental values enshrined within the European Union, namely: respect for human dignity, freedom, democracy, equality, solidarity, the rule of law, and the primacy of human rights, including the protection of minority rights. These principles reflect the content of the so-called European standards, which are based on the recognition of the universality, indivisibility, and interdependence of human rights and fundamental freedoms. Their implementation presupposes the promotion of pluralism, non-discrimination, tolerance, justice, and gender equality as essential conditions for the functioning of a democratic society.

Freedom of expression, proclaimed in the Universal Declaration of Human Rights, is one of the key prerequisites for democratic governance, the development of public dialogue, and the exercise of journalistic activity. In the digital era, its content has significantly expanded, as information and communication technologies create new channels for the dissemination of information, transform the role of the media, and change the nature of interaction between the state, society, and journalists. At the same time, the digital environment generates new challenges related to cyber offences, the abuse of freedom of speech, the dissemination of unlawful content, and interference with privacy.

Accordingly, the study of the constitutional and legal guarantees of media freedom and journalistic activity requires a comprehensive analysis of the case law of the European Court of Human Rights concerning the determination of the permissible limits of restrictions on freedom of expression, the criteria of proportionality of state interference, and the standards for the protection of journalists in the digital space. Such an approach makes it possible not only to outline the current state of legal regulation but also to determine the directions for its further development in the context of intensive digitalization and the growing number of cyber threats.

Continuing the analysis of the constitutional and legal guarantees of media freedom and journalistic activity in the digital environment, it is appropriate to turn to the fundamental principles of constitutionalism as the ideological and legal foundation of freedom of expression.

One of the key conditions of constitutionalism is freedom, which, according to the apt statement of Vsevolod Rechytskyi, acts as a genetic precondition for the diversified search for values and the general investment of human abilities and talents[1]. It follows that the right to freedom of expression, in its modern understanding, constitutes not only the foundation of a democratic system but also a necessary precondition for the realization of other constitutional rights and freedoms.

Within the framework of organic constitutionalism, freedom precedes democracy, since the latter cannot function without freedom of speech, the open exchange of opinions, the dissemination of ideas, public discussion, and the guaranteed right to receive information. The absence of an adequate level of protection of freedom of expression makes the full realization of such rights as freedom of peaceful assembly, freedom of conscience and religion, freedom of association, freedom of creativity, as well as electoral rights impossible.

Thus, the above provisions confirm the decisive importance of the right to freedom of expression within the system of constitutional rights and freedoms, its priority character, and its system-forming role in ensuring the functioning of a democratic state governed by the rule of law. Therefore, this right occupies a leading place among other rights and freedoms, which should be recognized as an indisputable general proposition[2].

For a more comprehensive understanding of the importance of the right to freedom of expression, it is appropriate to note that in the modern world there are two

[1] Речицький В. В. Конституційне АБВ. Харків: ТОВ «Видавництво «Права людини», 2016. 408 с.

[2] Frowein J. A. Freedom of Expression under the European Convention on Human Rights. Strasbourg: Monitor/Inf., 1997. 42 p.

typological approaches to defining constitutional design: the *American* approach, whose priorities are traditionally associated with the categories of freedom and the market and which from the very beginning has been oriented toward rapid and effective progress; and the *European* approach, which prioritizes democracy and freedom, the latter of which may be subject to certain limitations. A characteristic feature of the European model of constitutionalism is the recognition and effective guarantee of fundamental human rights and freedoms. These rights serve as the basis for establishing clear limits on the functioning of the state and the activities of its bodies, as well as for introducing constitutional and legal restrictions on state power. In this context, human rights are not a declarative category but rather a normative criterion for the legitimacy of public authority and the limits of its discretion.

The idea of the priority of individual freedom within the system of constitutional values was thoroughly developed in the works of John Stuart Mill. In particular, he emphasized that a society cannot be considered free, regardless of the form of government, if it does not ensure freedom of thought and speech, freedom of lifestyle, and freedom of association. A society can be regarded as free only when such freedoms are fully guaranteed and equally available to all its members. At the same time, the exercise of individual freedom is limited by the necessity of preventing violations of the rights and legitimate interests of others. Only such freedom, as he noted, «deserves the name of freedom when we are absolutely free to pursue what we consider our own good in our own way–provided that we do not attempt to deprive others of theirs or impede their efforts to obtain it»[3].

The aforementioned approach laid the foundations for the development of the doctrine concerning the limits of the exercise of rights and freedoms in modern constitutional law.

In further developing this concept, it should be noted that an organic constitution is regarded as a guarantor of individual freedom and the institutional autonomy of civil society. Such an understanding of the Basic Law is typical of the modern doctrine of constitutionalism, which in the Western legal tradition is closely connected with the principle of the rule of law. Freedom, in the political and legal sense, possesses the character of the highest normative value; therefore, its guarantee constitutes one of the key functions of the constitution as an act of the highest legal force that reflects and protects the interests of civil society.

In this regard, V. Rechytskyi emphasizes that the organic constitution and freedom have been conceptually interconnected since the moment of their historical formation. By guaranteeing freedom, the constitution ensures a state of autonomy of the individual and of society as a whole from the state[4], while establishing legal mechanisms for restraining public authority.

In the view of Friedrich August von Hayek, there is only one alternative for a constitution: either a free parliament or a free people. Therefore, the constitution protects the freedom of the individual and of civil society as a whole, including protection from the arbitrariness of a parliamentary majority[5]. In this context, the

[3] Міль Дж. Про свободу : есе. Київ : Вид-во Соломії Павличко «Основи», 2001. 463 с.

[4] Речицкий В.В. Конституционализм. Украинский опыт. Харьков. Фолио, 1998. С. 57.

[5] Hayek F. Law, Legislation and Liberti. Vol. 3. Chicago: University of Chicago Press, 1979. P. 111.

constitution is intended not only to organize the system of state power but also to guarantee the freedom of the individual and of civil society, including by preventing the arbitrariness of a parliamentary majority. Thus, the constitution functions as an instrument for the institutional limitation of power and as a legal guarantee for preserving the sphere of individual freedom.

Particular attention should be paid to the conceptually balanced formulation of the fundamental principles of freedom of expression and belief proposed by one of the leading representatives of the English legal tradition of the protection of free speech, Thomas Erskine. In his view, «the key legal guarantee lies in the fact that every person has the right freely to publish everything that his or her mind or conscience, even with the possibility of error, perceives as truth»[6].

Within this approach, freedom of speech is regarded not only as an individual right but also as a necessary condition for the functioning of a state governed by the rule of law and for the development of public discourse.

Continuing this line of reasoning, it should be noted that modern constitutions provide for various models of the normative entrenchment of freedom and the guarantees for its protection. However, the principal guarantees traditionally include: the proclamation of freedom as a goal of the state or as the highest social value; the recognition of freedom as an independent legal category; the establishment of a system of subjective rights and freedoms of the individual and the citizen; the revision or rejection of excessively «paternalistic» socio-economic constructs; the affirmation of freedom as a principle of the constitutional order; as well as the introduction of effective procedural mechanisms for the protection and safeguarding of freedom[7]. The combination of these elements forms an institutional framework aimed at ensuring the autonomy of the individual in relations with the state.

In this context, the concept of John Rawls is particularly illustrative. According to his approach, civil society cannot be reduced to a political association in the narrow sense. Rather, it appears as an open institutional space intended to create the broadest possible opportunities for the realization of primarily individual life projects and strategies[8]. This approach corresponds to the modern understanding of the constitution as a legal instrument that ensures a balance between public interests and individual autonomy.

Therefore, the normative enshrinement of freedom in the constitution as a goal of the state and society is consistent with the classical requirement of constitutionalism: the subject of constitutional protection should be those values that are universally significant and just for all citizens, regardless of their social status, role, or position in society. Such an approach ensures the legitimacy of the constitutional order and its compliance with the principle of the rule of law.

As already emphasized, it is precisely the system of guarantees that serves as the decisive criterion of the state's genuine attitude toward freedom of thought and speech, since it ensures the possibility of their unhindered exercise, proper protection

[6] Levy L. Freedom of Spreech and Press in Early American History: Legacy or Suppression. New York, 1963. P. 256.

[7] Речицкий В.В. Политический предмет конституции. Київ: Дух і літера, 2012. С. 349–350.

[8] Rawls J. Political Liberalism. New York: Columbia University Press, 1993. P. 42.

against potential unlawful encroachments, and effective safeguards against illegal restrictions. In this respect, guarantees function not as an auxiliary but as a structural element of the mechanism for ensuring constitutional rights.

At the same time, the declarative recognition of the right to freedom of thought and speech is not sufficient. It is necessary to establish appropriate institutional, normative, and procedural conditions, as well as to define effective legal means through which freedom of speech and information acquires real substance. Such a state of affairs is possible only in a democratic society based on the principles of the rule of law, political pluralism, and respect for human rights

Therefore, in the absence of adequate guarantees proclaimed in the Constitution of Ukraine and other normative legal acts, rights and freedoms risk remaining «an empty sound»[9], formal prescriptions devoid of practical effectiveness». For this reason, the prevailing approach in legal doctrine considers guarantees as a comprehensive system of means, methods, and legal norms aimed at ensuring the real implementation, protection, and safeguarding of the rights and freedoms of the individual and the citizen[10]. This interpretation organically fits into the general concept of constitutionalism, according to which the effectiveness of rights is determined not only by their normative enshrinement but also by the existence of an effective mechanism for their implementation.

According to representatives of constitutional legal thought, the effectiveness of the system of guarantees of rights and freedoms is determined by a set of interrelated factors. The key among them are: a) the existence of a Basic Law whose effect cannot be arbitrarily suspended; b) the recognition of state power as deriving from the power of the people and the Constitution; c) the constitutional enshrinement of the fundamental rights and freedoms of the individual and the citizen, as well as the means and conditions for their implementation; d) the existence of an independent judiciary; e) the possibility of protecting one's rights through the Ukrainian Parliament Commissioner for Human Rights and through international human rights organizations[11]. The totality of these elements forms an institutional mechanism without which constitutional provisions do not acquire proper practical effectiveness.

For the purpose of a comprehensive analysis of the guarantees of freedom of speech, it is advisable to turn to the comparative legal dimension. The provision of such guarantees is a characteristic feature of both classical and modern constitutions, including the Constitution of the United States (1787), the Federal Constitution of Switzerland (1874, 1999), the Constitution of Spain (1978), the Constitution of Japan (1947), the Constitution of Macedonia (1991), the Constitution of Bulgaria (1991), the Constitution of Slovakia (1992), the Constitution of France (1946), and the Constitution of Poland (1997). In the constitutions of a number of post-totalitarian states, freedom is directly proclaimed as the highest social value, which indicates an attempt to normatively reconsider the role of the individual in relations with the state.

---

[9] Пашинський В. М. Правові гарантії конституційних прав і свобод військовослужбовців. *Право України*. 2006. № 5. С. 61–65.

[10] Сліньо Т. М. Конституційно-правові гарантії свободи слова. *Наше право*. 2014. № 9. С.12.

[11] Колодій А. М., Олійник А. Ю. Права людини і громадянина в Україні : навч. посібник. Київ: Юрінком Інтер, 2004. С. 223.

Moreover, in the constitutions of several post-totalitarian states, freedom is directly proclaimed as the highest social value, demonstrating an aspiration toward a normative rethinking of the role of the individual in relations with the state. In particular, such provisions are contained in the Basic Laws of Croatia (1990), Uzbekistan (1992), Turkmenistan (1992), Kazakhstan (1993), Kyrgyzstan (1993), and Brazil (1988), among others.

However, the guarantees of freedom of speech in the above-mentioned constitutional acts lag behind the level of protection of civil liberty, for example, in the United States. This is largely due to the historical and doctrinal features of American constitutionalism, within which freedom of speech has traditionally been regarded as one of the fundamental values of the democratic system. The normative basis for this approach is the First Amendment to the Constitution of the United States, according to which Congress is prohibited from adopting laws that restrict freedom of speech, the press, conscience, or the right to petition.

Thus, the American constitutional model proceeds from the principle of minimal state interference in the sphere of the individual's exercise of the right to freedom of expression. This position serves as a benchmark for assessing the effectiveness of national mechanisms for guaranteeing freedom of speech and emphasizes the importance of real, rather than merely declarative, constitutional guarantees in the system of modern constitutionalism.

Freedom of expression and freedom of the media are fundamental values of the constitutional order of Ukraine and a necessary prerequisite for the functioning of a democratic society. In the digital environment, these freedoms acquire new forms of realization while simultaneously facing new risks related to cyber threats, mass data processing, online surveillance, and the use of digital evidence in criminal proceedings. The adaptation of constitutional and legal guarantees to these challenges requires a systematic analysis of the national legislation of Ukraine and the case law of the European Court of Human Rights (ECtHR).

The conducted analysis provides grounds to assert that freedom of expression and freedom of the media belong to the fundamental values of modern constitutionalism and constitute a necessary prerequisite for the functioning of a democratic rule-of-law state. Within the system of constitutional rights and freedoms, they perform a system-forming role, as they ensure the possibility of an open public dialogue, public oversight of the activities of state authorities, and the exercise of other political and civil rights of the individual.

In the theoretical and legal dimension, freedom of speech acts as one of the basic categories of the constitutional order, closely connected with the principles of the rule of law, political pluralism, and the autonomy of civil society. As demonstrated by the development of the doctrine of constitutionalism, beginning with the classical ideas of John Stuart Mill, Friedrich August von Hayek, and other representatives of the liberal legal tradition, freedom of expression is regarded not only as an individual right but also as a necessary condition for the functioning of democratic institutions and a safeguard against the arbitrariness of state power.

Under contemporary conditions of the digitalization of social relations, the content and mechanisms for the implementation of media freedom are undergoing significant transformations. Information and communication technologies create new

opportunities for the dissemination of information and the development of public debate, while simultaneously generating new challenges related to cyber threats, the spread of unlawful content, digital surveillance, and the use of electronic data in criminal proceedings. In this regard, the issue of ensuring an effective balance between guarantees of freedom of speech and the need to protect other socially significant interests, particularly national security, public order, and the rights of others, acquires special importance.

An analysis of constitutional and legal approaches in different legal systems demonstrates the existence of various models of normative protection of freedom of speech. The American model of constitutionalism has traditionally been characterized by a high level of protection of freedom of expression and minimal state interference in the sphere of information relations. In contrast, the European model proceeds from the necessity of ensuring a balance between freedom of speech and other constitutional values, which allows for its restriction provided that the principles of legality, legitimate aim, and proportionality are respected.

In this context, the case law of the European Court of Human Rights plays a particularly important role, as it forms modern European standards for the interpretation and application of the right to freedom of expression enshrined in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The Court's judgments define the criteria for the admissibility of state interference in media activities, establish requirements for the proportionality of restrictions on freedom of speech, and emphasize the special role of journalists as «public watchdogs» in a democratic society.

Thus, media freedom in the modern digital society acts not only as an individual right but also as an institutional guarantee of the functioning of the democratic constitutional order. Its effective protection requires a comprehensive combination of constitutional, legislative, and institutional mechanisms of protection, as well as consideration of the standards developed in the case law of the European Court of Human Rights. These standards constitute the methodological basis for further research into the constitutional and legal guarantees of media freedom and journalistic activity in the conditions of digitalization and the counteraction to cyber offenses, which determines the need to move to the analysis of the relevant mechanisms for their implementation within the legal system of Ukraine.

2. Constitutional and Legal Foundations for Guaranteeing Freedom of Speech and Media Activity in Ukraine

The provision proclaimed in Article 15 of the Constitution of Ukraine,[12] according to which social life in Ukraine is based on the principles of political and ideological diversity, belongs to the fundamental principles of the constitutional order of the state. This principle implies the state's orientation toward democratic values, the recognition of the priority of human and civil rights and freedoms, and establishes the normative prerequisites for the functioning of civil society. In this

[12] Конституція України: Закон України від 28 червня 1996р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

context, adherence to the principles of political and ideological pluralism serves as one of the key guarantees of freedom of thought and speech.

Moreover, the importance and significance of this provision have received official interpretation in the practice of the Constitutional Court of Ukraine. In particular, in Decision No. 18-rp/2001 of December 13, 2001 (the case on youth organizations), the Court formulated the legal position according to which «the principle of diversity of social life is fundamental in determining the foundations for the implementation of this constitutional right and the establishment of civil society institutions, a component of which includes various associations of citizens representing certain ideological and other views, as well as the interests of different social groups and individuals»[13]. This approach emphasizes the inseparable connection between freedom of association, freedom of expression, and the democratic character of the state.

In a broader sense, the global legal community proceeds from the premise that freedom of thought and speech, as well as the ability to freely express beliefs and conduct public discussions on issues of public importance, constitute a necessary prerequisite for the existence of a democratic and tolerant society. This concerns not only an individual right but also an institutional form of democracy itself, under which no position may be deprived of the right to be expressed and publicly discussed within the limits of the law. Under the modern conditions of the development of the information society, these rights acquire particular significance, since it is through mechanisms of information dissemination that public consciousness is formed, citizens' political rights are exercised, and transparency in the activities of public authorities is ensured.

Ideological diversity presupposes the free coexistence within society of various political and other worldview concepts, doctrines, and schools, as well as the possibility of their dissemination through mass media and their public defense without unlawful interference by the state. At the same time, the principle of ideological pluralism implies the prohibition of the establishment by the state of a mandatory ideology, that is, the inadmissibility of the normative consolidation of a system of universally binding views or beliefs that citizens would be obliged to adhere to under the threat of legal liability.

Thus, freedom of thought, speech, and information ensures the formation within society of an environment of ideological competition and diversity of information sources, which corresponds to Ukraine's democratic choice, its commitment to the principles of the rule of law, the republican form of government, and the affirmation of human rights and freedoms as the highest social value.

The enshrinement in the Constitution of Ukraine of the principle of political and ideological diversity essentially indicates that «Ukrainian democracy will be a constitutional weapon» capable of protecting itself from encroachments that occur in societies seeking to overcome their totalitarian past. This is evidenced, in particular, by the wording of the article in the first section of the Constitution devoted to the

[13] Рішення Конституційного Суду України від 13.12.2001 № 18-рп/2001. *Офіційний вісник України* від 04.01.2002. 2001. № 51. С. 466. Ст. 2310. URL: http://zakon0.rada.gov.ua/laws/show/v018p710-01

principle of a multiparty system, which remained almost unchanged at the stage of its final adoption[14]. Ideological diversity is a natural consequence of the exercise of a complex of constitutional rights and freedoms of the individual and the citizen, in particular freedom of thought and speech, freedom of conscience (religion), and other fundamental rights. Its normative consolidation reflects the nature of a democratic state in which diversity of worldviews is recognized as an objective social reality and is protected by law.

The ideological orientation of the Ukrainian state, which bears responsibility to the individual for its activities, also follows from the provisions of Article 3 of the Constitution of Ukraine, according to which the human being, his or her life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value. In this context, the principle of ideological pluralism enshrined in Chapter I of the Basic Law acts as an institutional guarantee preventing the persecution of individuals for their beliefs, which is of particular importance in light of the historical experience of the totalitarian past. These provisions should be interpreted systematically in conjunction with Articles 34, 35, and 54 of the Constitution of Ukraine, which guarantee freedom of expression, freedom of worldview and religion, and freedom of literary, artistic, scientific, and technical creativity.

Developing these principles, the Constitution of Ukraine, in Article 34, establishes the right of everyone to freedom of thought and speech, as well as to freely collect, store, use, and disseminate information orally, in writing, or in any other manner of their choice. This provision has direct effect and applies to all forms of media, including traditional mass media, online publications, social platforms, and other digital services, which corresponds to contemporary trends in the development of the information society.

At the same time, the constitutional model of guaranteeing freedom of speech presupposes its balancing with other fundamental rights. In particular, Article 32 of the Constitution of Ukraine guarantees the right to non-interference in personal and family life, while Article 31 ensures the secrecy of correspondence, telephone conversations, telegraph, and other communications. For journalistic activity–especially in the digital environment–these provisions are of fundamental importance, as they define the limits of permissible state interference in the sphere of private communications and ensure an appropriate level of protection of information sources.

Thus, the constitutional enshrinement of ideological diversity and the rights and freedoms associated with it forms a comprehensive system of guarantees of freedom of thought and speech that corresponds to the general principles of democratic constitutionalism and the rule of law. Within this system, freedom of expression is not regarded as absolute but as one that may be subject to restrictions exclusively under the conditions defined by the Constitution.

In Ukraine, as a European state, the issue of restrictions on freedom of speech is regulated in accordance with the generally recognized European legal paradigm formed under the influence of the Convention for the Protection of Human Rights

[14] Барабаш Ю.Г. Демократія як конституційна ідеологія: український варіант. Демократичні засади організації і функціонування вищих органів державної влади України : монографія. Харків : Право, 2013. С. 14.

and Fundamental Freedoms and the International Covenant on Civil and Political Rights. This approach provides that freedom of expression is not absolute; however, its restrictions are possible only on the basis of law and in compliance with the principles of legitimate aim, necessity, and proportionality.

According to Part 3 of Article 34 of the Constitution of Ukraine, the freedom to collect, store, use, and disseminate information may be restricted by law in the interests of national security, territorial integrity, or public order, for the purpose of preventing disturbances or crimes, protecting public health, safeguarding the reputation or rights of others, preventing the disclosure of confidential information, as well as maintaining the authority and impartiality of justice. This list of grounds is exhaustive and reproduces the standards developed within the European human rights tradition. In the digital environment, this means that state measures aimed at combating cyber offenses or ensuring information security cannot nullify the very essence of media freedom or create excessive obstacles to the exercise of the right to freedom of expression.

At the same time, according to Part 2 of Article 64 of the Constitution of Ukraine, certain restrictions on rights and freedoms may be introduced under conditions of martial law or a state of emergency, with an indication of the duration of their validity. In particular, the Constitution of Ukraine of 1996, drafted according to Eastern European constitutional models, contains thirteen, and with regard to martial law and a state of emergency fifteen, limitations on the fundamental freedom of speech. However, even in such circumstances, state interference must comply with constitutional criteria of legality and may not lead to the abolition of the very essence of the right to freedom of expression.

Important legal positions concerning the possibility of restricting this right were formulated by the Constitutional Court of Ukraine in its Decision of April 10, 2003 No. 8-rp/2003 (the case on dissemination of information) and in the Decision of January 20, 2012 No. 2-rp/2012, adopted in the case upon the constitutional petition of the Zhashkiv District Council of Cherkasy Region regarding the official interpretation of the provisions of Parts 1 and 2 of Article 32 and Parts 2 and 3 of Article 34 of the Constitution of Ukraine, as well as in the Decision of December 21, 2021 No. 3-r/2021.

An analysis of the provisions of the Constitution of Ukraine and the current legislation in the field of information relations provides grounds to assert that the established restrictions must comply with a number of fundamental requirements. First, they must be proportionate to the threats to the rights and freedoms protected by law and should not extend to other rights the exercise of which is not directly related to the relevant restrictions. Second, such restrictions must be consistent with the democratic principles of the functioning of the state. Third, they must be formulated with sufficient clarity and foreseeability, which ensures the possibility of properly understanding their content and predicting legal consequences. Fourth, the relevant provisions must not contradict Ukraine’s international obligations.

At the same time, in the legal systems of post-totalitarian states there is sometimes a tendency to use excessively broad or evaluative concepts, such as «interests of society», «public necessity», «interests of national security», «information security», or «information sovereignty» as grounds for indirect

restrictions on freedom of expression. In the absence of clear legal criteria, such categories may be used for excessive state interference in the sphere of intellectual and creative activity of individuals, which potentially creates risks of narrowing the space of freedom of thought and speech.

Thus, at the present stage of development Ukraine recognizes as an effective mechanism for ensuring freedom of speech not only its proclamation but also a clear and normatively defined delineation of the possible limits of its exercise. Such a model, based on the principle of legal certainty and judicial control, corresponds to the standards of democratic constitutionalism and ensures a balance between individual freedom and public interests.

At the same time, constitutional provisions correspond with the norms of international law and generally recognized standards in the field of human rights. In particular, Article 19 of the Universal Declaration of Human Rights enshrines the right of every person to freedom of opinion and expression, which includes the freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers. Similar guarantees are provided in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, which establishes standards for permissible restrictions on freedom of expression and forms the basis for their interpretation at the European level.

In addition, the relevant provisions are consistent with the norms of the International Covenant on Civil and Political Rights, as well as with the obligations arising from the Final Act of the Conference on Security and Cooperation in Europe. An important stage in the further institutionalization of freedom of speech standards was the adoption in 2000 of the Charter of Fundamental Rights of the European Union, which, in Article 11, guarantees freedom of expression and information, and in Article 13 guarantees freedom of the arts and sciences.

Thus, the constitutional foundations of freedom of speech in Ukraine were formed, taking into account international human rights standards. Ukraine, as a state oriented toward European democratic values, has incorporated into its legislation the approaches developed in international legal practice. In particular, the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as the International Covenant on Civil and Political Rights, have played an important role in shaping national standards of freedom of expression. These international legal instruments have defined the basic approaches to understanding the content of freedom of speech, the limits of its exercise, and permissible restrictions.

Therefore, the national model of guaranteeing freedom of speech in Ukraine constitutes a component of the broader European and universal system of human rights protection. Its normative structure demonstrates the integration of the principles of international law into the domestic legal order and confirms the orientation of Ukrainian constitutionalism toward ensuring the real, rather than merely declarative, nature of freedom of expression.

An important component of the guarantee of freedom of speech is the law-making activity of the European Court of Human Rights, the main international supervisory body in this field, and a widely recognized «creator» of standards of

judicial protection. The Court's case law (The Sunday Times v. the United Kingdom (1979), Lingens v. Austria (1986), Goodwin v. the United Kingdom (1996), Oberschlick v. Austria (1997), Fressoz and Roire v. France (1999), Romain and Schmit v. Luxembourg (2003), Busuioc v. Moldova (2004), Ukrainian Media Group v. Ukraine (2005), Gazeta Ukraina-Tsentr v. Ukraine (2010) and others) demonstrates its consistency in protecting freedom of speech and freedom of expression, as well as the right to freely receive and disseminate information. In addition, the ECtHR has established strict criteria for assessing the justification of restrictions on freedom of expression, as a result of which freedom of speech has obtained a clear priority over its limitations. In this context, it should be emphasized that in Ukraine, in accordance with the Law «On the Execution of Judgments and the Application of the Case Law of the European Court of Human Rights» of February 23, 2006 No. 3477-IV, the state is obliged to execute judgments of the European Court of Human Rights in cases against Ukraine; to eliminate the causes of violations of the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols by Ukraine; and to introduce European human rights standards into Ukrainian judicial and administrative practice.

The implementation of constitutional guarantees of freedom of speech and freedom of information in Ukraine is ensured not only by the provisions of the Basic Law but also by a developed system of special legislation regulating the sphere of media and information relations.

The modern Ukrainian media space operates based on several regulatory legal acts, among which an important place is occupied by the Law of Ukraine «On Information», the Law of Ukraine «On Media», as well as the Law of Ukraine «On Television and Radio Broadcasting» (in the part of provisions that continue to be applied). In addition, the relevant legal relations are regulated by the norms of civil and criminal legislation, which determine the grounds for legal liability for violations of information rights and abuses of freedom of speech.

The constitutional guarantees of freedom of speech and media activity in Ukraine have been further developed in a number of special legislative acts. In particular, relevant provisions are enshrined in the Law of Ukraine «On Media», the Law of Ukraine «On Electronic Communications», the Law of Ukraine «On Ensuring the Functioning of the Ukrainian Language as the State Language», the Law of Ukraine «On Cinematography», the Law of Ukraine «On Advertising», the Law of Ukraine «On the Public Media of Ukraine», the Law of Ukraine «On the System of Foreign Broadcasting of Ukraine», as well as the Law of Ukraine «On State Support for Media, Guarantees of Professional Activity and Social Protection of Journalists».

One of the key guarantees of freedom of speech in the national legal order is the prohibition of censorship, which is enshrined in Article 15 of the Constitution of Ukraine and further specified in Article 24 of the Law of Ukraine «On Information», as well as in the provisions of the Law of Ukraine «On the System of Foreign Broadcasting of Ukraine». The legislation also establishes the fundamental principles of information relations, including: the guaranteed right to information; openness and accessibility of information; freedom of exchange of information; reliability and completeness of information; freedom of expression of views and beliefs; legality

in obtaining, using, disseminating, storing, and protecting information; as well as the protection of individuals from unlawful interference in their personal and family life.

Particular importance is attached to the legislative provisions concerning the legal status of statements in the sphere of public communication. In particular, according to Article 30 of the Law of Ukraine «On Information», a person cannot be held liable for expressing value judgments that are not subject to refutation or proof of their truthfulness. This approach corresponds to European standards of freedom of expression and is aimed at ensuring appropriate conditions for the development of public debate in a democratic society.

An important place in the system of modern media legislation of Ukraine is occupied by the Law of Ukraine «On Media» (2022), which significantly updated the legal regulation of media activities in accordance with European standards. This normative legal act enshrines the fundamental principles of freedom of activity of entities in the media sphere, the prohibition of censorship, as well as guarantees of editorial independence that apply both to traditional mass media and to online media. At the same time, the law also provides for certain mechanisms of state regulation of the media sphere, the application of which must be carried out taking into account the constitutional guarantees of freedom of speech and the standards developed in the case law of the European Court of Human Rights, which defines the criteria for permissible state interference in the sphere of freedom of expression.

All provisions of the special national legislation aimed at ensuring freedom of speech and the functioning of the media are based on the constitutionally enshrined right to freedom of thought and speech guaranteed by the Constitution of Ukraine. At the same time, an important element of the system of legal protection of media freedom is the establishment of appropriate guarantees for the professional activities of journalists, particularly in conditions of armed conflict and martial law, when the risks for the exercise of journalistic activity significantly increase.

In this context, the provisions of Article 25 of the Law of Ukraine «On Information» are of key importance, as they define the main guarantees of the activities of mass media and journalists. In particular, a journalist has the right, after presenting a document confirming his or her professional affiliation, to collect information in areas of natural disasters, catastrophes, at sites of accidents, mass disturbances, and military actions, except in cases provided for by law[15]. In addition, the legislation guarantees journalists the right to freely choose the forms of recording information using the necessary technical means, the right to disseminate information under their own authorship or under a pseudonym, as well as the right not to disclose sources of information or information that may contribute to their identification.

The Law of Ukraine «On State Support for Media, Guarantees of Professional Activity and Social Protection of Journalists» is also of significant importance for ensuring proper conditions for the professional activities of journalists. It provides a system of social and legal guarantees for representatives of the media sphere and members of their families in the event of harm to life or health while performing professional duties. Such guarantees include, in particular, the right to proper

[15] Закон України від 02 жовтня 1992 р. № 2657-XII. *База даних «Законодавство України»* / Верховна Рада України.URL: https://zakon.rada.gov.ua/go/2657-12

working conditions, benefits, and compensation for work in difficult or hazardous conditions, medical examinations, social insurance, as well as the conduct of a comprehensive investigation into accidents, death, or harm caused to a journalist's health during the performance of professional duties.

In particular, the law establishes the right to appropriate compensation, financial assistance, and funeral assistance for the family members of journalists who died while performing their professional duties. It also provides for the payment of one-time financial assistance: for family members of a deceased journalist, in the amount of 100 subsistence minimums established by law for able-bodied persons at the time of payment; and for a journalist in the event of injury (concussion, trauma, or mutilation) sustained during the performance of professional duties – in the amount of 50 subsistence minimums[16].

The peculiarities of the legal status of journalists during an armed conflict are also reflected in departmental regulatory legal acts. In particular, according to the Order of the Ministry of Defence of Ukraine «On Approval of the Instruction on the Procedure for the Implementation of the Norms of International Humanitarian Law in the Armed Forces of Ukraine», journalists have the status of civilians, which corresponds to the provisions of international humanitarian law. This approach confirms that journalists enjoy the full range of guarantees provided by national legislation for the civilian population, including relevant social payments and compensation.

Taking into account the increased risks faced by media representatives while covering military events, the legislator has introduced additional legal mechanisms for their protection. Thus, Law of Ukraine No. 7367 «On Providing Additional Protection Guarantees for Journalists Working in Areas of Military (Combat) Operations» was adopted, which establishes the obligation of media organizations to provide journalists with personal protective equipment against firearm injuries and shrapnel wounds, as well as medical first-aid kits[17]. In addition, the law establishes the requirement for mandatory insurance of journalists at the employer's expense in the event of injury or death while performing professional duties in areas of hostilities or in temporarily occupied territories.

Thus, Detector Media conducted a survey of television channels and found that some of them already insure their employees, although there is still no complete clarity regarding the insurance mechanisms as well as the practical implementation of the law. Nevertheless, in May, an International Journalists' Insurance Fund was established in Ukraine, to which media professionals who travel to combat zones and do not have grounds for insurance at the employer's expense may apply.

An important political and legal signal regarding the significance of freedom of speech during wartime also became the Resolution of the Verkhovna Rada of

[16] Закон України «Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста» від 23.09.1997 № 540/97-ВР URL: https://zakon.rada.gov.ua/laws/show/540/97-вр#Text

[17] Про внесення змін до деяких законів України щодо надання додаткових гарантій захисту працівникам засобів масової інформації, які працюють у районах ведення воєнних (бойових) дій та/або на тимчасово окупованих територіях України. URL : https://document.vobu.ua/doc/14117

Ukraine No. 7266 «On the Statement of the Verkhovna Rada of Ukraine on the Value of Freedom of Speech, Guarantees of the Activities of Journalists and Mass Media during the Period of Martial Law». This document emphasizes that one of the key tasks of the state is to ensure the constitutional guarantees of freedom of speech, as well as the free receipt, collection, and dissemination of information, taking into account the restrictions associated with the introduction of martial law.

At the same time, the document stresses the inadmissibility of unlawful interference in the activities of journalists and mass media and the necessity of an appropriate response from law enforcement authorities to any offenses committed against journalists. It is also stated that any cases of technical disconnection of pro-Ukrainian television channels from broadcasting must receive a decisive response from law enforcement agencies, with those responsible being brought to fair legal liability.

Under the conditions of martial law, the state will support honest journalists and independent mass media, which are a defining feature of any democratic society, as undoubtedly is the society of Ukraine. Furthermore, the resolution calls upon all state authorities, including law enforcement bodies, as well as local self-government bodies, to ensure the protection of the rights of journalists and mass media during martial law, to respond promptly to reports of violations of their rights, and to guarantee freedom of speech as one of the most important features of a democratic society[18].

To summarize, it should be emphasized that the work of journalists during wartime is difficult to overestimate. They operate in combat zones, constantly under tension, focused and attentive, since the risks to their life and health require the highest level of caution. All of this is done to deliver the most complete, truthful, and impartial information possible and to reproduce an accurate picture of events. The Ukrainian state understands and highly values the contribution of representatives of both Ukrainian and foreign media to the country's information policy. For this reason, it has provided additional guarantees and developed mechanisms for the protection and support of journalists working in wartime conditions.

Of particular importance for journalists in the digital environment are the provisions of the Criminal Procedure Code of Ukraine, which regulate access to items and documents (Articles 159–166), the conduct of searches (Article 234), temporary seizure of property, and the inspection of electronic information systems. The application of these norms in cases related to cyber offenses directly affects the realization of media freedom.

Thus, in modern conditions, the legal regulation of media activities in Ukraine combines constitutional guarantees of freedom of speech with a system of special legislative mechanisms aimed at ensuring the safety and proper conditions for the professional activities of journalists. These guarantees acquire particular relevance under martial law, when journalists perform an important public function by informing society about the course of military events, often working in extremely dangerous conditions. For this reason, the Ukrainian state is gradually forming additional legal instruments for the protection of journalists aimed at ensuring a

[18] Постанова Верховної Ради України «Про Заяву Верховної Ради України про цінність свободи слова, гарантії діяльності журналістів і засобів масової інформації під час дії воєнного стану» від 14.04.2022 № 2190-IX URL: https://zakon.rada.gov.ua/laws/show/2190-20#Text

balance between the requirements of national security and the need to preserve democratic standards of freedom of speech and media activity.

The conducted analysis of the constitutional and legal foundations for guaranteeing freedom of speech and media activity in Ukraine provides grounds to conclude that the relevant system of legal regulation has been formed on the basis of a combination of national constitutional principles and international legal standards in the field of human rights. The central place in this system is occupied by the provisions of the Constitution of Ukraine, which enshrine freedom of thought and speech, the right to information, the prohibition of censorship, and the principle of political and ideological pluralism as fundamental elements of the democratic constitutional order of the state.

In particular, the provisions of Article 15 of the Constitution of Ukraine, which proclaim the principle of political and ideological pluralism, create the normative preconditions for the existence of an open information space and the functioning of independent media. In systemic connection with the provisions of Articles 3, 32, 34, 35, and 54 of the Basic Law, this principle forms a comprehensive constitutional model for the protection of freedom of expression aimed at ensuring a balance between individual human rights, the interests of society, and the needs of the state. An important role in the development of the relevant constitutional doctrine is played by the practice of the Constitutional Court of Ukraine, which, in its decisions, has repeatedly emphasized the inseparable link between the principle of ideological pluralism, freedom of association, and freedom of expression as necessary conditions for the functioning of a democratic state.

The national system of guaranteeing freedom of speech is also largely integrated into the European legal space through the implementation of the standards of the Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights. The jurisprudence of the Court plays a key role in shaping the criteria for the admissibility of restrictions on freedom of expression, particularly through the application of the principles of legality, legitimate aim, and proportionality of state interference. These standards have become an important reference point for the development of Ukrainian legislation and judicial practice in the field of media law.

An essential element of the national model for ensuring media freedom is the system of special legislation, which specifies constitutional guarantees and determines the mechanisms for their practical implementation. The key normative acts in this sphere include the Law of Ukraine «On Media», the Law of Ukraine «On Information», the Law of Ukraine «On Electronic Communications», as well as a number of other laws regulating particular aspects of the functioning of the media sphere. These normative acts establish the legal foundations of the activities of media market participants, define guarantees of editorial independence, the rights of journalists, and mechanisms of liability for abuse of freedom of speech.

These legal guarantees acquire particular significance in the context of the digitalization of social relations and the armed aggression against Ukraine. The development of the digital information environment creates new opportunities for the realization of freedom of speech, while simultaneously generating new challenges associated with the spread of disinformation, cyber threats, and the need

to ensure the information security of the state. Under such conditions, the Ukrainian legislator is gradually forming legal mechanisms aimed at achieving a balance between guarantees of media freedom and the need to protect national security.

At the same time, law enforcement practice demonstrates that the effectiveness of constitutional guarantees of freedom of speech largely depends on the proper functioning of judicial control, the legal certainty of normative restrictions, and compliance with the standards developed in the case law of the European Court of Human Rights. It is precisely the combination of constitutional principles, international legal obligations, and modern media legislation that forms a comprehensive system for ensuring media freedom in Ukraine.

Thus, the constitutional and legal model for guaranteeing freedom of speech in Ukraine reflects the gradual integration of the state into the European legal space and the consolidation of democratic standards in the field of information relations. In the contemporary conditions of digital transformation and counteraction to cyber offenses, this model acquires particular relevance, since the effective combination of guarantees of media freedom, protection of journalistic activity, and ensuring information security determines the ability of a democratic state to maintain an open public discourse and ensure an appropriate level of protection of human rights.

3. Case Law of the European Court of Human Rights on Media Freedom and Journalistic Activity in the Digital Environment

An important component of the system of guarantees of freedom of speech and media activity in a modern democratic society is the case law of the European Court of Human Rights, which plays a key role in shaping international standards for the protection of freedom of expression. The Court acts as an authoritative interpreter of the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms, primarily its Article 10, which guarantees everyone the right to freedom of expression, including the freedom to receive and impart information without interference by public authorities.

The Court's jurisprudence demonstrates a consistent position regarding the priority of freedom of expression in a democratic society. This legal position was formulated as early as the judgment in The Sunday Times v. the United Kingdom (1979), where the Court emphasized the importance of open public debate in a democratic society. These approaches were further developed in a number of the Court's judgments. In particular, in Lingens v. Austria (1986), the Court stressed that the limits of acceptable criticism regarding political figures are significantly wider than those concerning private individuals. In Goodwin v. the United Kingdom (1996), the Court formulated the fundamental principle of the protection of the confidentiality of journalistic sources, recognizing it as one of the basic guarantees of press freedom. In the judgment in Oberschlick v. Austria (1997), the Court confirmed the importance of protecting political criticism within the scope of freedom of expression.

Important guidance for legal practice was also provided in Fressoz and Roire v. France (1999), where the Court emphasized the right of journalists to use information of public interest, and in Roemen and Schmit v. Luxembourg (2003), in which a violation of Article 10 of the Convention was found in connection with searches aimed at identifying journalistic sources of information. Similar approaches

were confirmed in the judgment in Busuioc v. Moldova (2004), where the Court stressed the special role of journalists in covering issues of public interest.

The case law of the European Court of Human Rights is of significant importance for the development of national standards for the protection of freedom of speech and media activity in Ukraine, since the Court's legal positions serve as a guideline for the development of judicial practice and the improvement of legislative regulation in the field of information relations. Thus, in the judgment in Ukrainian Media Group v. Ukraine (2005), the Court found a violation of Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms due to the disproportionate application of civil liability to a mass media outlet for disseminating information of public interest. The European Court of Human Rights emphasized that the imposition of substantial financial sanctions on media outlets may have a chilling effect on journalistic activity and restrict public debate on issues of public importance.

A similar legal position was expressed in the case of Gazeta Ukraina-Tsentr v. Ukraine (2010), in which the judgment was delivered on 15 July 2010. In this decision, the European Court of Human Rights emphasized that holding the editorial board of a newspaper liable for publishing critical materials concerning public officials, without properly taking into account the public interest, constitutes a disproportionate interference with freedom of expression. The Court stressed that national courts must consider the public interest of the disseminated information and the special role of the media as a «public watchdog», ensuring an appropriate balance between the protection of reputation and freedom of expression.

These standards were further developed in Editorial Board of Pravoye Delo and Shtekel v. Ukraine (2011), where the Court found a violation of Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms in connection with the imposition of liability on a newspaper editorial board for reprinting material from the Internet. The Court noted that the automatic imposition of liability on journalists for disseminating information from online sources, without assessing the good faith of their actions and the public significance of the information, is incompatible with the principles of freedom of expression.

In addition, in Shapovalov v. Ukraine (2012), the Court established a violation of Article 10 of the Convention due to the unjustified imposition of liability on a journalist for criticizing public authorities. The Court emphasized that the limits of permissible criticism with regard to public authorities are wider than those concerning private individuals, since the activities of state bodies must remain under close public scrutiny.

In its more recent jurisprudence, the Court has also examined cases related to information security and media freedom in the context of the Russian aggression against Ukraine. In particular, in the inter-state case Ukraine and the Netherlands v. Russia (2025), in which the judgment was delivered on 9 July 2025, the European Court of Human Rights recognized systemic human rights violations in the occupied territories of Ukraine, including persecution of journalists, seizure of media infrastructure, and suppression of freedom of expression.

Thus, the case law of the European Court of Human Rights concerning Ukraine has developed some important legal standards, including the necessity of adhering to the principle of proportionality in interference with freedom of speech, taking into

account the public interest of disseminated information, ensuring special protection for journalistic activity, and guaranteeing an appropriate balance between media freedom and other rights and interests in a democratic society.

Particular importance in the Court's case law is attached to the development of clear criteria for the admissibility of restrictions on freedom of expression. The Court consistently applies *a three-part test*, according to which any interference with freedom of expression must be: *prescribed by law, pursue a legitimate aim, and be necessary in a democratic society*. This approach has effectively shaped the European paradigm for assessing the justification of restrictions on freedom of speech, according to which priority is given to ensuring openness of public debate and the free functioning of the media.

In Ukraine, the case law of the European Court of Human Rights has particular significance in connection with the provisions of the Law of Ukraine «On the Execution of Judgments and the Application of the Case Law of the European Court of Human Rights», which establishes the obligation of the state to execute the Court's judgments in cases against Ukraine and to take into account its legal positions in national judicial and administrative practice. The application of the Court's jurisprudence contributes to the implementation of European human rights standards into the national legal system and ensures the harmonization of Ukrainian legislation with the general European approaches to the protection of freedom of expression.

The rapid development of digital technologies has significantly transformed the nature of journalistic activity. Modern media actively use electronic devices, cloud services, encrypted communication channels, and digital platforms for the collection, processing, and dissemination of information.

At the same time, the digital environment creates new challenges for ensuring media freedom. During the investigation of cyber offenses, state authorities may apply measures of criminal procedural coercion related to access to journalists' electronic devices, servers, or digital accounts. Such actions potentially create a risk of revealing journalistic sources and interfering with professional activities.

In this context, particular importance is attached to ensuring a balance between the interests of criminal justice, on the one hand, and guarantees of freedom of speech and the protection of journalistic sources, on the other.

In its case law, the European Court of Human Rights consistently emphasizes that the Internet has become one of the key tools for the exercise of freedom of expression. For example, in Delfi AS v. Estonia (2015), the Court examined the issue of the liability of an internet portal for user comments. The Court recognized the possibility of holding online platforms liable for unlawful content, but emphasized the need to comply with the principle of proportionality and to take into account the role of internet media in ensuring public debate.

Another important precedent in the field of legal regulation of online media and internet platforms was established in Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary (2016), in which the European Court of Human Rights delivered its judgment on 2 February 2016. In this case, the Court examined the compatibility with the requirements of Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms of the practice of holding owners of internet resources liable for offensive or unlawful comments posted

by users on their websites. The applicants were the Association of Hungarian Internet Content Providers and the popular news portal Index.hu, which challenged the decisions of national courts that had imposed liability on them for comments made by third parties.

Analyzing the circumstances of the case, the European Court of Human Rights noted that internet platforms and online media play an important role in ensuring freedom of public debate in a modern democratic society. It is largely through internet resources that citizens exercise their right to freely receive and disseminate information, as well as their ability to participate in public discussions on issues of public interest.

The Court emphasized that the automatic imposition of liability on the owners of websites or internet platforms for user comments, without taking into account the specific circumstances of the case, may create disproportionate restrictions on freedom of expression. According to the Court, such an approach may lead to the so-called «chilling effect», which would restrain the development of online discussions and negatively affect the functioning of internet media as an open space for public dialogue.

At the same time, the European Court of Human Rights stressed that the assessment of the liability of internet resources should be carried out about several criteria, including: the nature of the comments, the existence of content moderation mechanisms, the promptness of the platform's response to notifications about unlawful content, and the role of the relevant resource in disseminating information of public significance.

Thus, the judgment in Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary (2016) became an important stage in the development of European standards for regulating the activities of online media. It confirmed the necessity of ensuring a fair balance between the protection of reputation and the rights of others, on the one hand, and guarantees of freedom of expression and the development of the digital information space, on the other. This legal position of the Court is of significant importance for national law-enforcement practice, particularly in the context of determining the limits of liability of media platforms for user-generated content on the Internet.

These approaches were further developed in Magyar Jeti Zrt v. Hungary (2018), where the Court concluded that holding journalists liable solely for posting hyperlinks may have a «chilling effect» on the freedom of journalistic activity in the digital environment. The Court emphasized that journalists should be able to use modern digital tools for disseminating information without the risk of disproportionate interference by the state.

Protection of journalistic sources of information is recognized by the European Court of Human Rights as one of the cornerstones of media freedom. Of particular relevance in the context of the digitalization of journalistic activity is the judgment in Sanoma Uitgevers B.V. v. the Netherlands (2010) (14 September 2010), in which the Court formulated the requirement of prior independent review before granting state authorities access to journalistic materials. Such access must be accompanied by effective procedural safeguards designed to prevent abuse. In the modern digital context, these guarantees acquire particular significance, since journalistic materials

are often stored in the form of electronic data – on servers, in cloud storage, or in electronic correspondence.

Another decision of significant importance for the development of modern standards for the protection of journalistic materials is Financial Times Ltd and Others v. the United Kingdom (2009), delivered on 15 December 2009. In this case, the European Court of Human Rights examined the legality of requiring several British media outlets to disclose a source of information related to confidential data concerning the possible takeover of one company by another. The Court concluded that a requirement by state authorities to disclose journalistic sources constitutes a serious interference with freedom of expression guaranteed by Article 10 of the European Convention on Human Rights. In its judgment, the Court emphasized that the protection of the confidentiality of journalistic sources is one of the fundamental prerequisites for press freedom, since without such guarantees potential informants may refrain from providing information of public interest.

The Court stressed that the obligation to disclose sources of information cannot be applied automatically even in cases where the relevant information is of interest to law-enforcement authorities or business entities. Any state interference in the protection of journalistic sources must meet strict requirements of necessity and proportionality and must be justified by the existence of a compelling public interest.

Furthermore, the Court noted that forcing journalists to disclose their sources may create the so-called «chilling effect», which negatively affects the ability of the media to perform their democratic function of informing the public. In this regard, the European Court of Human Rights recognized that national courts must apply particularly careful scrutiny when resolving issues related to access to journalistic materials, ensuring an appropriate balance between the interests of justice and the guarantees of freedom of expression.

The aforementioned judgment became an important guideline for the development of European standards for the protection of journalistic sources and reaffirmed the established position of the European Court of Human Rights that the confidentiality of information sources is one of the key elements of the effective functioning of independent media in a democratic society.

Important benchmarks in the field of digital surveillance were also established in the judgments Big Brother Watch and Others v. the United Kingdom (2021) (25 May 2021) and Centrum för rättvisa v. Sweden (2021) (25 May 2021), in which the Court recognized that mass electronic surveillance may pose a serious threat to media freedom if it is not accompanied by effective legal safeguards. For Ukraine, these standards are particularly relevant in light of the use of cybersecurity measures and intelligence activities.

Therefore, the analysis of the case-law of the European Court of Human Rights demonstrates the formation of a comprehensive system of international standards for the protection of media freedom and journalistic activity in the digital environment. In its judgments, the Court consistently emphasizes that freedom of expression, enshrined in the European Convention on Human Rights, extends to all modern forms of communication, including the Internet, digital platforms, and other information and communication technologies.

At the same time, the digitalization of social relations generates new challenges for ensuring media freedom, particularly those related to the use of digital evidence, searches of electronic devices, access to cloud services, or the application of mass digital surveillance tools. In this regard, the European Court of Human Rights has developed a number of fundamental legal positions according to which any interference by the state in journalistic activity must comply with the requirements of legality, pursue a legitimate aim, and be necessary in a democratic society.

The Court pays particular attention to the protection of journalistic sources of information, the prevention of the so-called «chilling effect» on journalistic activity, and the ensuring of effective judicial control over the application of measures of state interference. In the digital context, these guarantees become even more significant, since access to journalists' electronic communications, servers, or mobile devices may create a real risk of revealing confidential sources of information.

For Ukraine, the implementation of these standards is of particular importance in view of the need to simultaneously ensure effective counteraction to cybercrime, protect the state's information security, and respect fundamental human rights. In this context, the practice of the European Court of Human Rights serves as an important guideline for the development of national legislation and law-enforcement practice, contributing to the formation of a balanced model of legal regulation that ensures an appropriate balance between the interests of a democratic society, the needs of national security, and the guarantees of freedom of expression and media activity in the digital era.

CONCLUSION

The modern system of guaranteeing media freedom and journalistic activity is formed under the influence of the complex interaction of constitutional principles, international legal standards, and the practice of international judicial institutions. In this context, the key role is played by the legal combination of national constitutional guarantees enshrined in the Constitution of Ukraine with the standards of protection of freedom of expression developed within the European Convention on Human Rights and further elaborated in the jurisprudence of the European Court of Human Rights.

The analysis of the theoretical and normative foundations of the functioning of media freedom indicates that in a modern democratic society, it acquires not only the character of an individual subjective right but also performs an institutional function of ensuring the openness of public discourse, transparency in the activities of public authorities, and the effective functioning of civil society. For this reason, guarantees of freedom of speech and journalistic activity should be considered an important element of the system of democratic constitutionalism, which ensures the possibility of public oversight over government and the formation of informed public opinion.

At the same time, the development of digital technologies significantly changes the nature of media activity and creates new legal challenges for ensuring freedom of expression. The digital environment considerably expands the possibilities for disseminating information, but at the same time increases the risks of unlawful interference in journalistic activity through the use of digital control tools, access to electronic data, seizure of information carriers, or the use of electronic surveillance

technologies. Under such conditions, the formation of effective legal mechanisms capable of ensuring an appropriate balance between the needs of criminal justice, the interests of information security, and the guarantees of media freedom becomes particularly relevant.

The case-law of the European Court of Human Rights plays a decisive role in this process, since its judgments have developed the key standards for assessing the lawfulness of state interference in the sphere of freedom of expression. In particular, the Court consistently emphasizes the need to apply the principle of proportionality, to prevent the so-called «chilling effect» on journalistic activity, to ensure proper protection of journalistic sources of information, and to introduce effective procedural safeguards when the state uses control mechanisms in the digital environment.

For Ukraine, these standards are of particular importance given the simultaneous need to ensure democratic freedoms, counter cybercrime, and protect the state's information security in the conditions of armed aggression and hybrid information threats. Under such circumstances, the legal positions of the European Court of Human Rights serve as an important guideline for improving national legislation, developing judicial practice, and forming a balanced model of legal regulation of media activity in the digital environment.

Therefore, ensuring effective constitutional and legal guarantees of media freedom in the digital era requires a comprehensive approach that combines constitutional principles, international legal standards, and modern mechanisms for the legal protection of journalistic activity. Such an integrated model of legal regulation is capable of ensuring an adequate level of realization of freedom of expression while maintaining a balance between democratic values, the interests of society, and the needs of ensuring state security in the conditions of the rapid digital transformation of the information space.

SUMMARY

This article examines the constitutional and legal guarantees of media freedom and journalistic activity in the digital environment, with particular emphasis on the case law of the European Court of Human Rights in the context of cyber offences. The study analyzes freedom of expression as a fundamental value of modern constitutionalism and an essential prerequisite for the functioning of a democratic society governed by the rule of law. Special attention is devoted to the constitutional framework of freedom of speech and media activity in Ukraine, as well as its relationship with international human rights standards.

The article explores the role of the European Court of Human Rights in shaping contemporary legal standards for the protection of freedom of expression under Article 10 of the European Convention on Human Rights. It reviews key ECtHR judgments concerning media freedom, the protection of journalistic sources, and the limits of permissible state interference in journalistic activity. Particular attention is given to the legal challenges arising from digital technologies, including access to electronic data, digital surveillance, and the use of digital evidence in criminal proceedings.

The study concludes that effective protection of media freedom in the digital era requires a comprehensive system of constitutional, legislative, and institutional guarantees aligned with European human rights standards.

References:

1. Конституція України : Закон України від 28 червня 1996 р. №254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр
2. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004
3. Закон України «Про медіа» від 13 грудня 2022 р. №2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20
4. Закон України «Про інформацію» від 2 жовтня 1992 р. №2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12
5. Закон України «Про виконання рішень та застосування практики Європейського суду з прав людини» від 23 лютого 2006 р. №3477-IV. URL: https://zakon.rada.gov.ua/laws/show/3477-15
6. European Court of Human Rights. HUDOC database. URL: https://hudoc.echr.coe.int
7. The Sunday Times v. the United Kingdom, Judgment of 26 April 1979. URL: https://hudoc.echr.coe.int/?i=001-57584
8. Lingens v. Austria, Judgment of 8 July 1986. URL: https://hudoc.echr.coe.int/?i=001-57523
9. Goodwin v. the United Kingdom, Judgment of 27 March 1996. URL: https://hudoc.echr.coe.int/?i=001-57974
10. Fressoz and Roire v. France, Judgment of 21 January 1999. URL: https://hudoc.echr.coe.int/?i=001-58965
11. Roemen and Schmit v. Luxembourg, Judgment of 25 February 2003. URL: https://hudoc.echr.coe.int/?i=001-60958
12. Busuioc v. Moldova, Judgment of 21 December 2004. URL: https://hudoc.echr.coe.int/?i=001-67615
13. Ukrainian Media Group v. Ukraine, Judgment of 29 March 2005. URL: https://hudoc.echr.coe.int/eng?i=001-68648
14. Financial Times Ltd and Others v. the United Kingdom, Judgment of 15 December 2009. URL: https://hudoc.echr.coe.int/fre?i=001-96157
15. Gazeta Ukraina-Tsentr v. Ukraine, Judgment of 15 July 2010. URL: https://hudoc.echr.coe.int/rus?i=001-99854
16. Sanoma Uitgevers B.V. v. the Netherlands, Judgment of 14 September 2010. URL: https://hudoc.echr.coe.int/?i=001-100448
17. Editorial Board of Pravoye Delo and Shtekel v. Ukraine, Judgment of 5 May 2011. URL: https://hudoc.echr.coe.int/eng?i=001-104685
18. Shapovalov v. Ukraine, Judgment of 31 July 2012. URL: https://hudoc.echr.coe.int/fre?i=001-112570
19. Delfi AS v. Estonia, Judgment of 16 June 2015. URL: https://hudoc.echr.coe.int/eng?i=002-10636
20. Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, Judgment of 2 February 2016. URL: https://hudoc.echr.coe.int/eng?i=001-160314

21. Magyar Jeti Zrt v. Hungary, Judgment of 4 December 2018. URL: https://hudoc.echr.coe.int/fre?i=001-187930
22. Big Brother Watch and Others v. the United Kingdom, Judgment of 25 May 2021. URL: https://hudoc.echr.coe.int/fre?i=001-210077
23. Centrum för rättvisa v. Sweden, Judgment of 25 May 2021. URL: https://hudoc.echr.coe.int/?i=001-210078
24. Council of Europe. Freedom of Expression and Media Freedom Standards. URL: https://www.coe.int/en/web/freedom-expression
25. Organization for Security and Co-operation in Europe. Media Freedom and Safety of Journalists. URL: https://www.osce.org/representative-on-freedom-of-media

Information about the authors:
Slinko Tetiana Mykolaivna,
Professor,
Head of the Department of Constitutional Law of Ukraine at the
Yaroslav Mudryi National Law University,
77, Hryhorii Skovoroda St., Kharkiv, Ukraine, 61024

Slinko Kateryna Mykolaivna,
Ph.D. in Law,
Visiting professor at State University of Northern Paraná (Brazil),
215, Av. Manoel Ribas, Jacarezinho – PR, Brazil, 86400-000

DOI https://doi.org/10.30525/978-9934-26-686-7-17

ІНСТИТУЦІОНАЛІЗАЦІЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ: ПРАВОВИЙ СТАТУС ТА ПОВНОВАЖЕННЯ СУБ'ЄКТІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Співак М. В., Дубіна О. М.

ВСТУП

Масштабна російська кіберагресія проти України стала ключовим каталізатором, що не лише виявив критичні вразливості, а й підкреслив екзистенційну необхідність прискореного розвитку національної індустрії продуктів та послуг кібербезпеки. Сучасний стан інформаційного протистояння характеризується безпрецедентною кількістю та складністю атак: Україна стабільно входить до переліку країн світу, що зазнають найбільшого цифрового тиску, поступаючись за інтенсивністю лише США. Лише протягом 2023 року було офіційно зафіксовано 2544 кіберінциденти, що на 16% перевищило показники попереднього року. Ця динаміка свідчить про перехід кіберзагроз у фазу перманентного тиску на державні інституції, оборонно-промисловий комплекс, енергетику та фінансовий сектор. Постійні атаки з боку російських хакерських угруповань, що використовують методи DDoS, розповсюдження програм-вимагачів (Ransomware) та фішингу, змусили український ринок еволюціонувати швидше за світові тренди.

Як наслідок, за останні вісім років обсяг українського ринку кібербезпеки продемонстрував стрімке зростання, збільшившись у чотири рази – з 32 млн доларів у 2016 році до 138 млн доларів у 2024-му. Попри те, що частка України на глобальному ринку поки що становить менше 1%, країна перетворилася на світового трендсеттера та унікальний полігон для R&D-інновацій. Специфіка воєнного стану зумовила домінування сегмента кіберрішень, який займає 57% ринку, випереджаючи глобальний показник, де переважають сервіси. Це пояснюється гострою потребою у впровадженні автоматизованих систем захисту на основі штучного інтелекту, здатних миттєво реагувати на загрози за умов обмеженого людського ресурсу. Прогнози вказують на подальшу інтенсифікацію галузі: очікується, що до 2029 року ринок зросте ще на 50%, досягнувши позначки у 209 млн доларів. Такий розвиток є не просто економічним показником, а стратегічним елементом національної безпеки, оскільки масштаби загроз диктують вимоги до створення повністю автономної та високотехнологічної екосистеми кіберзахисту, здатної протистояти викликам першої у світі повномасштабної кібервійни[1].

[1] Огляд ринку кібербезпеки в Україні : звіт / DataDriven, підкомітет з кібербезпеки EBA, CyberTech комітет Асоціації IT Ukraine за сприяння Аспен Інституту Київ, за підтримки Проєкту USAID. Січень 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 10.02.2026).

1. Кібербезпека як багатоаспектне явище: різні підходи до визначення та забезпечення захисту

Світ стрімко змінюється. Нинішнє різко контрастує із вчорашнім. Розвиток нових комунікацій і технологій (зокрема Інтернет) супроводжуються новими дестабілізаційними викликами (сучасні інформаційні війни, кіберзагрози), «полікризами» та «пермакризами» (значна кількість проблем, які виникають одночасно) які почали формуватися ще наприкінці 2010-х років[2]. Однак теоретичним викликом для сучасної науки є не лише проблеми концептуалізацій сучасних трансформацій а й продукування нових типів знання та конструювання нових типів відносин. Позаяк ми живимо за доби глобалізації знань і спільних проблем людства, більша відкритість інформаційного простору потребує захисту. Адже у ньому нашаровуються поєднання національного, соціального, культурного і навіть суто особистого із глобальним, загальнолюдським, універсальним і безпековим. В сучасних умовах проблеми інформаційних відносин актуалізувалися у зв'язку з глобалізацією інформаційних процесів, бурхливим розвитком і пануванням, стало очевидним відокремлення такого явища, як «кібербезпека».

Кібербезпека – це складний і багатогранний процес, що охоплює різні аспекти напрямків, механізмів і методів захисту. Хоча структура кібербезпеки ще не повністю систематизована, її розуміння як комплексної діяльності дозволяє гармонізувати термінологію та глибше проаналізувати суттєві аспекти цієї сфери. Вивчаючи кібербезпеку, необхідно пам'ятати, що вона є невід'ємною частиною інформаційних технологій. У сучасному світі стрімкий розвиток і поширення нових інформаційно-комунікаційних технологій створює умови для глобальної інформаційної революції. Цей процес має безпосередній вплив на всі аспекти діяльності держави, включаючи політичну, економічну, управлінську, фінансову, культурну, наукову та інформаційну сфери. Як слушно зазначає В. Бондаренко людство живе в інформаційному суспільстві. Інформація – є рушійною силою перетворень та розвитку людства, а запорукою його процвітання є людська інтелектуальна творчість. Головним об'єктом, на якому концентрується безпосередній інформаційний деструктивний вплив у межах інформаційної війни, стали громадська думка та свідомість окремої людини. Саме тому духовні, культурні, історичні, етнічні й загальнонаціональні цінності, традиції, надбання держави стають полем кібербитви, адже це той простір, де дуже багато вразливих й чутливих рецепторів суспільства[3].

Нині, особливу увагу приділяється людиноцентричним підходам, збалансованому управлінню ресурсами та розширенні можливостей цифровізації. Цифровізація включає в себе комплексний аналіз та впровадження цифрових технологій у всі аспекти діяльності підприємств. Д. Попова, С. Яременко під кібербезпекою, розуміють систему комплексних заходів, що забезпечують захист

[2] Екзистенційні виклики перед Україною. Демографія. DeepState. 23.09.2023. URL: https://deepstateua.com/iekzistientsialni-vikliki-ukrayini-chastina-i-diemoghrafiia/ (дата звернення: 11.02.2026).

[3] Бондаренко В. Кібербезпека: роль держави у захисті суспільства та окремої особистості у збереженні міжетнічного миру. *Аспекти публічного управління*. 2020. Т. 8, № Спец. вип. 1. С. 18–21. DOI: 10.15421/152031

інформаційних ресурсів, технологій та інфраструктури від загроз будь-якого походження з метою забезпечення стійкості, надійності та безперервного розвитку держави, суспільства та окремих осіб в умовах цифрової трансформації та Індустрії 5.0. На їх думку Індустрію 5.0 не слід сприймати як заміну попередній парадигмі – Індустрії 4.0, а радше як її розвиток та доповнення, яке вносить нові ключові аспекти:

– Людиноцентричний підхід. Індустрія 5.0 підкреслює значення створення безпечного та інклюзивного робочого середовища, де пріоритетом є здоров'я та благополуччя працівників, з метою досягнення не лише високої продуктивності, а й задоволення потреб кожного працівника.

– Стійкість. Здатність швидко адаптуватися до змін є критично важливою для підприємств, які прагнуть залишатися конкурентоспроможними в умовах невизначеності, включаючи нові технологічні розробки та зміни в ринкових потребах.

– Екологічний розвиток. Індустрія 5.0 наголошує на важливості циркулярних процесів, які сприяють переробці та повторному використанню природних ресурсів, зменшенню відходів та зниженню екологічного впливу, тим самим підвищуючи ефективність виробничих процесів[4].

За іншим підходом, кібербезпека полягає в захисті від кібератак, які націлені на корпоративні мережі[5]. Л. Бєлкін, Ю. Юринець, М. Бєлкін, Є. Криволап доводять, що кібербезпека є окремим випадком загального поняття безпеки інформації, але такої інформації, яка обертається у кіберпросторі. При цьому причиною підвищеної уваги саме до кіберзагрозам і кібербезпеки є дедалі зростаюча роль обігу інформації в комп'ютерних системах і електронно-комунікаційних мережах. Та пропонують ввести у стабільний науковий і практичний оборот поняття «когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство[6].

Г. Форос та В. Жогов в одній зі своїх публікацій наголошують на двох підходах до поняття кібербезпека: вузькому та широкому. При розгляді кібербезпеки у вузькому значенні, на думку науковців, необхідно говорити, перш за все про захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. У широкому сенсі, їхнє бачення полягає в тому, що кібербезпека – це сукупність вольових суспільних відносин, що складаються в процесі свідомого

[4] Попова Д. В. Кібербезпека в епоху Індустрії 5.0: нові виклики та можливості. *Економічний вісник Донбасу.* 2024. № 3. С. 203-216. DOI: https://doi.org/10.12958/1817-3772-2024-3(77)-203-216

[5] Костроміна М. О. Кіберстійкість і кібербезпека: у чому різниця? *Сучасний захист інформації.* 2022. № 4. С. 71-75. DOI: 10.31673/2409-7292.2022.040012

[6] Бєлкін Л. М. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Юридичний вісник. Повітряне і космічне право*. 2022. № 3. С. 78-86. DOI: 10.18372/2307-9061.64.16893

і добровільного дотримання громадянами встановлених в нормах права та в інших нормах неюридичного характеру правил поведінки в кіберпросторі, і тим самим забезпечуються злагоджене, стійке, спільне життя людей в умовах розвинутого суспільства[7].

І. Яковів вважає, що ключовим терміном для розуміння сутності «кібербезпеки» є «кіберпростір». Зазвичай його пов'язують з: глобально розподіленими системами, що реалізовують цифрові комп'ютерні технології обробки інформації; віртуальним середовищем на основі цих систем, в якому можуть існувати видумані активні об'єкти (різноманітні герої комп'ютерних ігор і цифрової анімації, симуляційні моделі та інше). Ці інформаційні об'єкти, що існують тільки в комп'ютерах, здатні здійснювати реальний сенсорний вплив на психіку людини (візуальний, звуковий та іншій); можливістю здійснювати приховані (анонімні) інформаційні впливи на людей і різні пристрої; відсутністю «територіальних кордонів» при комунікаціях людей різних держав (відсутність «кіберкордонів»)[8].

У науковому доробку О. Ткаченка та К. Ткаченко представлена комплексна дефініція ключових категорій сфери цифрової безпеки, зокрема понять «кіберпростір», «кібербезпека» та «забезпечення кібербезпеки». Автори пропонують розглядати кіберпростір як специфічне кіберінформаційне середовище, що акумулює в собі семантичну сутність об'єктів профільної інфраструктури, а також архітектуру взаємозв'язків між ними. У межах цієї концепції об'єкти кіберінформаційної інфраструктури диференціюються на три засадничі рівні: апаратно-технічний (кінцеве обладнання, гаджети, персональні обчислювальні машини); програмно-технологічний (мережева інфраструктура та відповідне програмне забезпечення); інформаційний (бази даних, вебконтент та масиви інтернет-відомостей). Під кібербезпекою дослідники розуміють динамічний стан захищеності кіберпростору держави та його структурних елементів від деструктивного зовнішнього впливу. Такий стан характеризується мінімізацією ризиків порушення стабільності системи та її сталого розвитку. Ключовим аспектом кібербезпеки в інтерпретації авторів є здатність до своєчасної ідентифікації, превенції та нейтралізації кіберзагроз і кіберзлочинів, що можуть загрожувати інтересам особи, корпоративного сектору, державних інституцій чи національній безпеці загалом. Логічним продовженням цієї концепції є дефініція забезпечення кібербезпеки, яке трактується як цілеспрямована сукупність заходів, орієнтованих на редукцію ризиків заподіяння шкоди внаслідок технічних збоїв, програмних помилок або несанкціонованого (некоректного) використання ресурсів кіберпростору. Крім

[7] Форос Г. В. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава.* 2019. № 33. С. 128-134. DOI: https://doi.org/10.18524/2411-2054.2019.33.162068

[8] Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. Vol. 5, № 2. С. 134-144. DOI: https://doi.org/10.20535/2411-1031.2017.5.2.136981

того, цей процес охоплює заходи з оперативного відновлення функціональності всіх складових кіберінфраструктури після настання деструктивних подій[9].

2. Законодавче регулювання кібербезпеки в Україні: аналіз імплементації та стратегічних напрямків

Оскільки кібербезпека стала національним пріоритетом, відповідальність за розробку та реалізацію політики кібербезпеки була чітко розподілена в державному секторі. Однак жоден з існуючих органів влади не має комплексного розуміння та достатньо широкого мандату для управління всіма аспектами кібербезпеки. В. Дзюндзюк та Є. Котух виділяють низку загальних аспектів, які, на їх погляд, мають бути присутніми в політиці та стратегії кібербезпеки в Україні. Зокрема, це: урахування питань суверенітету при розробці політики; важливість діалогу за участю багатьох зацікавлених сторін; важливість економічних аспектів кібербезпеки; покращення міжнародного співробітництва; гнучкий підхід до формування та реалізації політики; повага до фундаментальних цінностей; посилення координації органів влади на політичному та оперативному рівнях; зміцнення публічно-приватного співробітництва[10].

Окремі питання кіберзахисту містяться в Кодексі цивільного захисту України, в Законах України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру». В постановах Кабінету Міністрів України: Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (від 31.12.2025 № 1799), Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту (від17.12.2025 № 1668), Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах (від 03.12.2025 № 1580), Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози (від 26.11.2025 № 1533), Про затвердження Порядку призначення керівника з кіберзахисту на посаду в органі державної влади (від 26.11.2025 № 1516) та ін.

Послідовність у намірах законодавця прослідковується з 2016 року. Зокрема з затвердження Стратегії кібербезпеки України, що стала важливим кроком у запровадженні підходів довгострокового планування в цій сфері. Метою Стратегії кібербезпеки України (2016 року) стало створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідними було: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю,

[9] Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. Вип. 1. С. 75-86. DOI: https://doi.org/10.31866/2617-796x.1.2018.147257

[10] Дзюндзюк В. Б. Кібербезпека як один з пріоритетів національної політики. *Державне будівництво*. 2020. № 2. С. 1-19. DOI: 10.34213/db.20.02.01

поглиблення міжнародного співробітництва у цій сфері; забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура)[11].

У 2017 році був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України». Закон визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У ст. 1 законодавець тлумачить такі терміни як: індикатори кіберзагроз, інформація про інцидент кібербезпеки, інцидент кібербезпеки, кібератака, кіберзагроза, кіберзахист, кіберзлочин, кіберзлочинність, кібероборона, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство та інші. Зокрема, законодавець термін кібербезпека трактує як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі[12]. Відповідно до ст. 4 Закону об'єктами кібербезпеки є: 1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об'єкти критичної інфраструктури. Об'єктами кіберзахисту визначені: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу[13].

[11] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 14.02.2026).

[12] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

[13] Там само.

Нова Стратегія кібербезпеки України (2021 року) врахувала попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав – членів ЄС та держав – членів НАТО. Були визначені нові загрози кібербезпеці України: гібридна агресія Російської Федерації проти України у кіберпросторі; кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат; організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності; використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності. Відповідно визначені передумови та чинники, які формують окреслені загрози:

– висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій, відсутність системи оцінки відповідності такої продукції вимогам з безпеки, що підвищує ступінь уразливості інформаційної інфраструктури від незадекларованих функцій та звужує спроможності протидії кіберзагрозам;

– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства, недостатня врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

– відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки;

– недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

– невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, низький рівень обізнаності суспільства щодо кіберзагроз та кіберзахисту[14].

Для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування); набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість); забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами – членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія)[15].

Згодом затверджено план заходів на 2025 рік з реалізації Стратегії кібербезпеки України. У таблиці Плану Урядом було визначено 29 завдань. Зокрема такими є: створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору; запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони; розроблення та забезпечення виконання плану кібероборони як складової частини плану оборони України; посилення спроможностей щодо проведення негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, поступове охоплення такими заходами всіх об'єктів; посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, що спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку у сфері кібербезпеки[16].

[14] Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021 (рішення РНБО від 14.05.2021). URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 14.02.2026).

[15] Там само.

[16] Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення: 14.02.2026).

3. Класифікація та механізми управління кіберінцидентами: синергія наукових підходів та державних стандартів

Дослідження української наукової спільноти демонструють еволюцію від теоретичного осмислення кіберзахисту до розробки прикладних методик протидії в умовах реальної кібервійни. Аналіз праць провідних фахівців дозволяє виокремити ключові вектори розвитку вітчизняної наукової думки щодо класифікації та управління кіберінцидентами. Праці Є. Живила та І. Ромашки зосереджені на створенні системних протоколів спільної дії. Їхній підхід підкреслює важливість злагодженої взаємодії різних суб'єктів кібербезпеки не лише під час атаки, а й у процесі ліквідації її наслідків, що фактично формує операційну основу для державної системи реагування[17]. В. Федик та Г. Денисенко акцентують увагу на захисті об'єктів критичної інфраструктури. Їхні дослідження класифікують інциденти крізь призму менеджменту кризових ситуацій, пропонуючи методологію, де реагування є невід'ємною частиною загальної стратегії управління ризиками[18]. Питання вимірюваності успіху команд реагування піднімають В. Кінзерявий та В. Гнатюк. Встановлення базових показників ефективності дозволяє об'єктивно оцінювати спроможність підрозділів і класифікувати їх за рівнем готовності до відбиття загроз[19]. О. Сахарова та І. Близнюк розглядають виявлення інцидентів як стратегічний інструмент запобігання кіберзлочинності. Їхня позиція інтегрує технічні заходи реагування у загальну правову рамку боротьби зі злочинністю в цифровому просторі[20]. Сучасним доповненням до технічних аспектів є робота О. Гарасимчука, Т. Костишина, О. Любчика та М. Швед, які фокусуються на розробці методик оповіщення населення. Це розширює класичне розуміння реагування, виводячи його за межі вузькоспеціалізованих ІТ-департаментів у площину суспільної безпеки[21].

На думку А. Вавіленко залежно від характеру та масштабів кіберінциденти можуть бути класифіковані так: 1) інциденти низької важливості – мінімальний вплив на систему, який не призводить до серйозних наслідків; 2) серйозні інциденти – інциденти, які суттєво впливають на функціонування системи або можуть спричинити витоки конфіденційних даних; 3) критичні інциденти –

---

[17] Живило Є. О. Протокол спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти, а також при усуненні їх наслідків. *Системи управління, навігації та зв'язку.* 2024. Вип. 1. С. 66-76. DOI: 10.26906/SUNZ.2024.1.066

[18] Федик В. Р. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об'єктах критичної інфраструктури: реагування на кіберінциденти та менеджмент кризових ситуацій. *Інформація і право.* 2024. № 1. С. 195-202. DOI: 10.37750/2616-6798.2024.1(48).300822

[19] Кінзерявий В. Базові показники ефективності роботи команд реагування на кіберінциденти. *Безпека інформації.* 2014. Т. 20, № 2. С. 193-196.

[20] Сахарова О. Б. Виявлення та реагування на кіберінциденти і кібератаки як заходи запобігання кіберзлочинності. *Наука і правоохорона*. 2023. Вип. 2. С. 220-231. DOI (Issue): https: //doi.org/10.36486/np.2023.2(60)

[21] Гарасимчук О. І. Розробка вдосконаленої методики оповіщення населення про кіберінциденти. *Інформатика та математичні методи в моделюванні.* 2025. Т. 15, № 2. С. 187-195. DOI 10.15276/imms.v15.no2.187

інциденти, що мають великий масштаб і можуть призвести до значних фінансових або репутаційних втрат для організації[22].

Чотирирівнева модель класифікації інцидентів, запропонована О. Саморай та О. Семенюк, становить методологічну базу для комплексного аналізу потенційних деструктивних впливів. Поділ загроз на технічні, соціальні, фізичні та інциденти безпеки дозволяє сформувати цілісну архітектуру моніторингу та обрати найбільш релевантні стратегії детекції й алгоритми реагування для кожного специфічного сценарію. Такий структурований підхід забезпечує високу адаптивність систем захисту до різнопланових викликів сучасної IT-інфраструктури. Розглянемо кожен із зазначених рівнів детальніше. Технічні інциденти становлять категорію деструктивних подій, зумовлених апаратними чи програмними деградаціями, що призводять до дестабілізації або повної зупинки роботи інформаційних систем. Етіологія таких збоїв зазвичай охоплює широкий спектр чинників, серед яких першочергове значення мають критичні несправності фізичного обладнання – серверної інфраструктури, накопичувачів даних та мережевих вузлів. Поряд із цим суттєвий ризик становлять недосконаліть програмного коду, наявність уразливостей, а також виникнення міжаплікаційних конфліктів або помилок під час оновлення систем через їхню технологічну несумісність. Окрему групу чинників формують порушення в роботі комунікаційних каналів, що включають відмови маршрутизаторів, перевантаження ліній зв'язку та низьку експлуатаційну якість послуг інтернет-провайдерів. Крім того, критичний вплив на доступність ресурсів мають цілеспрямовані DDoS-атаки, механізм яких полягає у штучному створенні масового потоку запитів для вичерпання лімітів системи, що неминуче спричиняє часткову або повну відмову в обслуговуванні користувачів[23]. Інциденти безпеки класифікуються як події, що несуть пряму загрозу цілісності, доступності та конфіденційності інформаційних активів, потенційно призводячи до несанкціонованого витоку або ексфільтрації даних. Спектр таких інцидентів охоплює компрометацію облікових записів користувачів шляхом ініціації атак типу «brute-force» (підбір паролів) або експлуатацію системних уразливостей для несанкціонованого проникнення в периметр корпоративних і державних мереж. Додатковим аспектом є деструктивні дії, спрямовані на копіювання, несанкціоновану публікацію чи передачу критично важливих відомостей третім особам. Суттєву роль у структурі таких загроз відіграє впровадження шкідливого програмного забезпечення – вірусів, троянських програм та криптолокерів (програм-вимагачів), що здатні зашифровувати інформаційні масиви з метою шантажу або встановлювати повний адміністративний контроль над інфікованою системою[24]. Соціальні інциденти становлять категорію загроз, що реалізуються

[22] Вавіленко А.І. Процес управління кіберінцидентами як необхідний етап в організації кібербезпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1 (38). С.64-71. DOI: 10.511369/2707-7276-2025-1(38)-6

[23] Саморай О.К., Семенюк О.О. Теоретичні і практичні підходи до розуміння кіберінцидентів та їхньої ідентифікації. *Європейський правничий часопис.* 2025. Вип. 8. С. 56-62. DOI 10.36919/3041-1149 (Print).8.2025.56-62

[24] Там само.

через методи цілеспрямованого психологічного впливу на суб'єктів інформаційних відносин для отримання несанкціонованого доступу до конфіденційних активів. Ключовим інструментарієм таких атак є фішинг – розсилка фальсифікованих електронних листів або повідомлень, які імітують верифіковані офіційні джерела з метою ексфільтрації облікових даних користувачів. Окреме місце займають різноманітні техніки соціальної інженерії, що базуються на прямій маніпуляції свідомістю для компрометації систем або викрадення інформації. Це може відбуватися через нав'язливу телефонну комунікацію (вішинг), створення шахрайських запитів або застосування методів обману в соціальних медіа, де зловмисники використовують когнітивні упередження та довіру користувачів для подолання встановлених протоколів безпеки. Фізичні інциденти класифікуються як події, наслідком яких є матеріальна деградація, механічне пошкодження або безпосередня втрата елементів інформаційних систем, мережевої інфраструктури та фізичних носіїв даних. Найбільш критичними проявами таких інцидентів є акти незаконного відчуження або навмисного знищення апаратних засобів, зокрема крадіжки мобільних робочих станцій, серверних модулів чи накопичувачів інформації. Суттєвий деструктивний потенціал мають також природні чинники форс-мажорного характеру – повені, пожежі, сейсмічна активність та інші катаклізми, здатні спричинити масштабні руйнування серверних приміщень і центрів обробки даних. Крім того, до цієї категорії відносять критичні збої в допоміжних інженерних системах, таких як модулі електроживлення або кондиціонування. Порушення регламентних умов експлуатації призводить до термічного перевантаження серверів, що тягне за собою апаратну відмову компонентів або безповоротну втрату цифрових масивів даних[25].

У науковому середовищі підхід до виявлення та аналізу кіберзагроз часто базується на гнучких евристичних моделях та предиктивній аналітиці, де головна увага приділяється динамічній природі атак і пошуку інноваційних методів захисту. Натомість законодавець оперує категоріями жорсткої регламентації та правової визначеності, фокусуючись на встановленні чіткої таксономії, часових лімітів інформування та суворого розподілу відповідальності між суб'єктами кібербезпеки. Таким чином, якщо науковці прагнуть розширити межі пізнання механізмів загроз, то правотворча позиція спрямована на створення стабільного, юридично значущого протоколу, що забезпечує невідворотність реагування в масштабах усієї держави.

Постановою Кабінету Міністрів України «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» від 26 листопада 2025 р. № 1533 було затверджено: Національний план реагування на кіберінциденти, кібератаки та кіберзагрози; критерії віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мету розкриття такої інформації; Порядок публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх

[25] Саморай О.К., Семенюк О.О. Теоретичні і практичні підходи до розуміння кіберінцидентів та їхнбої ідентифікації. *Європейський правничий часопис.* 2025. Вип. 8. С. 56-62. DOI 10.36919/3041-1149 (Print).8.2025.56-62

наслідків.[26] Зокрема у Національному плані законодавець визначив загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та суб'єктами забезпечення кібербезпеки, їх роль в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози. Дія цього Національного плану поширюється на основних суб'єктів національної системи кібербезпеки, суб'єктів національної системи реагування, органи державної влади, державні органи, органи місцевого самоврядування, операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури, інших суб'єктів забезпечення кібербезпеки, які відповідно до законодавства залучені до виконання завдань в рамках функціонування національної системи реагування. Окрім цього, законодавець розкриває такі поняття як: власна команда реагування на кіберінциденти, кібератаки та кіберзагрози (CSIRT); підрозділ з кіберзахисту; подія кібербезпеки; ризик кібербезпеки[27].

Процес протидії кіберзагрозам, атакам та інцидентам ініціюється стадією підготовки, у межах якої суб'єкти національної системи кібербезпеки здійснюють фундаментальні дослідження наявних типів кіберзагроз та розробляють превентивні механізми захисту. Цей етап передбачає формування комплексу організаційних, технічних і кадрових умов, необхідних для оперативного та результативного відбиття загроз. Зокрема, суб'єкти забезпечують системне планування заходів реагування, ґрунтуючись на результатах безперервного управління кіберризиками. Важливим аспектом є налагодження чіткої вертикальної та горизонтальної взаємодії між керівниками напрямів кіберзахисту, профільними підрозділами, внутрішніми командами реагування (CSIRT) та загальнодержавними структурами. Нормативна база підготовки включає розробку та постійну актуалізацію стандартних операційних процедур (SOP) для різних сценаріїв атак, що базуються на методичних рекомендаціях Адміністрації Держспецзв'язку. Окрему увагу приділено освітньому компоненту: організації диференційованого навчання персоналу, програма якого адаптується під функціональні ролі та професійну кваліфікацію співробітників. Технічна складова підготовчого етапу реалізується через створення необхідної інфраструктури для інтеграції локальних систем із державними технічними засобами реагування, зокрема через підключення до централізованої системи Державного центру кіберзахисту Держспецзв'язку[28].

Етап виявлення та аналізу базується на безперервному моніторингу систем для ідентифікації аномальної активності та індикаторів компрометації. Процес реагування активується як внутрішніми службами безпеки, так і через державні платформи обміну даними. У разі підтвердження інциденту суб'єкти безпеки

[26] Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 14.02.2026).

[27] Там само.

[28] Там само.

спільно з CERT-UA або профільними командами CSIRT класифікують його за національною таксономією та визначають рівень критичності: від 0 (білий) – некритичний, до 5 (чорний) – надзвичайний, що загрожує життю людей або функціонуванню держави. Процес інформування здійснюється в режимі реального часу через принцип «єдиного вікна» та платформу MISP-UA (керовану СБУ), з обов'язковим дотриманням протоколу конфіденційності TLP. Для об'єктів критичної інфраструктури та держустанов встановлено жорсткий регламент: повідомлення про значні інциденти має бути надіслане протягом однієї години. Подальша звітність перед Національним координаційним центром кібербезпеки передбачає чіткі часові межі: попередній звіт – 24 години, поточний – 72 години, та фінальний – протягом місяця. Це забезпечує злагоджену координацію між приватними, галузевими та національними центрами кіберзахисту для оперативної локалізації загроз[29].

4. Взаємодія суб'єктів забезпечення кібербезпеки щодо фіксації цифрових доказів та нейтралізації кіберінцидентів: емпіричний аналіз діяльності органів правопорядку

Відповідно до ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та загальний контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, загальну координацію суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; подає до Ради національної безпеки і оборони України пропозиції щодо оголошення кризової ситуації в кібербезпеці; координує реалізацію Стратегії кібербезпеки України, подає до Ради національної безпеки і оборони України пропозиції щодо формування та уточнення Стратегії, у тому числі з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive); визначає пріоритети, розробляє концептуальні засади та вносить Президентові України пропозиції щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони та забезпечує координацію суб'єктів сектору безпеки і оборони щодо їх проведення; координує стратегічні комунікації у сфері кібербезпеки[30].

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю;

[29] Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 14.02.2026).

[30] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; затверджує національний план реагування; затверджує загальні вимоги з кіберзахисту об'єктів критичної інфраструктури; затверджує порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (крім систем та об'єктів банків); встановлює порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, з правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності[31].

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування; Національний банк України; оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом[32].

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції: здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору[33].

Інституційне забезпечення кібербезпеки на рівні державних інституцій та критичної інфраструктури реалізується через обов'язкове створення профільних структурних одиниць – підрозділів з кіберзахисту. Законодавець у ст. 5-1 Закону «Про основні засади забезпечення кібербезпеки України» встановлює вимогу для органів державної влади, які оперують державними інформаційними ресурсами або таємною інформацією, не лише формувати такі підрозділи, а й призначати керівників з кіберзахисту з прямим підпорядкуванням.

[31] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

[32] Там само.

[33] Там само.

Аналогічні функції в органах місцевого самоврядування та на об'єктах критичної інформаційної інфраструктури покладаються на спеціально призначених відповідальних осіб. Особлива увага приділяється процедурі кадрового відбору: призначення керівника з кіберзахисту в державному секторі потребує обов'язкового погодження з Держспецзв'язку та проходження перевірки з боку Служби безпеки України. При цьому діє механізм «мовчазної згоди», якщо вмотивована відмова не була надана протягом місяця. Функціональне навантаження таких керівників передбачає здійснення безперервного керівництва, координації та контролю заходів кіберзахисту, що залишається незмінним пріоритетом навіть в умовах правового режиму воєнного стану. Це підкреслює стратегічну роль управлінської ланки у забезпеченні стійкості інформаційних систем до критичних впливів[34].

Відповідно до ст. 8 Закону національна система кібербезпеки України розглядається як багатоаспектна екосистема, що інтегрує широку сукупність суб'єктів та взаємоузгоджених заходів для комплексного захисту цифрового суверенітету. Її архітектура охоплює не лише технічні та інженерні рішення, а й заходи політичного, наукового, освітнього та правового характеру. Окреме місце в структурі системи посідає реалізація специфічних державних функцій: оперативно-розшукової, розвідувальної та контррозвідувальної діяльності, а також оборонних стратегій. Такий підхід забезпечує надійний криптографічний і технічний захист національних інформаційних активів та гарантує кіберстійкість об'єктів критичної інформаційної інфраструктури[35].

Координація зусиль у цій сфері покладається на ключових суб'єктів національної системи кібербезпеки, кожен з яких діє в межах визначеної законом компетенції. До основного інституційного ядра належать Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Національна поліція, Міністерство оборони разом із Генеральним штабом ЗСУ, а також розвідувальні органи. Окрім силового та технічного блоку, до системи інтегровані Національний банк України та Міністерство закордонних справ, що дозволяє забезпечувати економічну стабільність та дипломатичну підтримку кіберзахисту на міжнародній арені. Така розгалужена структура суб'єктів забезпечує цілісність державного реагування на кіберзагрози будь-якого рівня складності.

Ефективність функціонування національної системи кібербезпеки безпосередньо залежить від спроможності правоохоронних органів та суб'єктів державного контролю здійснювати кваліфікований збір, фіксацію та аналіз цифрових доказів. Провідна роль у цьому процесі належить Департаменту кіберполіції Національної поліції України, який забезпечує процесуальне супроводження кіберінцидентів у межах кримінального судочинства. Діяльність цього підрозділу спрямована на виявлення індикаторів компрометації (IoC) та вилучення цифрових слідів за допомогою спеціалізованих програмно-апаратних комплексів, що гарантують збереження автентичності даних через створення дзеркальних образів носіїв інформації. Важливою складовою є легалізація

[34] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

[35] Там само.

технічних параметрів атаки, де результати криміналістичного аналізу (forensics) трансформуються у юридично значущу доказову базу, що відповідає критеріям допустимості та цілісності.

Аналіз практичної діяльності Департаменту кіберполіції Національної поліції України у 2024 році свідчить про перехід до стратегії активного наступального протистояння загрозам у цифровому просторі. У звітному періоді зусилля підрозділу були зосереджені на превенції, детекції та нейтралізації кіберінцидентів, що підтверджується вагомими статистичними показниками оперативно-службової діяльності. Емпіричні дані вказують на високу інтенсивність боротьби з консолідованими злочинними угрупованнями. Зокрема, у 2024 році було ліквідовано 57 організованих груп, з яких 9 складали злочинні організації. До кримінальної відповідальності притягнуто 254 учас-ники, чия деструктивна діяльність охоплювала понад 1 000 епізодів. Загальна динаміка процесуальної діяльності ДКП за рік характеризується наступними показниками: реєстрація 2,5 тис. кіберзлочинів; оголошення про підозру 1,7 тис. особам у вчиненні 3,5 тис. правопорушень; завершення досудового розслідування у 4,4 тис. провадженнях; направлення до суду обвинувальних актів щодо понад 4 тис. злочинів. Ефективність функцій відшкодування збитків демонструє позитивну тенденцію: потерпілим забезпечено повернення понад 168,6 млн грн, що становить 42,5% від загальної суми завданої матеріальної шкоди.

Дослідження виявило адаптацію кіберзлочинності до актуальних соціальних трендів. Специфічними для періоду воєнного стану стали правопорушення, пов'язані з наданням фіктивних послуг чоловікам призовного віку, фальсифікацією волонтерської допомоги та шахрайством у сфері оренди житла для ВПО. У цьому сегменті правоохоронцями ідентифіковано та повідомлено про підозру понад 700 особам, а щодо 620 осіб матеріали передано до суду. В межах міжвідомчої взаємодії з НБУ та Держспецзв'язку було реалізовано механізм масового обмеження доступу до доменних імен, задіяних у фішингових кампаніях та соціальній інженерії.

Сучасний рівень інтеграції ДКП у світову архітектуру кібербезпеки підтверджується участю у 17 масштабних міжнародних поліцейських операціях, проведених спільно з іноземними партнерами та Європолом. Результатом став демонтаж інфраструктури кількох транснаціональних хакерських об'єднань. Важливим кроком у межах реалізації Стратегії кібербезпеки України стало отримання доступу до комунікаційної системи «Інтерпол I-24/7», що прискорило транскордонний обмін цифровими доказами.

Особливого значення набула екосистема «BRAMA», створена за координації кіберполіції як приклад державно-приватного партнерства. Проєкт об'єднав волонтерів та IT-фахівців для блокування ворожих джерел дезінформації. Ефективність платформи підтверджується динамікою охоплення аудиторії: на кінець 2024 року кількість активних підписників каналу протидії ворожому контенту досягла майже 148 тисяч осіб.

Таким чином, результати 2024 року підтверджують роль Департаменту кіберполіції як суб'єкта, що забезпечує не лише кримінально-правове переслідування зловмисників, а й безперервний моніторинг національних

комунікаційних мереж у режимі реального часу, інтегруючи сучасні технологічні рішення в архітектуру національної безпеки[36].

Паралельно з поліцейським блоком, органи державного контролю, зокрема Державна служба спеціального зв'язку та захисту інформації України, виконують роль первинної ланки технічного реагування. Через Державний центр кіберзахисту та команду CERT-UA здійснюється моніторинг об'єктів критичної інфраструктури, фіксація лог-файлів та встановлення методичних стандартів збереження цифрової інформації. У випадках, коли кіберінцидент загрожує національній безпеці або територіальній цілісності, до процесу долучається Служба безпеки України. Її функції зосереджені на контррозвідувальній атрибуції атак, що дозволяє ідентифікувати причетність іноземних спецслужб або APT-угруповань. Координація між цими суб'єктами базується на принципі «ланцюжка зберігання» (chain of custody), де технічні дані, зібрані під час моніторингу, стають основою для експертних висновків. Таким чином, синергія правоохоронних та контролюючих органів створює надійний механізм використання електронних доказів, що забезпечує невідворотність відповідальності за правопорушення у кіберпросторі.

Сучасний етап гібридної агресії проти України характеризується подальшою ескалацією в кіберпросторі, що підтверджується даними аналітичного звіту Державної служби спеціального зв'язку та захисту інформації України за перше півріччя 2025 року. Ключовою особливістю звітного періоду стала висока ступінь координації кібероперацій із конвенційними військовими діями, зокрема ракетно-дроновими ударами по об'єктах інфраструктури, що свідчить про інтеграцію цифрових атак у загальний стратегічний задум противника. Протягом першої половини 2025 року зафіксовано 3 018 кіберінцидентів, що відображає зростання інтенсивності на 17% порівняно з другим півріччям 2024 року. В аспекті якісної оцінки спостерігається трансформація структури інцидентів: при загальному збільшенні кількості атак середнього рівня критичності зафіксовано зниження частки критичних та високих інцидентів. Така тенденція є прямим наслідком превентивного посилення національних систем кіберзахисту. Розподіл цілей кібератак демонструє пріоритетність впливу на систему державного управління та сектор безпеки. Найбільшого деструктивного тиску зазнали: органи місцевого самоврядування – 34%; сектор безпеки та оборони – 23%; урядові організації та центральні органи виконавчої влади – 19%. У структурі використовуваного інструментарію домінують фішинг (27%), інфікування шкідливим програмним забезпеченням (21%) та компрометація облікових записів (5,4%). Характерною ознакою звітного періоду стало використання високотехнологічних методів проникнення хакерськими угрупованнями, афілійованими з ГУ ГШ ЗС РФ. Зокрема, зафіксовано активну експлуатацію Zero-Click вразливостей, які не потребують взаємодії з користувачем для інфікування системи. Основними векторами атак залишаються поштові платформи Roundcube та Zimbra, а також використання легітимних хмарних сервісів (Dropbox, Google Drive, Cloudflare)

[36] Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : звіт від 31.01.2025. Офіційний сайт Кіберполіції України. URL: https://cyberpolice.gov.ua/news/zvit-pro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 17.02.2026).

для прихованої доставки шкідливого контенту[37]. Окрему наукову увагу привертає зафіксоване CERT-UA використання технологій штучного інтелекту для генерації адаптивних фішингових повідомлень та автоматизації розробки експлуатаційного коду. Це свідчить про якісний стрибок у технологічній оснащеності суб'єктів кіберагресії. Незважаючи на зростаючу інтенсивність викликів, рівень резистентності державних і приватних інституцій продемонстрував стійку позитивну динаміку.

Фундаментом для цих змін стала імплементація положень Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», що регламентує розбудову мережі регіональних та секторальних команд реагування (CSIRT). Важливим етапом інституційної трансформації стало реформування CERT-UA у статус національного CSIRT, що забезпечило централізацію координаційних процесів та підвищило оперативність реагування на значні кіберінциденти[38].

ВИСНОВКИ

Дослідження продемонструвало, що в сучасних умовах «пермакриз» кібербезпека трансформувалася з вузькотехнічної дисципліни у багатоаспектне соціально-правове явище. Наукові підходи (зокрема концепції Індустрії 5.0 та когнітивної безпеки) акцентують увагу на захисті не лише інфраструктури, а й свідомості людини як головного об'єкта деструктивного впливу. Встановлено, що ключовим для розуміння галузі є трирівневе трактування кіберпростору (апаратний, програмний, інформаційний рівні), де безпека забезпечується через сталий розвиток і своєчасну нейтралізацію загроз на кожному з етапів.

Аналіз нормативної бази свідчить про системність зусиль держави у розбудові правового фундаменту кіберзахисту. Простежується перехід до жорсткої регламентації процедур реагування. Створення Національного плану реагування та запровадження обов'язкових посад керівників з кіберзахисту з прямим підпорядкуванням Держспецзв'язку та СБУ завершило формування вертикалі управління, що забезпечує стійкість державних інформаційних ресурсів навіть в умовах воєнного стану.

Емпіричні дані свідчать про експоненціальне зростання вітчизняного ринку кібербезпеки (з 32 млн дол. у 2016 р. до 138 млн дол. у 2024 р.). Україна перетворилася на глобальний R&D-полігон, де специфіка воєнного стану стимулювала домінування сегмента кіберрішень (57% ринку) над сервісами. Прогнозоване досягнення відмітки у 209 млн дол. до 2029 року та розвиток екосистем на кшталт «BRAMA» підкреслюють формування автономної та високотехнологічної індустрії, здатної забезпечити цифровий суверенітет держави в умовах глобального інформаційного протистояння.

[37] Фішинг, Zero Click-експлойти, AI-атаки: тенденції кіберзагроз в Україні у 2025 році. IT Ukraine. 07.10.2025. URL: https://itukraine.org.ua/fishing-zero-click-eksplojti-ai-ataki-tendentsiyi-kiberzagroz-v-ukrayini-u-2025-rotsi/ (дата звернення: 17.02.2026).

[38] Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 17.02.2026).

Узагальнення представлених теоретичних положень, нормативно-правового аналізу та емпіричних даних дозволяє сформулювати низку тез: 1. З огляду на активне використання AI для автоматизації атак і захисту, критично важливим є дослідження юридичних аспектів «автономної кібервійни». Пріоритетним є аналіз імплементації європейського AI Act у національне законодавство та розробка етичних протоколів застосування алгоритмів у діяльності правоохоронних органів. 2. Трансформація кіберзагроз у площину когнітивної війни (FIMI – Foreign Information Manipulation and Interference) вимагає перегляду класичних підходів. Наступні дослідження мають зосередитися на розробці методів захисту від маніпуляцій свідомістю, де цифрові технології використовуються як інструмент руйнування соціальної довіри. 3. Після законодавчого закріплення створення кібервійськ (кінець 2025 р.), актуальним стає наукове обґрунтування їхнього статусу, розробка доктрин ведення наступальних операцій у цифровому просторі та механізмів залучення «кіберрезерву» з-поміж цивільних фахівців. 4. Враховуючи масову цифровізацію та використання хмарних сервісів (Dropbox, Google Drive, Cloudflare) як векторів атак, перспективним є дослідження гармонізації національних стандартів безпеки IoT-пристроїв із міжнародними вимогами, що закладено в планах реагування. 5. Необхідно глибше дослідити механізми стимулювання вітчизняного ринку кібербезпеки. Пріоритетом є розробка моделей державно-приватного партнерства, де приватний сектор стає не лише постачальником послуг, а й інтегрованим елементом національної системи реагування. 6. Зважаючи на розвиток квантових обчислень, науковий інтерес становить перехід об’єктів критичної інфраструктури на постквантові алгоритми шифрування, що стане ключовим викликом для національної безпеки вже у найближчі роки.

АНОТАЦІЯ

Здійснено комплексне дослідження інституційних та правових засад функціонування національної системи кібербезпеки України. Проаналізовано еволюцію наукових підходів до дефініції ключових категорій галузі, зокрема понять «кіберпростір» та «кібербезпека», у контексті людиноцентричної парадигми та Індустрії 5.0. Особливу увагу приділено трансформації вітчизняного законодавства протягом 2016–2025 років, зокрема впровадженню Національного плану реагування на кіберінциденти та реформуванню CERT-UA у національний CSIRT. На основі актуальних емпіричних даних за 2024 та перше півріччя 2025 року висвітлено динаміку кібератак, проаналізовано роль Департаменту кіберполіції та Держспецзв’язку у забезпеченні цифрової стійкості держави. Деталізовано чотирирівневу модель класифікації кіберінцидентів та розкрито механізми збору цифрових доказів у межах кримінального судочинства. Виокремлено стратегічну роль державно-приватного партнерства та міжнародної співпраці через системи Інтерполу та Європолу. Обґрунтовано перспективи подальшого розвитку галузі, включаючи створення кібервійськ та імплементацію штучного інтелекту в архітектуру національної безпеки.

Література

1. Огляд ринку кібербезпеки в Україні : звіт / DataDriven, підкомітет з кібербезпеки EBA, CyberTech комітет Асоціації IT Ukraine за сприяння Аспен Інституту Київ, за підтримки Проєкту USAID. Січень 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 10.02.2026).
2. Екзистенційні виклики перед Україною. Демографія. *DeepState*. 23.09.2023. URL: https://deepstateua.com/iekzistientsialni-vikliki-ukrayini-chastina-i-diemoghrafiia/ (дата звернення: 11.02.2026).
3. Бондаренко В. Кібербезпека: роль держави у захисті суспільства та окремої особистості у збереженні міжетнічного миру. *Аспекти публічного управління*. 2020. Т. 8, № Спец. вип. 1. С. 18–21. DOI: 10.15421/152031
4. Попова Д. В. Кібербезпека в епоху Індустрії 5.0: нові виклики та можливості. *Економічний вісник Донбасу*. 2024. № 3. С. 203–216. DOI: https://doi.org/10.12958/1817-3772-2024-3(77)-203-216
5. Костроміна М. О. Кіберстійкість і кібербезпека: у чому різниця? *Сучасний захист інформації*. 2022. № 4. С. 71–75. DOI: 10.31673/2409-7292.2022.040012
6. Бєлкін Л. М. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Юридичний вісник. Повітряне і космічне право*. 2022. № 3. С. 78–86. DOI: 10.18372/2307-9061.64.16893
7. Форос Г. В. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128–134. DOI: https://doi.org/10.18524/2411-2054.2019.33.162068
8. Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. Vol. 5, № 2. С. 134–144. DOI: https://doi.org/10.20535/2411-1031.2017.5.2.136981
9. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. Вип. 1. С. 75–86. DOI: https://doi.org/10.31866/2617-796x.1.2018.147257
10. Дзюндзюк В. Б. Кібербезпека як один з пріоритетів національної політики. *Державне будівництво*. 2020. № 2. С.1-19. DOI: 10.34213/db.20.02.01
11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 14.02.2026).
12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).
13. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021 (рішення РНБО від 14.05.2021). URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 14.02.2026).
14. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення: 14.02.2026).
15. Живило Є. О., Ромашко І. В. Протокол спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти, а також при усуненні їх наслідків. *Системи управління, навігації та зв'язку*. 2024. Вип. 1. С. 66–76. DOI: 10.26906/SUNZ.2024.1.066
16. Федик В. Р., Денисенко Г. В. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об'єктах критичної інфраструктури:

реагування на кіберінциденти та менеджмент кризових ситуацій. *Інформація і право*. 2024. № 1. С. 195–202. DOI: 10.37750/2616-6798.2024.1(48).300822

17. Кінзерявий В., Гнатюк В. Базові показники ефективності роботи команд реагування на кіберінциденти. *Безпека інформації*. 2014. Т. 20, № 2. С. 193–196.

18. Сахарова О. Б., Близнюк І. Л. Виявлення та реагування на кіберінциденти і кібератаки як заходи запобігання кіберзлочинності. *Наука і правоохорона*. 2023. Вип. 2. С. 220–231. DOI (Issue): https: //doi.org/10.36486/np.2023.2(60)

19. Гарасимчук О. І., Костишин Т. А., Любчик О. О., Швед М. Є. Розробка вдосконаленої методики оповіщення населення про кіберінциденти. *Інформатика та математичні методи в моделюванні*. 2025. Т. 15, № 2. С. 187–195. DOI 10.15276/imms.v15.no2.187

20. Вавіленко А. І. Процес управління кіберінцидентами як необхідний етап в організації кібербезпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1 (38). С. 64–71. DOI: 10.511369/2707-7276-2025-1(38)-6.

21. Саморай О. К., Семенюк О. О. Теоретичні і практичні підходи до розуміння кіберінцидентів та їхньої ідентифікації. *Європейський правничий часопис*. 2025. Вип. 8. С. 56–62. DOI: 10.36919/3041-1149(Print).8.2025.56-62.

22. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 14.02.2026).

23. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : звіт від 31.01.2025. *Офіційний сайт Кіберполіції України.* URL: https://cyberpolice.gov.ua/news/zvit-pro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 17.02.2026).

24. Фішинг, Zero Click-експлойти, AI-атаки: тенденції кіберзагроз в Україні у 2025 році. *IT Ukraine.* 07.10.2025. URL: https://itukraine.org.ua/fishing-zero-click-eksplojti-ai-ataki-tendentsiyi-kiberzagroz-v-ukrayini-u-2025-rotsi/ (дата звернення: 17.02.2026).

25. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 17.02.2026).

Information about the authors:
Spivak Maryna Viktorivna,
Doctor of Political Sciences, Professor,
Professor of the Department of Administrative Law and Process
National Academy of Internal Affairs,
1, Solomjanska Square, Kyiv, 03035, Ukraine

Dubina Oleh Mykolaiovych,
PhD, Head of the 4th division of the cybercrime counteraction
Department (in the city of Kyiv) of the
Cyberpolice Department of the National Police of Ukraine,
10, Akademika Bohomoltsia St, Kyiv, 01024, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-18

ОКРЕМІ ПРОБЛЕМИ ЦИФРОВОЇ ІНФОРМАЦІЇ ТА ДОСТОВІРНОСТІ, ДОПУСТИМОСТІ ЦИФРОВИХ ДОКАЗІВ

Стратонов В. М., Басиста І. В., Гутник А. В.

ВСТУП

Для формування належної доказової бази надважливо не лише зібрати певну сукупність інформації, а основний акцент слід зробити на таких обставинах, які прогнозовано дозволять такій сукупності відповідати вимогам, які наявні у чинному кримінальному процесуальному законодавстві до доказів.

Отож варто розрізняти терміни «докази» та «інформація». Маємо і такі ситуації (мова про різнопланові порушення), за існування яких є велика доля ймовірності, що здобуто лише інформацію, яка фактично у цьому статусі й залишиться, бо не має шансу іменуватися допустимим та достовірним доказом.

Маємо правову невизначеність у чинному кримінальному процесуальному законодавстві, яка «позбавляє суд та учасників кримінального провадження бути впевненими у правильності правових результатів своїх дій та рішень: щодо електронних (цифрових) доказів – у допустимості цифрової інформації як доказу в кримінальному провадженні»[1]. Частково допомагають практикам поради із Протоколу Берклі, але коли ж слід до нього звертатися?

Сучасний цифровий розвиток дозволяє з упевненістю вести мову не лише про цифрові докази, а й про те, що у найближчому часі виникне необхідність пошуку нових найменувань для інформації, її слідів та доказів[2].

Авторами поставлено собі за мету, на основі аналізу доктринальних підходів, судової практики, наявних практично-орієнтованих порад, не лише окреслити окремі проблеми цифрової інформації та достовірності, допустимості цифрових доказів, а й узагальнити кілька дієвих правил перевірки і підтвердження достовірності цифрової інформації.

---

[1] Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 274. DOI: https://doi.org/10.31359/9786178612139

[2] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 110–112. DOI: https://doi.org/10.31359/9789669982940

Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 200. DOI: https://doi.org/10.31359/9786178612139

1. Інформація чи докази? Електронна (і), цифрова (і), електронно-цифрова (і)?

Не вперше задаючись таким питанням[3], та як воно вже перебувало у полі зору Афоніна Д.С., Гаврилюк Л.В., Глинської Н.В., Гловюк І.В., Зозулі Н.,

[3] Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: журнал. Серія Право. 2024. Вип. 17 (29). С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 1 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

Глинська Н. В., Клепка Д. І. Основні аспекти стратегії унормування інституту цифрових доказів в кримінальному процесуальному законодавстві. *Питання боротьби зі злочинністю.* 2023. Вип. 46. С. 49. DOI: https://doi.org/10.31359/2079-6242-2022-46-49

Басиста І.В., Гутник А.В. Цифрова інформація та цифрові докази з відкритих джерел: окремі теоретичні та практичні проблеми. Цифровізація кримінального провадження: стан та перспективи: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р./ редкол. Н.В. Глинська, Д.І. Клепка, А.А. Барабаш. НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 21–24. DOI: https://doi.org/10.31359/9786178411565

Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л.В. Гаврилюк, І.В. Басиста, Д.С. Афонін, А.В. Шевчишен та ін.; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178

Басиста І.В., Гутник А.В., Хитра А.Я. Окремі складові до алгоритму процесуальної діяльності залучених у кримінальне провадження уповноважених суб'єктів, які працюють із відкритими джерелами цифрової інформації у перебігу розслідувань, зокрема злочинів проти миру, безпеки людства та міжнародного правопорядку. Українська кримінальна юстиція у пост/воєнній парадигмі: матеріали X (XXIII) Львівського форуму кримінальної юстиції (м. Львів, 19–20 вересня 2024 року) / упорядник І. Б. Газдайка-Василишин. Львів: ЛьвДУВС, 2024. С. 14-20. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8323/1/19-20_09_2024.pdf

Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747

Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні: дис. … д-ра юрид. наук: 12.00.2009. МВС України. Дніпропетров. держ. ун-т внутр. справ. Дніпро, 2018. 648 с.

Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. 408 с. DOI: https://doi.org/10.31359/9789669982940

Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС.* 2023. № 3(102). С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43

Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право.* 08.05.2018. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_ zmin_do_protsesualnogo_zakonodavstva

Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 256–260. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58

Каланчі І.Г., Клепки Д.І., Коваленка А.В., Скрипника А.В., Столітнього А.В., Стратонова В.М., Хитри А.Я, Цехана Д.М. та інших вчених, але і не спостерігаючи певних зрушень у чинному законодавстві, підкреслимо, що очевидно національним орієнтиром у цій царині поки що є лише настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, які містить Національний стандарт України ДСТУ ISO/IEC 27037:2017, який чинний від 01.01.2019 року та покликаний допомогти «організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями»[4]. Не дивлячись на те, що у інших галузевих законах все ж йде мова про «електронні докази»[5], у аналізованому стандарті згадуються виключно «цифрові докази» і про це вже підкреслювали автори[6]. В силу такого стану справ і у процесуальних документах, і у судових рішеннях, як і у оприлюднених науково-практичних позиціях суддів у слововжитку превалює «електронний»[7], бо передбачувано, що якщо цивільний процесуальний закон оперує цим поняттям, а у кримінальному процесуальному наявна із цього приводу прогалина, то її заповнюють шляхом описаної рецепції. Але така ситуація є не зовсім вірною, про що вже також йшла мова[8].

Зазначений вище стандарт, вміщуючи настанови для роботи із конкретними пристроями, як от: носій для зберігання цифрових даних, використовуваний у стандартних комп'ютерах, мобільні телефони, персональні цифрові помічники персональні електронні прилади (PEDs), карти пам'яті, мобільні

---

[4] ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

[5] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/1618-15?find=1&text=електронні+#w1_11

[6] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія/ Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 74–75, 94. DOI: https://doi.org/10.31359/9789669982940

Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. С. 15. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178

[7] Суддя Верховного Суду Наталія Марчук розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні. *Судово-юридична газета* : веб-сайт. 05.02.2025. URL: https://sud.ua/uk/news/sud-info/322490-sudya-verkhovnogo-suda-natalya-marchuk-rasskazala-o-sudebnoy-praktike-po-otsenke-elektronnykh-dokazatelstv-v-ugolovnom-proizvodstve

Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

[8] Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: журнал. Серія Право.* 2024. Вип. 17 (29). С. 230. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

навігаційні системи, цифрові фото- та відеокамери, стандартний комп'ютер з мережевими з'єднаннями; мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах, а також прилади з функціями, подібними наведеним вище[9], все ж підкреслює, що запропонований перелік не претендує на вичерпність[10] і це логічне, у силу розвитку технологій. При цьому, у стандарті йдеться виключно про «цифровість», хоча, згоджуємося, що очевидно згодом з'являться не лише «нові види пристроїв, але і нові типи запису інформації»[11], як і її передавання[12], що зумовить пошук нових найменувань для інформації, її слідів та доказів. При цьому поділяємо наукову позицію щодо виокремлення окремого джерела таких цифрових доказів[13]. Також розділяємо процесуальні хвилювання тих наших колег, які аргументовано підкреслюють, що «відсутність належної правової регламентації певного правового явища, зокрема електронних (цифрових) доказів є окремим ризиком у правозастосуванні, оскільки правова невизначеність позбавляє суд та учасників кримінального провадження бути впевненими у правильності правових результатів своїх дій та рішень: щодо електронних (цифрових) доказів – у допустимості цифрової інформації як доказу в кримінальному провадженні»[14].

Ще однією спірною ситуацією є ототожнення цифрової інформації та цифрових доказів. У будь-якому випадку жодна інформація одразу не здатна набути процесуального статусу доказу у кримінальному провадженні. Цифрова інформація не є винятком. Лише перевірена та достовірна інформація, яка відповідає вимогам належності та допустимості, отримана в передбаченому КПК України порядку та може бути використана для встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню[15] має «процесуальний шанс»

[9] ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

[10] Там само.

[11] Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС*. 2023. № 3(102). С. 209–210. DOI: https://doi.org/10.32631/v.2023.3.43

[12] Коваленко А.В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 4 (100). С. 233. https://doi.org/10.33766/2524-0323.100.226-236

[13] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 110–112. DOI: https://doi.org/10.31359/9789669982940

Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 200. DOI: https://doi.org/10.31359/9786178612139

[14] Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 274. DOI: https://doi.org/10.31359/9786178612139

[15] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

іменуватися доказом. Отож варто розрізняти терміни «докази» та «інформація». Маємо і такі ситуації, за яких несанкціонований доступ до інформації, викрадення облікових записів, порушення умов надання послуг, як от користувацької угоди щодо веб-сайту або платформи, скрейпінг (коли це заборонено певною юрисдикцією) тощо унеможливлять набуття нею статусу доказу у кримінальному провадженні, тобто інформацію ми здобудемо, а допустимий та достовірний доказ – ні[16].

2. Достовірність та допустимість, як досягнути?

Здавалось би, такий процес збору інформації є не складним, проте нами вже була встановлена ціла низка наявних труднощів, зокрема і щодо помилкових підходів до збору цифрової інформації загалом, та із відкритих джерел, зокрема, ланцюга її збереження, відсутності спеціальних критеріїв для її оцінки тощо[17], виходячи із тих вимог, які окрім КПК України наявні і у Протоколі Берклі[18]. Дослідниці навіть запропонували вирішити проблеми із цифровими доказами через комплексний крок законодавця, як от Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо цифровізації кримінального провадження» та підготували і оприлюднили відповідну пояснювальну записка до його проєкту[19].

Суддя Верховного Суду, розповідаючи про судову практику щодо оцінювання електронних доказів у кримінальному провадженні в рамках курсу HELP «Кіберзлочинність та електронні докази», серед іншого важливого, підкреслювала, що не маловажливою є якість таких доказів, йшлося

---

[16] Басиста І.В., Гутник А.В. Цифрова інформація та *цифрові докази з відкритих джерел: окремі теоретичні та практичні проблеми. Цифровізація кримінального провадження: стан та перспективи*: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р./ редкол. Н.В. Глинська, Д.І. Клепка, А.А. Барабаш. НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 21–24. DOI: https://doi.org/10.31359/9786178411565

[17] Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького* : журнал. *Серія Право*. 2024. Вип. 17 (29). С. 229. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

[18] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

[19] Глинська Н.В., Клепка Д.І. Пропозиції до чинного кримінального процесуального законодавства України. Цифровізація кримінального провадження: стан та перспективи : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д.І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 165–173. DOI: https://doi.org/10.31359/9786178411565

безпосередньо про якість відеозапису. Також акцентовано, що «дублікат документа, а також копії інформації, у тому числі комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Прокурор має обґрунтувати походження електронних доказів та інші процесуальні питання, які стосуються наданих ним електронних доказів»[20].

Також судді звертають увагу на часті звернення сторони захисту, тобто клопотання про недопустимість таких доказів через те, що «певний файл кілька разів копіювався на різні носії (особливо якщо також змінювався формат цифрових даних), а тому він не є оригіналом і його цілісність порушено»[21]. І з цього приводу правильно підмічено, що за описаної ситуації сумнів має стосуватися не допустимості, а «достовірності (автентичності): чи дійсно електронний доказ є справжнім і чи можна йому довіряти»?[22]

І у продовження цілком вірно діагностовано про те, що для доведення достовірності доказу (принаймні відсутності втручання з боку сторони обвинувачення) має спосіб документування і забезпечення безперервності контролю над доказами з моменту їх отримання і до моменту їх дослідження в суді (тобто те, що в англомовній літературі називають «chain of custody», тобто ланцюг забезпечення зберігання речових доказів під час їх поетапної передачі, який має усунути будь-які розумні сумніви щодо можливої підробки з боку правоохоронців). На жаль, вітчизняна практика судів першої інстанції з аналізу ланцюга зберігання електронних доказів не є поширеною і поняття «chain of custody» рідко фігурує в рішеннях»[23].

У 2024 році авторським колективом науково-практичного порадника «Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі)», серед інших важливих порад для представників органів досудового розслідування, підкреслювалося про складові кожного із етапів chain of custody та його важливості загалом для набуття здобутою інформацією статусу доказу

[20] Суддя Верховного Суду Наталія Марчук розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні. *Судово-юридична газета* : веб-сайт. 05.02.2025. URL: https://sud.ua/uk/news/sud-info/322490-sudya-verkhovnogo-suda-natalya-marchuk-rasskazala-o-sudebnoy-praktike-po-otsenke-elektronnykh-dokazatelstv-v-ugolovnom-proizvodstve

[21] Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

Судді ККС ВС обговорили *проблемні питання допустимості електронних доказів під час судового розгляду. Верховний Суд* : веб-сайт. 28.10.2021. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/

[22] Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

[23] Там само.

у кримінальному провадженні[24]. І за ситуації дотримання всіх пропонованих рекомендацій отримаємо серед іншого процесуально-бажаного і процесуальну економію, адже під час правильного отримання цифрової інформації та належного поводження із нею взагалі може відпасти будь-яка потреба в призначенні та проведенні експертиз, бо саме такою є наявна практика Верховного Суду[25]. Вірно помітили автори, що через обраний підхід колегією суддів Третьої судової палати ККС ВС від 12.06.2024 у справі № 569/1908/23, для сторін сформувалася «чітка інструкція: якщо вони бажають заявити про недостовірність електронного доказу, таке питання може вирішуватися через проведення експертизи»[26]. Звісно є й такі ситуації у перебігу досудового розслідування та й судового розгляду, коли без проведення експертизи не обійтися, зокрема це пов'язане із deepfakes, участі ШІ тощо, про що теж більш розлоге вже йшлося[27].

З огляду значної кількості не вирішених проблем у цій царині вже навіть на монографічному рівні І.Г. Каланча запропонувала, серед іншого нагального, і комплекс алгоритмів пошуку та фіксації цифрових доказів та методику підтвердження їх автентичності та цілісності, вживаючи їх означення через словосполучення «докази електронної форми»[28].

Цікавим є досвід інших країн щодо використання цифрових доказів у кримінальному судочинстві. Г. Авдєєва та Е. Живуцька-Козловська встановили, що на сьогодні у США діють Federal Rules of Evidence[29], які

---

[24] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. https://rep.dnuvs.ukr.education/handle/123456789/4178

[25] Постанова колегії суддів Третьої судової палати ККС ВС від 12.06.2024 у справі № 569/1908/23.URL: https://reyestr.court.gov.ua/Review/119741340

[26] Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? JUSTTALK : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

[27] Басиста І.В., Гутник А.В., Хитра А.Я. Розпізнавання deepfakes як домінантна складова протидії інформаційним загрозам. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези III Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 року). Хмельницький : Видавництво НАДПСУ, 2025. С. 1097–1099.

Басиста І.В. Використання ШІ в криміналістичних цілях та співвіднесення із допустимістю зібраних доказів: огляд сучасного стану справ: розділ до монографії «Нове століття криміналістики та судових наук : Liber Amicorum на честь академіка В. Ю. Шепітька»: монографія / [М. Шепітько, А. Гетьман, В. Журавель та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого ; Нац. акад. прав. наук України ; Міжнар. конгрес криміналістів ; [за ред. М. В. Шепітька]. Харків : Право, 2026. С. 388–405. URL: https://dspace.nlu.edu.ua/handle/123456789/20701

[28] Каланча І.Г. Докази електронної форми у кримінальному процесі України: теорія та практика. Дисертація на здоб. ступеня д.ю.н. спец. 12.00.09. Національна академія внутрішніх справ, Київ, 2025. С. 34–35 та ін. https://elar.navs.edu.ua/handle/123456789/38317

[29] Federal Rules of Evidence amended to December 1, 2024. Legal Information Institute. URL: https://www.law.cornell.edu/rules/fre

кільканадцять разів змінювали та доповнювали. Опитуванням практиків у США було встановлено, що їм також «не вистачає знань про технічні характеристики цифрової інформації, правила її вилучення та зберігання. Слідчі потребують комплектів науково-технічних засобів для роботи з цифровими доказами, зокрема сумок Фарадея для ізолювання електронних пристроїв»[30]. При цьому важливо, що на відміну від нашого стану справ, ще «наприкінці XX ст. цифрові докази у США виокремили у групу доказів у зв'язку з особливостями їх створення, зберігання, виявлення, дослідження й оцінки їх допустимості та достовірності. 1995 р. спільними зусиллями правоохоронні органи США, Канади й деяких країн Європи створили міжнародну організацію з комп'ютерних доказів (англ. International Organization on Computer Evidence, IOCE)[31], а 1998 р.– Наукову робочу групу з дослідження цифрових доказів (англ. Scientific Working Group on Digital Evidence, далі – SWGDE)[32], яка об'єднала роботу правоохоронних, академічних і комерційних організацій у галузі цифрової криміналістики з метою розроблення міждисциплінарних посібників і стандартів щодо відновлення, збереження й дослідження цифрових доказів. Група SWGDE розробила основні стандарти та принципи роботи з цифровими доказами, що забезпечує належність і допустимість цих доказів у судочинстві»[33].

Із Federal Rules of Evidence (https://www.law.cornell.edu/rules/fre) слідує важливе правило, яке також констатоване і вище цитованими авторками та котре, на жаль, нехтується у національних розслідуваннях та судових розглядах, про допущення до дослідження цифрових доказів лише кваліфікованих IT-спеціалістів із метою максимального збереження їх цілісності[34].

3. Перевірка і підтвердження достовірності цифрової інформації

Перевірка достовірності цифрової інформації як елемент її доказового значення не є унікальною для кримінального процесу. У суміжних сферах (журналістика, OSINT, аналітика відкритих джерел) вже сформовані сталі підходи до верифікації цифрового контенту, які можуть бути адаптовані до потреб кримінального провадження. Наприклад, Етичний кодекс українського журналіста визначає, що найпершим обов'язком журналіста є повага до права громадськості на повну та об'єктивну інформацію про факти та події. Будь-яка тема потребує максимально повного набору фактів і думок. Тому завдання

[30] Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. Теорія та практика судової експертизи і криміналістики. 2023. Вип. 1 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

[31] International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648

[32] Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/

[33] Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики.* 2023. Вип. 1 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

[34] Там само.

журналіста все це знайти в компетентних джерелах[35]. Серед ключових принципів медіаграмотності є «правило трьох джерел». Це правило зводиться до перевірки інформації у мінімум трьох різних (за назвою, формою власності, редакційною політикою, географічним розташуванням) джерелах[36]. Схожий принцип використовують OSINTери – «трикутник перевірки» (Verification Triangle). Суть підходу – перевірити інформацію щонайменше з трьох різних джерел або точок зору: (1) оригінальні документи чи офіційні дані; (2) незалежні відкриті джерела (новини, бази даних, свідки); (3) технічні чи цифрові підтвердження (геолокація, метадані, фото/відеоаналіз). Тільки коли трикутник «замикається» – можна говорити, що факт підтверджено. Автори наводять приклад, що для початку аналізують джерело публікації, далі шукають інші підтвердження, на останок здійснюють цифрову перевірку [37].

Способи перевірки цифрової інформації на достовірність у кримінальному провадженні також надавались нами раніше[38]. Аналізуючи достовірність результатів OSINT у судовій практиці, І. Главюк пропонує під час роботи з відкритими джерелами визначити, чи є інформація або твердження в цифровому контенті на перший погляд надійними, шляхом перегляду та оцінки контенту, а також контекстуальної інформації, що міститься у файлі. Зокрема, це перевірка вбудованих метаданих, пов'язаної інформації та джерела. Цей процес повинен включати спробу ідентифікувати оригінальне джерело матеріалу, що може вимагати відстеження походження даних в Інтернеті, особи, яка завантажила їх, або автора[39].

Тож, з урахуванням цих висновків, з метою підтвердження чи спростування достовірності цифрової інформації пропонуємо адаптований під кримінальне провадження «трикутник перевірки» цифрової інформації на достовірність. Запропонований нами підхід фактично формує рівневу модель перевірки

---

[35] Кодекс етики українського журналіста. *Комісія журналістської етики* : веб-сайт. URL: https://cje.org.ua/ethics-codex/?fbclid=IwY2xjawPJ59NleHRuA2FlbQIxMABicmlkETF4d1FuTWloZlk1T3ZEN1pwc3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHsqw8h9Oh1aWfNOZBnZqXuxSBrJIRYAiNvwPx76s8XnuKMKV4mdz3vTw1Xb0_aem_YGU4piOQHM4oz1Zfvz92Jw

[36] Майданюк В. Правило трьох джерел: чому важливо перевіряти інформацію з різних, незалежних джерел. *Онлайн-медіа Дослідницько-аналітичної групи «ІнфоЛайт»*. 29.05.2025. URL: https://infolight.in.ua/2025/05/29/pravylo-troh-dzherel-chomu-vazhlyvo-pereviryaty-informatsiyu-z-riznyh-nezalezhnyh-dzherel/

[37] Трикутник перевірки інформації в OSINT: як відрізнити факт від маніпуляції. *InsightOps* : веб-сайт. 26.08.2025. URL: https://insightops.com.ua/2025/08/26/%D1%82%D1%80%D0%B8%D0%BA%D1%83%D1%82%D0%BD%D0%B8%D0%BA-%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D1%96%D1%80%D0%BA%D0%B8-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-%D0%B2-osint-%D1%8F%D0%BA/

[38] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванн : колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. С. 100.

[39] Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2025. Випуск 91: частина 4. С. 255. DOI https://doi.org/10.24144/2307-3322.2025.91.4.35

цифрової інформації, яка охоплює як змістовну, так і технічну складову цифрового доказу.

Першим кроком є *перевірка джерела публікації.* Що розуміти під «аналізом джерела» пояснено у п.177 Протоколу Берклі. Рекомендації щодо ідентифікації і перевірки першоджерела і змісту (включаючи місце події, дату і приблизний час) можна знайти у Посібнику з Верифікації[40].

У цьому блоці звернемо увагу тільки щодо проблем встановлення автора цифрової інформації. Так, у п. 177 Протоколу Берклі зазначено, що «…Інтернет-середовище створює труднощі для аналізу джерел, оскільки багато джерел є анонімними або псевдонімними …[41]. Наприклад, є випадки, коли автор цифрової інформації видає себе за іншу особу. Так, підозрюваний з метою приховання вбивства та дезорієнтації правоохоронних органів організував поїздку до Єгипту, штучно створивши собі алібі щодо перебування за межами України у момент вчинення злочину. Перебуваючи в м. Шарм-ель-Шейх, він від імені потерпілого публікував повідомлення та фото в соціальній мережі Фейсбук, які мали створити уявлення, що потерпілий живий і самостійно залишив територію України, чим намагався приховати реальну дату та обставини вчинення вбивства[42]. Аналізуючи цю ухвалу у іншому дослідженні, ми висловлювали свої застереження що використання одного ізольованого доказу, зокрема даних про місце перебування особи, є недостатнім для достовірного підтвердження алібі та потребує перевірки у сукупності з іншими доказами[43].

Можуть бути і інші ситуації, наприклад коли цифрова інформація публікується від імені фейкової особи. Наприклад, у січні 2024 року з метою компрометації журналістів створено фейкове видання, у редакції якого зазначено вигаданих осіб з фотографіями, які згенерував штучний інтелект[44]. Публікація від імені вигаданої особи це те ж саме що і публікація від імені невідомої особи. Також уважно слід відноситись до баз-даних, які невідомо ким створені та адмініструються. Наприклад, база-даних «Миротворець». Дані з цієї мережі можуть не відповідати, окрім інших вимог, вимозі достовірності (неможливо

[40] Посібник з Верифікації. Редактор: Крейг Сільверман, Інститут Пойнтера. Редагування та адаптацію перекладу на українську мову здійснено Українською Асоціацією Видавців під керівництвом Олексія Погорелова Переклад, літературне редагування та верстка В'ячеслав Білоусов Фінальна верстка – Європейський центр журналістики. С. 106–109. URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf

[41] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. С. 92. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

[42] Ухвала Печерського районного суду м. Києва від 17.03.2016 року у справі № 757/12089/16-к. URL: http://reyestr.court.gov. ua/Review/56950544

[43] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. С. 56.

[44] Романюк А. Метод «гнилого оселедця»: хто і навіщо атакує журналістів. *Детектор медіа* : веб-сайт. 16.01.2025. URL: https://detector.media/blogs/article/221791/2024-01-16-metod-gnylogo-oseledtsya-khto-i-navishcho-atakuie-zhurnalistiv/

встановити хто, коли та для чого публікував інформацію, яка лежить в основі досьє, хто наповнює базу)[45]. Є також випадки, коли власник сайту відомий, однак, через співпрацю з анонімними джерелами виникають сумніви щодо достовірності інформації. Наприклад, приватний сайт-парсер YouControl, який раніше використовував у своїй роботі тільки державні реєстри додав базу даних «Миротворець». Тож використання інформації із таких баз даних для доказування несе певні ризики[46]. Аналогічно, неможливо беззастережно довіряти інформації, опублікованій ворогом, адже є непоодинокі випадки викривлення чи вигадання інформації, яка публікується на його офіційних сайтах.

У п. 177 Протоколу Берклі також зазначено, що хоча визначення авторства є корисним, втім його відсутність, як правило, не є критичним для встановлення автентичності онлайн-елемента[47]. Таким чином, у сучасних міжнародних підходах акцент зміщується з ідентифікації автора цифрового контенту на встановлення автентичності самого цифрового об'єкта та цілісності інформації. Однак, у деяких категоріях кримінальних правопорушень, зокрема під час перевірки достовірності відео жорстокого поводження над твариною, встановлення особи автора є однією із обставин, що підлягає доказуванню.

Наступним кроком є пошук *підтвердження у інших джерелах*. Для цього слід провести слідчі або негласні (слідчі) розшукові дії. Також можна перевірити доказову інформацію з використанням відкритих джерел (медіа, соціальні медіа, веб-сайти, бази даних, офіційні дані тощо[48]). Під час пошуку підтверджень у інших джерелах, як ми зазначали вище, у журналістів є стандарт перевірки якнайменше в трьох різних джерелах[49].

---

[45] Басиста І., Гутник А. Використання інформації з бази даних Центру «Миротворець» у перебігу досудового розслідування: окремі аспекти. *Держава і суспільство: сучасні виклики та пошук рішень* : Збірник матеріалів ІІІ Всеукраїнської науково-теоретичної конференції, 16 травня 2024 р. К.: КТГГ, 2024. С. 397.

[46] Басиста І.В., Гутник А.В. Цифрова інформація та цифрові докази з відритих джерел: окремі теоретичні та практичні проблеми. *Цифровізація кримінального провадження: стан та перспективи* : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В . Глинська (голов. ред.), Д. І . Клепка, А. А . Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В. В . С ташиса НАП рН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 21.

[47] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. С. 92. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

[48] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкірідзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. С. 23–30. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178

[49] Посібник з Верифікації. Редактор: Крейг Сільверман, Інститут Пойнтера. Редагування та адаптацію перекладу на українську мову здійснено Українською Асоціацією Видавців під керівництвом Олексія Погорелова. Переклад, літературне редагування та верстка – В'ячеслав Білоусов. Фінальна верстка – Європейський центр журналістики. С. 105. URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf

Підтвердження певної інформації можна знайти у матеріалах журналістських розслідувань. Наприклад, на підставі фактів, оприлюднених у журналістському розслідуванні щодо діяльності на території одного з монастирів Голосіївського району міста Києва підпільного навчального закладу СБУ розпочали досудове розслідування за ч. 1 ст. 436-1 КК[50].

Однак, для того, щоб ця інформація стала доказом, її слід «легалізувати». Уповноважений суб'єкт має фактично повторно її зібрати за допомогою засобів і способів, що визначені КПК. Орієнтовний алгоритм «легалізації» матеріалів журналістського розслідування та блогів пропонує А. Коваленко. Автор резонно зазначає, що матеріал журналістського розслідування перед використанням повинен бути оціненим з точки зору належності, допустимості і достовірності[51]. Адже опублікованими можуть бути замовні чи неправдиві матеріали.

Закінченням перевірки є *цифрова перевірка.* Сюди можна віднести технічний аналіз та верифікацію метаданих[52], дослідження хеш-значень для підтвердження цілісності, оцінка технічних параметрів пристрою, експертиза тощо. Про деякі із цих процесів вже йшла мова у попередньому підрозділі.

ВИСНОВКИ

Отож, інформація одразу не здатна набути процесуального статусу доказу у кримінальному провадженні. Цифрова інформація не є винятком. Лише перевірена та достовірна інформація, яка відповідає вимогам належності та допустимості, отримана в передбаченому КПК України порядку та може бути використана для встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню має «процесуальний шанс» іменуватися доказом. При цьому, кваліфіковані ІТ-спеціалісти повинні залучатися на допомогу слідчому, детективу до відповідних оглядів, обшуків, для відшукання цифрових слідів тощо.

Розділяємо наукову позицію щодо виокремлення окремого джерела цифрових доказів та про правову невизначеність у кримінальному процесуальному законодавстві у царині допустимості цифрової інформації, як доказу в кримінальному провадженні.

Перевірка і підтвердження достовірності цифрової інформації у кримінальному провадженні має здійснюватися як багаторівневий процес, що поєднує аналіз джерела, пошук підтверджень у незалежних джерелах та технічну (цифрову) перевірку. Адаптація підходів, сформованих у журналістиці, OSINT, до вимог кримінального процесу дозволяє мінімізувати ризики використання недостовірних даних.

---

[50] Розпочато досудове розслідування за фактами, *оприлюдненими журналістами Слідство.Інфо, щодо підпільної школи на території монастиря. Офіс Генерального прокурора* : веб-сайт. 07.01.2026. URL: https://gp.gov.ua/ua/posts/rozpocato-dosudove-rozsliduvannya-za-faktami-oprilyudnenimi-zurnalistami-slidstvoinfo-shhodo-pidpilnoyi-skoli-na-teritoriyi-monastirya

[51] Розслідування колабораційної діяльності : практ. посібник / Є.О. Письменський, С.В. Головкін, А.В. Коваленко, В.В. Коваленко. Київ: ВД Дакор, 2024. С. 182–183.

[52] Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*, 2025. *Серія ПРАВО*. Випуск 91: частина 4. С. 257. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35

АНОТАЦІЯ

Запропонована публікація є продовженням серії авторських науково-практичних роздумів щодо розмежування сукупності інформації від сукупності доказів. Вкотре аргументовано, що екстраполюючи ці висновки на цифрову інформацію, варто не лише знати межу, яка відділяє цифрову інформацію від статусу цифрового доказу, а й розуміти, як уникати тих процесуальних та інших порушень, які не дозволять цифровій інформації іменуватися допустимим та достовірним доказом.

Зроблено спробу частково заповнити правову невизначеність, яка має місце у чинному кримінальному процесуальному законодавстві, порадами із Протоколу Берклі задля забезпечення допустимості цифрової інформації, як доказу в кримінальному провадженні. Також узагальнено кілька дієвих правил перевірки і підтвердження достовірності цифрової інформації та продовжено прогнози щодо наслідків сучасного цифрового розвитку для доказового права загалом та кримінальної процесуальної діяльності зі збору, перевірки та оцінки цифрової інформації зокрема.

Література

1. Federal Rules of Evidence amended to December 1, 2024. Legal Information Institute. URL: https://www.law.cornell.edu/rules/fre

2. International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648

3. Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/

4. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики.* 2023. Вип. 1 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

5. Басиста І., Гутник А. Використання інформації з бази даних Центру «Миротворець» у перебігу досудового розслідування: окремі аспекти. *Держава і суспільство: сучасні виклики та пошук рішень:* Збірник матеріалів ІІІ Всеукраїнської науково-теоретичної конференції, 16 травня 2024 р. К.: КТГГ, 2024. С. 395–398.

6. Басиста І.В. Використання ШІ в криміналістичних цілях та співвіднесення із допустимістю зібраних доказів: огляд сучасного стану справ: розділ до монографії «Нове століття криміналістики та судових наук : Liber Amicorum на честь академіка В. Ю. Шепітька»: монографія / [М. Шепітько, А. Гетьман, В. Журавель та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого ; Нац. акад. прав. наук України ; Міжнар. конгрес криміналістів ; [за ред. М.В. Шепітька]. Харків : Право, 2026. С. 388–405. URL: https://dspace.nlu.edu.ua/handle/123456789/20701

7. Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: журнал. Серія Право.* 2024. Вип. 17 (29). С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

8. Басиста І.В., Гутник А.В. Цифрова інформація та цифрові докази з відкритих джерел: окремі теоретичні та практичні проблеми. *Цифровізація кримінального провадження:* стан та перспективи : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р./ редкол. Н.В. Глинська, Д.І. Клепка, А.А. Барабаш. НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 21–24. DOI: https://doi.org/10.31359/9786178411565

9. Басиста І.В., Гутник А.В., Хитра А.Я. Окремі складові до алгоритму процесуальної діяльності залучених у кримінальне провадження уповноважених суб'єктів, які працюють із відкритими джерелами цифрової інформації у перебігу розслідувань, зокрема злочинів проти миру, безпеки людства та міжнародного правопорядку. *Українська кримінальна юстиція у пост/воєнній парадигмі:* матеріали X (XXIII) Львівського форуму кримінальної юстиції (м. Львів, 19–20 вересня 2024 року) / упорядник І. Б. Газдайка-Василишин. Львів: ЛьвДУВС, 2024. С. 14-20. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8323/1/19-20_09_2024.pdf (дата звернення: 19.01.2026).

10. Басиста І.В., Гутник А.В., Хитра А.Я. Розпізнавання deepfakes як домінантна складова протидії інформаційним загрозам. *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану :* тези III Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 року). Хмельницький : Видавництво НАДПСУ, 2025. С. 1097–1099.

11. Басиста І.В., Дроздов О.М., Стратонов В.М. Провадження за нововиявленими обставинами та провадження за виключними обставинами. Особливості, перебіг та взаємозв'язок. *Науковий вісник Херсонського державного університету. Серія юридичні науки Випуск 2 Гельветика, 2023.* С. 10. https://lj.journal.kspu.edu/index.php/lj/issue/view/ 11/55 (дата звернення: 19.01.2026).

12. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкірідзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178 (дата звернення: 19.01.2026).

13. Глинська Н. В., Клепка Д. І. Основні аспекти стратегії унормування інституту цифрових доказів в кримінальному процесуальному законодавстві. *Питання боротьби зі злочинністю.* 2023. Вип. 46. С. 48–66. DOI: https://doi.org/10.31359/2079-6242- 2022-46-49 (дата звернення: 19.01.2026).

14. Глинська Н.В., Клепка Д.І. Пропозиції до чинного кримінального процесуального законодавства України. *Цифровізація кримінального провадження: стан та перспективи :* матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д.І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 165–173. DOI: https://doi.org/10.31359/9786178411565 (дата звернення: 19.01.2026).

15. Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2025. Випуск 91: частина 4. С. 251–259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35 (дата звернення: 19.01.2026).

16. Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi (дата звернення: 19.01.2026).

17. Military offences and war crimes: background, theory and practice / Ed. by V.M. Stratonov. – Riga, Latvia: «Baltija Publishing», 2023. 876 p

18. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

19. Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. Українське право. 08.05.2018. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva (дата звернення: 19.01.2026).

20. Каланча І.Г. Докази електронної форми у кримінальному процесі України: теорія та практика. Дисертація на здоб. ступеня д.ю.н. спец. 12.00.09. Національна академія внутрішніх справ, Київ, 2025. 617 с. URL: https://elar.navs.edu.ua/handle/123456789/38317

21. Коваленко А.В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 4 (100). С. 226–236. DOI: https://doi.org/10.33766/2524-0323.100.226-236

22. Кодекс етики українського журналіста. *Комісія журналістської етики :* веб-сайт. URL: https://cje.org.ua/ethics-codex/?fbclid=IwY2xjaw PJ59NleHRuA2FlbQIxMABicmlkETF4d1FuTWloZlk1T3ZEN1pwc3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHsqw8h9Oh1aWfNOZBnZqXuxSBrJIRYAiNvwPx76s8XnuKMKV4mdz3vTw1Xb0_aem_YGU4piOQHM4oz1Zfvz92Jw

23. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139

24. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

25. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. 204 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%D0%93%D1%83%D1%82%D0%BD%D0%B8%D0%BA%2C%20%D0%A5%D0%B8%D1%82%D1%80%D0%B0_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_21_06_2022.pdf

26. Майданюк В. Правило трьох джерел: чому важливо перевіряти інформацію з різних, незалежних джерел. *Онлайн-медіа Дослідницько-*

аналітичної групи «ІнфоЛайт» : веб-сайт. 29.05.2025. URL: https://infolight.in.ua/2025/05/29/pravylo-troh-dzherel-chomu-vazhlyvo-pereviryaty-informatsiyu-z-riznyh-nezalezhnyh-dzherel/ (дата звернення: 19.01.2026).

27. Науково-практичний коментар Кримінального процесуального кодексу України – науково-методична робота. Станом на 14 квітня 2024 року / За заг. ред. Стратонова В.М. Київ: Видавничий дім «Професіонал», 2024. 1208 с. (дата звернення: 19.01.2026).

28. Посібник з Верифікації. Редактор: Крейг Сільверман, Інститут Пойнтера. Редагування та адаптацію перекладу на українську мову здійснено Українською Асоціацією Видавців під керівництвом Олексія Погорелова Переклад, літературне редагування та верстка – В'ячеслав Білоусов Фінальна верстка – Європейський центр журналістики. 130 с. URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf (дата звернення: 19.01.2026).

29. Постанова колегії суддів Третьої судової палати ККС ВС від 12.06.2024 у справі № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340 (дата звернення: 19.01.2026).

30. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/ 2022/03/ Berkeley-ProtocolUkrainian.pdf (дата звернення: 19.01.2026).

31. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747 (дата звернення: 19.01.2026).

32. Розпочато досудове розслідування за фактами, оприлюдненими журналістами Слідство.Інфо, щодо підпільної школи на території монастиря. *Офіс Генерального прокурора :* веб-сайт. 07.01.2026. URL: https://gp.gov.ua/ua/posts/rozpocato-dosudove-rozsliduvannya-za-faktami-oprilyudnenimi-zurnalistami-slidstvoinfo-shhodo-pidpilnoyi-skoli-na-teritoriyi-monastirya

33. Розслідування колаборaційної діяльності: практ. посібник/ Є.О. Письменський, С.В.Головкін, А.В. Коваленко, В.В. Коваленко. Київ : ВД Дакор, 2024. 260 с.

34. Романюк А. Метод «гнилого оселедця»: хто і навіщо атакує журналістів. *Детектор медіа :* веб-сайт. 16.01.2025. URL: https://detector.media/blogs/article/221791/2024-01-16-metod-gnylogo-oseledtsya-khto-i-navishcho-atakuie-zhurnalistiv/

35. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. 408 с. DOI: https://doi.org/ 10.31359/ 9789669982940

36. Слінько Д. С, Слінько С. В., Стратонов В. М. Критерії процесуальної самостійності слідчого. *Наше право №1, 2023. С.35-41* http://nashe-pravo.unesco-socio.in.ua/wp-content/uploads/archive/NP-2023-1/NP-2023-1_044. pdf

37. Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні : дис. … д-ра юрид. наук: 12.00.2009. МВС України. Дніпропетров. держ. ун-т внутр. справ. Дніпро, 2018. 648 с. URL: https://dduvs.edu.ua/wpcontent/uploads/files/Structure/science/rada/dissertations/20/3.pdf

38. Стратонов В.М. Актуальні проблеми кримінального процесуального законодавства України в період воєнного стану. *Науковий вісник Херсонського державного університету. Серія: «Юридичні науки»* Випуск 4. 2025. С. 35-40. DOI https://doi.org/10.32999/ksu2307-8049/2025-4-6 (дата звернення: 19.01.2026).

39. Стратонов В.М. Повноваження слідчого судді у кримінальному провадженні. *Криміналістика і судова експертиза:* міжвідом. наук.-метод. зб. / Київський НДІ судових експертиз; редкол.: Д. В. Журавльов (голов. ред.), О. Г. Рувін (заст. голов. ред.) та ін. Київ : Видавництво Ліра-К, 2021. Вип. 66. С. 264-272 (дата звернення: 19.01.2026).

40. Стратонов В.М. Дзюрбель А.Д. Використання штучного інтелекту та інформаційних можливостей у створенні профіля злочинця. *Науковий вісник Херсонського державного університету. Серія: «Юридичні науки»* Випуск 5. 2024. Гельветика, 2024. С. 21-27. DOI: https://doi.org/10.32999/ksu2307-8049/2024-5-4 (дата звернення: 19.01.2026).

41. Стратонов В.М. Використання цифрових технологій у виявленні та документуванні фактів експлуатації людини під час збройних: доказова база в міжнародних судах. *Вчені записки ТНУ імені В.І. Вернадского. Серія: юридичні науки* Том 36 (75) № 1. 2025. С. 173-178. DOI https://doi.org/10.32782/TNU-2707-0581/2025.1/28 30.pdf (дата звернення: 19.01.2026).

42. Стратонов В.М., Гончарова О.В Відмова прокурора від підтримання державного обвинувачення – навчально-методичний посібник. Харків: Право, 2020. 134 с.

43. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. *Верховний Суд :* веб-сайт. 28.10.2021. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (дата звернення: 19.01.2026).

44. Суддя Верховного Суду Наталія Марчук розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні. *Судово-юридична газета* : веб-сайт. 05.02.2025. URL: https://sud.ua/uk/news/sud-info/322490-sudya-verkhovnogo-suda-natalya-marchuk-rasskazala-o-sudebnoy-praktike-po-otsenke-elektronnykh-dokazatelstv-v-ugolovnom-proizvodstve (дата звернення: 19.01.2026).

45. Трикутник перевірки інформації в OSINT: як відрізнити факт від маніпуляції. *InsightOps :* веб-сайт. 26.08.2025. URL: https://insightops.com.ua/2025/08/26/%D1%82%D1%80%D0%B8%D0%BA%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D1%96%D1%80%D0%BA%D0%B8%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-%D0%B2-osint-%D1%8F%D0%BA/ (дата звернення: 19.01.2026).

46. Ухвала Печерського районного суду м. Києва від 17.03.2016 року у справі № 757/12089/16-к. URL: http://reyestr.court.gov.ua/Review/56950544

47. Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС.* 2023. № 3(102). С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43 (дата звернення: 19.01.2026).

48. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2013. Вип. 5. С. 256–260. URL: http://nbuv. gov.ua/UJRN/ Nvmgu_jur_2013_5_58 (дата звернення: 19.01.2026).

49. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 №1618-IV (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/1618-15?find=1&text=електронні+#w1_11 (дата звернення: 19.01.2026).

Information about the authors:
Stratonov Vasyl Mykolaiovych,
Doctor of Law, Associate Professor, honored lawyer of Ukraine,
Professor of the Department of National, International Law and Law Enforcement Kherson State University,
27, Universytetska st., Kherson, 73035, Ukraine

Basysta Iryna Volodymyrivna,
Doctor of Legal Sciences, Professor,
Member of the Academic Advisory Council under the Supreme Court,
Professor at the Department of Law and Public Administration
King Danylo University
35, Y. Konovaltsia st., Ivano-Frankivsk, 76018, Ukraine

Hutnyk Alina,
Doctor of Philosophy in Law
10, Tykhoho Str., Kalush, 77300, Ukraine

DOI https://doi.org/10.30525/978-9934-26-686-7-19

DIGITAL CRIMINALISTICS AS A STRATEGIC DIRECTION FOR THE DEVELOPMENT OF MODERN CRIMINALISTICS

Shevchuk V. M., Zatenatskyi D. V., Kolesnikova I. A.

INTRODUCTION

The modern stage of the development of criminalistics is characterized by global digitalization, which is not just a technical update, but a fundamental scientific prerequisite for the transformation of its theoretical foundations. In today's realities, the processes of digitization and digitalization are objective, inevitable, they cannot be stopped, because they are such that they reflect the objective requirements set forth by scientific, technical and social progress[1]. The transfer of information into digital form and digitization trends under such conditions are a new stage in the development of our society, they appear as a new era of development of the digital economy in Ukraine. They influence all spheres of activity of society and the state, including the activity of law enforcement agencies in the field of combating crime, modernize and update the development of legal science and criminalistics[2].

Under such circumstances, the processes of digital transformation of criminalistics, which create prerequisites for the development and formation of new criminalistic knowledge, become especially relevant. The essence of the digitization of criminalistics is the application of digital technologies to identify, research and secure evidence of a digital nature[3]. These processes affect the development of criminalistics as an applied science, which includes the latest methods of investigation related to digital information, as well as ways to detect and prevent them[4].

Digitization in criminalistics is first of all manifested in the integration of digital technologies in criminalistic activities, which includes the development and use of special methods, techniques and tools for working with digital evidence and

[1] Shevchuk, V., Zhuravel, V., Yevdokimenko, S., Yevdokimenko, S., Myshkov, Y. (2025). Forensic Examination and Criminalistics in Investigating War Crimes: European and Ukrainian Experiences. *Jurnal Media Hukum*, 32 (1), 59-77. DOI: https://doi.org/10.18196/jmh.v32i1.25056

[2] Шевчук В. М. Діджиталізація, цифровізація та технологізація криміналістики: проблеми сьогодення та перспективи майбутього. *Діджиталізація судово-експертної науки в умовах воєнного стану:* матеріали міжн. наукю-практ. конф. (8 листопада 2024 р., м. Харків). Харків: Право, 2024. С. 324-327.

[3] Shevchuk, V., Bululukov, O., Chornyi, H., Tyshchenko, O., & Baranchuk, V. Latest Criminalistic Tools and Technologies in the Investigation of Cybercrimes: International and Ukrainian Experience. *Law, State & Telecommunications Review*, 2025, *17* (2), 207-235. DOI: https://doi.org/10.26512/lstr.v17i2.55927

[4] Konovalova V.O., Shevchuk V.M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries of modern science: experience, approaches and innovations*: III International Scientific and Theoretical Conference, January 20, 2023. Amsterdam: European Scientific Platform. Pp. 73-77.

investigating crimes in the digital sphere[5]. It enables the search, retrieval, preservation and investigation of digital evidence for the detection, detection and investigation of criminal offences. Such processes created the prerequisites for the formation of a new strategic direction in criminalistics – digital criminalistics[6], the concept of which requires special scientific research and determination of the vector of prospects for its development in modern conditions and in the future[7].

1. Digital transformation of criminalistics – a scientific prerequisite and methodological basis for the formation of new criminalistic knowledge

Strategic planning in science allows not only to record current changes, but to anticipate the dynamics of crime through the creation of proactive models of law enforcement[8]. The strategic vector shifts the emphasis from " criminalistics of the past" (investigation by material traces) to " criminalistics of the future". This involves the development of theoretical models of criminal activity in cyberspace[9], forecasting ways to counter the investigation, and creation of algorithms for neutralizing methods of anonymization and data encryption.

It is believed that the digitization of criminalistics should include several aspects: 1) the use of digital technologies to increase the efficiency of the investigator's search and cognitive activity, effective organization of this activity at the modern level, optimization of the interaction of various bodies and institutions in the investigation of criminal offenses; 2) the use of information and communication (informational computer) technologies for the investigation of criminal offenses, which contributes to the algorithmization of the pre-trial investigation process as a whole and its individual stages; 3) solving didactic tasks in the field of training, retraining, advanced training of investigators, forensic investigators, forensic experts, exchange of experience[10] . In these directions, the processes of digital transformation of forensics in the modern conditions of hybrid warfare, taking into account the trends of Europeanization and technologization of our society, are taking place.

---

[5] Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики,* 4 (29), 2023, 19.

[6] Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал*. 2022. № 4. С. 378–380.

[7] Shevchuk, V., Zhuravel, V., Yevdokimenko, S., Yevdokimenko, S., Myshkov, Y. (2025). Forensic Examination and Criminalistics in Investigating War Crimes: European and Ukrainian Experiences. *Jurnal Media Hukum*, 32(1), 59-77. DOI: https://doi.org/10.18196/jmh.v32i1.25056

[8] Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: Proceedings of the 5th International scientific and practical conference (August7-9, 2022). Sci-conf.com.ual. Lviv, Ukraine. 2022. Pp. 896–903. https://sci-conf.com.ua/wp-content/uploads/2022/08/MODERN-RESEARCH-IN-WORLD-SCIENCE-7-9.08.2022.pdf

[9] Баранов Р. О. Протидія легалізації злочинних доходів та фінансуванню тероризму з використанням віртуальних валют. *Державне управління: удосконалення та розвиток.* 2016, 6. URL: http://www.dy.nayka.com.ua/?op=1&z=978 (дата звернення: 19.02.2026).

[10] Думчиков М.О. Процеси діджиталізації і криміналістика: реторспективний аналіз. *Криміналістика і судова експертиза*. 2020. Вип. 65. 2020. Вип. 65. С.100-108.

Digital transformation leads to a transition from the traditional paradigm of the study of material traces to the study of information and computer patterns of the emergence and existence of evidentiary information. The development of modern criminology and its digital transformation today is not a opportunistic response to technical progress, but represents a global change in the scientific paradigm[11]. Traditional criminalistics, which for decades was based on the theory of the reflection of the material world in a material environment, is now faced with the phenomenon of «digital reality». This makes it necessary to review the methodological basis in this field of knowledge.

The scientific premise of this transformation is the convergence of criminalistics with informatics and the theory of systems and forecasting. If previously the object of knowledge was a physical object (media), now it is an information process – an algorithm for creating, transmitting, and saving data. This requires the development of a new theory of the digital trace picture, which includes not only data directly, but also metadata that allows establishing the context of the event without physical contact with the attacker[12]. The methodological basis of this process is based on the integration of special knowledge in the field of information technology, cyber security and programming into the system of criminalistic knowledge. The formation of new knowledge occurs through the expansion of the object sphere: from physical media to virtual environments. This requires the development of new research methods, which became the basis for distinguishing digital forensics as a new scientific direction in the system of criminalistic knowledge and forensic sciences.The methodological basis of the formation of new knowledge in this context is structured according to three vectors: a) epistemological; b) systemic and structural; c) axiomatic. The epistemological vector is associated with a change in the nature of cognition. In digital forensics, the path from «trace» to «fact» is through software mediation. The expert does not observe the object directly; he sees the result of the algorithm. Therefore, the methodology necessarily includes verification of the toolkit – proving that the software does not distort the original digital matter. The system-structural vector affects the formation of knowledge about the «virtual environment» as a space for committing a crime. This environment has the following properties: cross-border, anonymity, easy changeability and the possibility of instant destruction of evidence. Accordingly, criminalistic knowledge is adapted to work with «ephemeral» objects that exist only under voltage (random memory) or in cloud storage. The axiomatic vector involves a revision of basic criminalistic categories, because digital transformation introduces new axioms: the «copy identity principle», according to which a duplicate digital file is legally and technically identical to the

[11] Шевчук В. М., Тищенко О. І. Технологізація криміналістики, судової експертизи і кримінального провадження в сучасних умовах цифровізації. *Юридичний науковий електронний журнал.* № 12. 2024. С. 375-380. URL: http://www.lsej.org.ua/12_2024/88.pdf

[12] Shevchuk, V., Zatenatskyi, D., Kapustina, M., Kolesnikova, I., & Shevchuk, A. Criminalistics Means and Methods of Combating Ecocide in the Modern Conditions of Military Threats. *Journal of Environmental Law and Policy*, 2024, 04 (03), 82-120. DOI: https://doi.org/10.33002/jelp040304

original, provided the hash sum matches. This extends identification methods by adding algorithmic methods for comparing large data sets[13].

Thus, digital transformation acts as a catalyst for the creation of digital criminalistics, as a strategic direction for the development of modern criminalistics, which becomes an integrative bridge between traditional forensics and computer science. It provides a transition from «technical assistance» to the investigator to the formation of a new strategy and approach to the process of evidence collection, investigation, and trial, where digital information is the central link of evidence[14].

Today, the tasks of criminalistics, depending on theoretical-cognitive and applied problems, can be divided into three levels: 1) tasks aimed at improving the theoretical and methodological foundations of criminalistics, the formation and development of the general theory of criminalistics; 2) tasks aimed at improving law enforcement practice, that is, scientific and practical developments for the development of the theory of criminology and for the practice of law enforcement, taking into account the modern realities of consent; 3) tasks aimed at developing and implementing forensic innovations into practice, as well as improving the strategy of combating crime by means of criminalistics. In this context, we are talking about the formation and the need to develop new directions in criminalistics, in particular, criminalistic innovations, forensics strategy, military forensics, medical, nuclear and digital criminalistics[15]. Therefore, an urgent issue today is the need to develop scientific recommendations regarding the use of modern digital technologies, work with certain types of digital evidence, procedural processing of detected digital traces of a criminal offense; the need to ensure the integrity and authenticity of digital evidence by applying modern information protection methods[16]. Therefore, digital criminalistics is a strategic direction of research in the system of criminalistic knowledge and modern criminalistics [17].

In view of the above, it can be seen that the formation of strategic directions of research in criminalistics is a response to the systemic crisis of traditional approaches, which arose as a result of the technological gap between the methods of committing criminal offenses and the methods of their investigation. The formation

[13] Shevchuk V. M. Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*. 2020, 27, 2, 170–183. URL: http://visnyk.kh.ua/en/article/metodologichni-problemi-formuvannya-ponyatiynogo-aparatu-kriminalistichnoyi-innovatiki

[14] Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 208 с.

[15] Шепітько В.Ю. Теоретико-методологічна модель криміналістики та її нові напрями. *Те- орія та практика судової експертизи і криміналістики*. 2021. Вип. 3 (25). С. 10–20.

[16] Демидова Є.Є. Тенденції розвитку цифрової криміналістики: виклики та перспективи для органів кримінальної юстиції. *Проблеми законності.* 2025. № 168. С. 164–182.

[17] Цифрова криміналістика та її роль у формуванні доказової інформації в умовах воєнних дій : монографія / [В. Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова] ; за ред. В. Ю. Шепітька ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2025. 200 с. С. 174.

of strategic directions contributes to the synthesis of criminalistic knowledge with the achievements of various technical, legal (criminalistic) sciences, neurosciences, biotechnology and artificial intelligence. This makes it possible to create complex methods where, for example, the digital profile of the offender is integrated with his biometric and psychological characteristics, forming a complete identification system in the absence of physical contact traces.

Strategic research allows criminalistics to go beyond the local investigation. In the conditions of hybrid threats and cross-border crime, the unification of standards for working with digital evidence is of strategic importance, which ensures their recognition by international judicial authorities. This turns forensics into a tool of international security and protection of national sovereignty in the information space. The strategic direction of such research makes it possible to increase efficiency and optimize the process of criminal proceedings, resource and procedural support. Determining strategic priorities allows you to concentrate intellectual and financial resources on the development of domestic expert software and the training of a new type of personnel – digital criminalistics or criminalistic-analysts capable of working with Big Data and cloud technologies[18].

Therefore, such studies ensure the viability and innovative essence of criminalistic science, transforming it from a theoretical-descriptive discipline to a fundamental projective-applied science that effectively counters crime with criminalistic means, methods and technologies to ensure national security, defense and state sovereignty in the era of global digitalization and military realities.

The value of digital criminalistic for the formation of a criminalistic strategy lies in the transition from a tactical response to individual episodes to the creation of a comprehensive model of anticipatory documentation, investigation and prevention of criminal activity. Within the framework of further scientific research, this aspect is revealed through the following conceptual provisions.

First, the change of the object of strategic planning. Under such circumstances, criminalistic science ceases to be a science of «things» and becomes a science of «connections and algorithms». This approach necessitates the formation of a new normative model of criminal proceedings, where digital information is recognized as primary, and not derived from physical media. If previously the traditional strategy was built around the physical representation of the crime scene, today the digital transformation moves the center of strategic planning to the digital (virtual) space, where digital information and digital evidence become the key element, that is, digital traces are the key source of evidentiary information. The object of strategic analysis is not a single file or document, but the correlation of gigantic arrays of data from various sources (billing systems, cameras with FaceID, registries). Strategic planning is aimed at the development of intelligent search algorithms in these arrays, which makes it possible to separate evidentiary information from informational noise. The strategy in today's environment is now aimed at intercepting and preserving data before it is remotely destroyed.

[18] Shevchuk, V., Morozova T., Chornyi, H., Nehrebetskyi V., and Slobodeniuk, I. (2025). Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues. *International Annals of Criminology*, 2025. Pp. 1-19. DOI: https://doi.org/10.1017/cri.2025.10090

Secondly, projectivity and intellectualization. They act as the highest steps in the evolution of digital criminalistics, transforming it from a retrospective discipline to a strategic-level proactive tool. Projectivity (from the Latin projectio – projection forward) defines the ability not only to analyze and investigate past events, but also to project (model) possible scenarios of criminal activity and methods of their neutralization. Digital criminalistics introduces the method of criminalistic forecasting into the strategy. The analysis of digital traces allows not only to identify patterns of behavior of criminals, but also to predict possible threat vectors (use of weapons of mass destruction, cyber attacks, etc.) and to prepare means and methods of their neutralization in advance[19]. This turns the strategy from figuratively speaking "catch-up" to "preemptive". Intellectualization of digital forensics means the integration of AI and machine learning technologies[20] in the methodology of criminalistic research, which fundamentally changes the role of the forensic expert and specialist in criminal proceedings. It makes it possible to use neural networks for automatic detection of anomalies, hidden connections between figures and recognition of behavior patterns that a person is physically unable to notice. Digital forensics is becoming the intellectual core of national security, as it ensures the state's ability to legally and technically respond to threats arising in a high-tech environment.

Third, evidentiary reliability in the long term. The development of a methodology for preserving the authenticity of digital evidence over the years (for example, for international tribunals) is of strategic importance. Forming a strategy for using blockchain technologies or creating public registries of hash sums of evidence ensures that digital data will not lose its power due to changes in software standards in the future. Effective application of the strategy involves harmonization of procedural legislation with international and European standards and domestic realities. This includes taking into account the international experience of using digital forensics tools and their ability to collect evidentiary information in pre-trial investigation, as well as the processes of its verification and legitimization of remote methods of evidence collection and recognition of the results of automated data analysis algorithms as independent elements of the investigation strategy and judicial review of court decisions.

The formation of strategic directions contributes to the synthesis of criminalistic knowledge with the achievements of neuroscience, biotechnology and artificial intelligence. This makes it possible to create complex methods where, for example, the digital profile of the offender is integrated with his biometric and psychological characteristics, forming a complete identification system in the absence of physical contact traces. Strategic research allows forensics to go beyond the local investigation. In the conditions of hybrid threats and cross-border crime, the unification of standards for working with digital evidence is of strategic importance, which ensures their recognition by international judicial authorities.

---

[19] Шевчук В. М. Криміналістика: традиції, новації, перспективи : добірка наук. пр. Харків : Право. 2020. 1280 с. с. 778. URL: http://library.nlu.edu.ua/POLN_TEXT/POSIBNIKI_2020/Kriminalistika_Shevchu k_2020.pdf.

[20] Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки і обороноздатності України. *Юридичний науковий електронний журнал.* № 6. 2024. С. 356–361.

Thus, a criminalistic strategy strengthened by a digital component becomes the foundation for building a system of national resilience, where every digital footprint is seen as a strategic resource for establishing the truth and restoring justice. The forensic strategy should combine the efforts of investigators, technology experts, intelligence (OSINT), blockchain technologies and significantly increase the level of work with evidentiary information, taking into account the predictive function of forensics. In this context, the importance of digital forensics lies in the creation of a single digital forensic space in Ukraine and the world, which will allow the exchange of information, strengthen international cooperation and quickly integrate data from various digital sources (drones, smartphones, satellites) into an integrated system of evidence of war crimes and effectively investigate them and form an evidence base for consideration in international and national courts.

The formation of strategic directions of research in modern criminalistics is a response to the systemic crisis of traditional approaches, which arose as a result of the technological gap between the methods of committing criminal activities and the methods of their investigation. Strategizing in forensics primarily helps in ensuring scientific prognostication. The strategic vector shifts the emphasis from «criminalistics of the past» (investigation by material traces) to «criminalistics of the future». This involves the development of theoretical models of criminal activity in cyberspace, forecasting methods of countering the investigation, and creating algorithms for neutralizing methods of anonymization and data encryption. This turns modern criminalistics into a tool for the international security of Ukraine's digital environment and the protection of national sovereignty in the information space.

2. Digital criminalistics: concepts and significance in the formation of evidentiary information in the conditions of hybrid warfare

In the modern conditions of martial law, the question of increasing the effectiveness of the investigation of modern crime, including war crimes and cybercrimes, using the tools of digital criminalistics[21]. Today's digital evidence is becoming a reliable means of recording and verifying real events, refuting disinformation, and identifying subjects acting remotely[22]. The process of forming evidentiary information in a digital environment is complicated by use opponent of methods of anonymization and destruction of digital traces. Under such circumstances, the trend of the formation of a new scientific direction – *digital criminalistics* [23].

[21] Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: Proceedings of the 5th International scientific and practical conference (August 7-9, 2022). Sci-conf.com.ua. Lviv, Ukraine. 2022. Pp. 896-903.

[22] Avdeeva G. Technological breakthrough in criminalistics and forensic examination : new horizons. *Archive of Criminology and Forensic Sciences*, 2025, 11(1), 100–110. https://doi.org/10.32353/acfs.11.2025.06

[23] Когутич І. І. Застосування цифрових технологій – новий напрям криміналістики. *Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79-84.

In the conditions of hybrid warfare, the importance of digital criminalistics is growing critically, as the line between a cyber attack, an information operation and a physical act of aggression becomes more and more transparent. It ensures the procedural fixation of immaterial objects (e-mails, metadata, log files), turning them into legitimate sources of evidence that meet the criteria of admissibility and reliability, facilitates the detection, recording and analysis of digital traces, assists in the investigation and prevention of criminal offenses, and also ensures the use of digital evidence in judicial proceedings and the process of proof. Digital criminalistics is basically understood as a system of scientific provisions and forensic means, methods and technologies aimed at detecting, recording and analyzing digital traces in order to establish the circumstances of the commission of a criminal offense.

In the specialized literature, various terms are used to denote this direction – «computer criminalistics»[24], «electronic criminalistics»[25] or «forensics in computer systems»[26], «digital criminalistics» (Digital Forensics, Digital Forensic Science or Digital Criminalistics)[27].

In the specialized literature, there are different approaches to defining the concept of digital forensics and its place in the system of forensics and criminalistic sciences. Some scientists point out that digital forensics is a separate branch of forensic science, which is a system of scientific methods for researching digital evidence in order to facilitate the detection and investigation of criminal offenses[28]. Others point out that digital criminalistics is related to the process of collecting, receiving, saving, analyzing and submitting digital data for the purpose of obtaining investigative information, evidentiary information and carrying out investigations and criminal prosecutions in relation to various types of criminal offenses[29], including war crimes committed by the occupying forces of the Russian on the territory of Ukraine.

Some sources indicate that digital forensics is «one of the branches of criminalistics that focuses on criminal procedural law and evidence regarding computers and related devices»[30], such as mobile devices (for example, phones and

[24] Полотай О.І. Комп'ютерна криміналістика: основні завдання та проблеми. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*": матеріали Міжн. наук. інтернет-конф. Тернопіль. Вип. 68. 2022. С. 29-30

[25] Заєць І. С. Перспективи криміналістики в умовах інформатизації суспільства. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід* : матеріали Міжнар. наук.-практ. круглого столу (Київ, 19 лют. 2020 р.). Київ : Нац. акад. внутр. справ, 2020. С. 77-81. С.79.

[26] Шепітько В., Шепітько М. Формування цифрової криміналістики як стратегічний напрямок розвитку науки. *XVII Medzinarodny Kongres Kriminalistika a Forenzne Vedy. Criminalistics and Forensic Expertology: Science, Studies, Practice*. XVII International Congress (September 16-17, 2021). Bratislava, Slovak Republic. 2021. С. 187-198.

[27] Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал*. 2022. № 4. С. 378–380.

[28] Степанюк, Р. Л. Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка. 2022. № 3 (99). С. 283-294. С. 290.

[29] Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*, 2022, (1), 176-180.

[30] Maras M.-H. Computer Forensic: Cybercriminals, Laws, and Evidence. Second Edition, 2014. 408 p. P. 29.

smartphones), game consoles and other devices that function through the Internet. In addition, digital forensics is related to the process of collecting, obtaining, preserving, analyzing and presenting electronic (digital) evidence in pretrial and judicial proceedings. Therefore, digital criminalistics can be a strategic direction in the development of criminalistic science[31] .

In view of the above, it can be asserted that the subject of digital criminalistic is the regularities of detection, recording, preliminary research, use of computer information, digital traces and means of their processing in order to solve the tasks of detection, investigation and prevention of criminal offenses, as well as the development of these regularities of technical means and methodological recommendations aimed at optimizing activities to combat criminal offenses in the digital space.

The object of digital criminalistics is, on the one hand, criminal offenses related to the use of computer (digital) technologies and social relations that arise in the course of detection, disclosure, investigation and prevention of criminal offenses, when detection, recording, research, use of computer information, digital traces and means of their processing is carried out, and on the other hand, the activities of law enforcement agencies in relation to the investigation of such criminal offenses and the issue of the development and application of forensic techniques, methods, means of using computer (digital) technologies in the fight against crime in the digital space.

Therefore, digital criminalistics is a branch of forensics that studies the patterns of occurrence and use of digital traces and, based on the knowledge of these patterns, develops technical means, techniques and methods for detecting, recording, extracting and researching digital information (evidence) and means of its processing for the purpose of disclosure, investigation and prevention of criminal offenses.

It is important for scientific research to take into account the relationship between digital forensics and the digitalization of forensics and forensic examinations. Thus, we believe that it is necessary to clearly distinguish digital forensics as a system, a field of criminalistic knowledge aimed at the study of digital traces, on the one hand, and on the other – the use of digital technologies in the investigation and judicial proceedings, that is, the process of digitization of forensics as a natural modern stage of its development and formation, which involves the introduction of digital technologies in various fields of forensic technology and forensic examination, to the very process of pre-trial investigation[32].

Regarding the relationship between digital criminalistics (properly computer-technical examination) and forensic examination, it is worth noting that they perform different functions in the process of collecting and analyzing evidence in criminal proceedings. So, in particular, digital criminalistics (computer forensics) primarily focuses on digital data, while forensics focuses on physical evidence, such as fingerprints, traces, and biological samples, etc. Also, experts in the field of computer

[31] Шепітько В., Шепітько М. Формування цифрової криміналістики як стратегічний напрямок розвитку науки. *XVII Medzinarodny Kongres Kriminalistika a Forenzne Vedy. Criminalistics and Forensic Expertology: Science, Studies, Practice*. XVII International Congress (September 16-17, 2021). Bratislava, Slovak Republic. 2021. С. 187-198. С. 192.

[32] Степанюк Р. Л. Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2022. № 3 (99). С. 283-294. С. 288.

and technical expertise have specialized knowledge in the IT field, while forensic scientists use various techniques from different fields of science.

In addition, digital criminalistics and computer-technical expertise, in its name, already has an emphasis on the fact that the mention is a technical expertise, which excludes it from the composition of forensic types of expertise defined by the law "On forensic expertise". And also, Art. 7 of this Law, it is stated that the performance of examinations can be entrusted to other specialists (experts) from the relevant fields of knowledge in the manner and under the conditions specified by this Law. Also in Art. 7 states that the basis for conducting a forensic examination is a contract with an expert or an expert institution, if the examination is carried out on the order of other persons. Although these fields are closely intertwined, their distinction is based on the object of research and methodology: forensic examination (in the classical sense) focuses on material traces of the real world (prints, biological samples, documents), while digital forensics works with virtual data stored on physical media. Its specificity lies in the fact that the evidence is intangible, easily changed and requires special software to extract it without violating its integrity. The main difference in functions: criminalistic identifies a person or object through physical properties, while digital forensics restores the chronology of actions and the content of information in the digital environment[33].

The connection between the use of special knowledge in the study of digital traces and the collection of evidentiary information, the determination of the possibilities of criminalistic research, the evaluation and use of the results of forensic examinations in evidence in the conditions of the activation of the use of digital technologies is important[34]. Currently, objects in digital form are submitted for forensic examination, both on individual data carriers and on computer systems. Therefore, in order to legally obtain digital traces, it is necessary to use relevant special knowledge, as well as to conduct forensic computer-technical examination and examination of telecommunication systems and means (examination of digital and analog devices)[35].

In today's military realities, digital criminalistics is a reliable tool in the system of ensuring national security and defense of Ukraine. Digital criminalistics in the conditions of the modern scientific paradigm should be considered as a complex system of theoretical provisions, criminalistic tools, technologies and methods of detection, fixation, extraction and research of digital traces that exist in virtual space or on physical media. In the context of doctoral research, it is important to emphasize that the object of knowledge here is not only "computer information", but digital

[33] Aharkova, O. I., Korosteleva, L. A., and Krasnopolskyi, V. E. The Use of Innovative Soft-ware Packages in Digital Forensics to Combat Crime in Ukraine. Sci. innov., 2025, 21(6), 60–67. https://doi.org/10.15407/scine21.06.060

[34] Shepitko V. Yu., Konovalova V.O., Shevchuk V.M. et. al. Scientific and technical support of investigative activities in the context of an adversarial criminal procedure. *Issues of Crime Prevention*. Vol. 1. № . 42. 2021. Pp. 92-102.

[35] Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. Право України. 2021. № 8. С. 12–27.

reality – a dynamic set of data, algorithms and network connections that reconstruct the circumstances of the event of a criminal offense[36] .

Digital criminalistics is important in the formation of evidentiary information in the conditions of hybrid warfare. It ensures the formation of an evidence base for legal responsibility for armed aggression and the commission of war crimes, where it is especially important to establish a cause-and-effect relationship between actions and consequences, which are accompanied by traces, including digital (metadata, IP address, code) and criminal actions of specific persons who committed such war crimes (military personnel, commanders of military units, military political leadership of the aggressor country etc.).

Hybrid warfare is accompanied by massive information and psychological operations (IPSO).In such situations, the role of digital forensics lies in the ability to disprove fake content (deepfakes, photo/video manipulation) by analyzing metadata, file structure and information distribution logs, which turns criminalistic computer-technical examination and examination of telecommunication systems and means into an effective tool for establishing the objective truth against propaganda. Digital evidence often exists in cloud storage, self-destructing messengers, or destroyed critical infrastructure. Digital forensics allows for the formation of an evidence base through remote methods of data extraction and recovery, which is critical when physical access to the scene is limited by combat operations.

The formation of evidentiary information in the conditions of war has a strategic goal – the presentation of evidence at the International Criminal Court (hereinafter referred to as the ICC). Digital forensics ensures data integrity and authenticity through the use of hash functions and digital signatures, ensuring that a digital copy from a crime scene (such as data from a drone or smartphone) has not been altered since recovery[37]. The value of the synergy of the technical and tactical direction lies in the integration of OSINT data into the classical process of proof. Digital criminalistics legitimizes data from satellites, social networks, and closed databases, turning disparate digital activity into a systematic evidence model of military aggression.

In the context of hybrid threats, the further development of criminalistics in the conditions of the information society, digitization and military realities of today is impossible without the wide use of innovative and fundamental knowledge in the field of digital criminalistics [38]. Today, forensics corresponds to the development of digital technologies, creating means and methods for the possibility of extracting

[36] Степанюк, Р. Л. Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2022. № 3 (99). С. 283-294. С. 288.

[37] Затенацький Д.В. Роль криміналістичної стратегії в розслідуванні воєнних злочинів в Україні. *Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє* : матеріали панельної дискусії VII Харківського Міжн. юрид. форуму 25 вересня 2023 року. Київ : Алерта, 2023. С. 33-38.

[38] Когутич І. І. Застосування цифрових технологій – новий напрям криміналістики. *Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79-84.

forensically significant information from a new type of media[39]. Thanks to scientific and technical progress, it is possible to use digital technologies in criminal proceedings, which speeds up the investigation process, allows more complete formation of the evidence base in the investigation of war crimes[40], and in the future should ensure the quality of the judicial review of proceedings and the prospects of court decisions, both in international and national courts.

Therefore, digital criminalistics is of great importance in the formation of evidentiary information in the conditions of hybrid warfare. It becomes a kind of digital tool that allows you to translate virtual and online acts of Russian military aggression into the plane of criminal procedural evidence, ensuring the inevitability of punishment for war crimes committed both in the physical environment and in cyberspace in the context of hostilities.

3. The role of digital criminalistics tools in the detection, recording and investigation of war crimes in Ukraine

Digital forensics tools are transforming the process of investigating war crimes, making it high-tech and cross-border. They make it possible to overcome difficulties in processing digital information and collecting digital evidence and, in turn, to form a reliable evidence base, which is the foundation for bringing to justice the highest political and military leadership of the aggressor at the international level. The role of digital forensics in the investigation of war crimes of the Russian Federation against Ukraine is determined by the need to process colossal data sets (Big Data) and the impossibility of traditional access to the locations of events in occupied territories or in active combat zones.

The main areas of application of the tools of digital criminalistics in the detection, recording and investigation of war crimes are: a) remote means and technologies for recording war crimes; b) digital data analysis and mobile forensics (Mobile Forensics); c) expert study of UAVs (Drone Forensics); d) 3D scanning and photogrammetry of the scene; e) use of blockchain technologies and cryptographic algorithms (hashing); g) application of artificial intelligence technologies, etc.

Remote means and technologies for recording war crimes make it possible to reconstruct the circumstances of shelling of civilian objects and identify the aggressor's units without the physical presence of an investigator at the scene. Digital criminalistics tools allow you to legitimize data from open sources (OSINT (Open Source Intelligence) technologies by analyzing social networks, Telegram channels, Maxar/Planet Labs satellite images, etc.The role of analytical platforms consists in verifying the authenticity of the content, establishing the exact time (timestamping) and geolocation of the event. This makes it possible to reconstruct the circumstances

[39] Борисова, К. Є., Світличний, В. А. Застосування цифрової криміналістики. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану*: тези доп. Міжнар. наук.-практ. конф.(м. Харків, 25 листоп. 2022 р.). Харків: ХНУВС, 2022. С. 83-84.

[40] Домашенко О. М. Проблемні питання використання цифрових доказів у криміналістиці. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці:* матеріали міжнар. «круглого столу» (Харків, 12.12.2019) / В. Шепітько, В. Журавель, В. Шевчук. Х. : Право, 2019. С. 52–55.

of shelling of civilian objects and to identify the aggressor's units without the physical presence of the investigator at the scene of the incident. Satellite reconnaissance and remote sensing of the Earth (Satellite Imagery) are becoming important. The role of satellite technologies (Maxar, Planet Labs, ICEYE) is to provide retrospective recording of landscape changes. This allows for documentary confirmation of: moments of mass burials (for example, the case of Buchi and Mariupol); the dynamics of civil infrastructure destruction as a result of artillery shelling; moving military equipment and deploying artillery positions in territories where investigators do not have physical access.

The analysis of digital data in criminal proceedings involves the use of software and hardware complexes (for example, Cellebrite UFED, MSAB Oxygen) and allows to extract data from phones, chest cameras and GPS navigators of captured or liquidated occupiers. Analysis of data from GPS-navigators and geotagging of photos allow you to reproduce the combat path of a specific unit. Such digital information is often the key to linking specific individuals to places of mass executions or torture in a certain period of time. Studying and analyzing chats in Telegram, WhatsApp or Signal (even deleted messages) allows you to identify the members of the groups, their callsigns and real identification data, which is often the only way to identify war criminals. Removed digital orders, screenshots of orders in messengers and recordings of conversations make it impossible for the defense to use the argument about "arbitrary actions of privates". This makes it possible to raise the level of responsibility to senior officers and plays a decisive role in revealing direct evidence: orders for executions, photo and video recordings of torture, as well as establishing the chain of command (command responsibility).

An important means of collecting evidentiary information by means of digital forensics is the forensic investigation of UAVs, which constitutes a new scientific direction, which is often called "Drone Forensics" in foreign literature. The formation of this direction as a system of scientific knowledge is a strategic task to ensure the completeness of the investigation of war crimes committed with the use of high-tech weapons.The object of Drone Forensics is a complex system that includes not only the aircraft itself, but also the ground control station (remote), mobile applications and cloud services of the manufacturer. Expert research allows you to extract: a) telemetry data: speed, height, angles of inclination and flight coordinates in real time; 2) metadata of media files: EXIF data of photos and videos containing exact geographical coordinates and time of shooting; 3) system logs: information about failures, critical commands and equipment identifiers (serial numbers of components), which allows you to track the supply chain of components to circumvent sanctions. A key role of Drone Forensics in the investigation of war crimes is the ability to retrospectively reconstruct the route. Specialized tools (eg VTO Labs) allow you to reconstruct the flight paths of kamikaze drones and reconnaissance UAVs. This is critical for fixing launch points from the territory of the Russian Federation or Belarus, which is direct evidence of aggression and violation of state sovereignty. Identifying the point of departure is direct evidence of an attack from a specific territory (for example, from the territory of the Russian Federation or the occupied territories of Ukraine), which is of critical importance for the legal qualification of the crime of aggression.

3D scanning and photogrammetry of the scene of the incident is an important area of application of the tools of digital **criminalistics** in the detection, recording and investigation of war crimes. The use of laser scanners and photogrammetry drones allows creating digital duplicates of destroyed objects (schools, hospitals, residential buildings). This provides "conservation" of the crime scene in virtual space, which allows ballistics and explosives examinations to be carried out years after the event, when the physical object can already be demolished or rebuilt. The use of drones for remote inspection of the scene of the incident allows for the creation of highly accurate orthophoto plans and 3D models of destroyed objects. Photogrammetric processing allows you to turn a series of pictures from a drone into a metrically accurate digital copy of a building. This allows ballistics experts to remotely calculate the angle of arrival of a projectile and identify the type of weapon without exposing themselves to danger under rubble.

The use of blockchain technologies and cryptographic algorithms (hashing) in digital forensics is a strategic response to the fundamental challenge of ensuring the authenticity and immutability of digital evidence over a long period of time (from the moment of extraction on the battlefield to presentation in the ISS). Cryptographic hashing performs the function of creating a unique digital fingerprint of any file or the entire image of the medium, which provides a guarantee of integrity and is of procedural importance. It is obvious that Any minimal change of at least one bit of information in the proof will lead to a complete change of the hash sum.This allows the expert to mathematically prove to the court that the provided copy of the data is bit-by-bit identical to the original, seized from the occupier or from the site of the shelling. Procedural significance – hashing becomes a mandatory element of the "chain of custody" (Chain of Custody), recording the state of digital information at every stage – from the inspection of the scene to the forensic examination. Cryptographic algorithms and blockchain transform digital forensics from a "method of technical analysis" to a system of guaranteed trust. In a strategic dimension, this allows Ukraine to build such a mechanism for gathering evidence, where the technological impossibility of falsifying data becomes the main argument of prosecution in international tribunals.

The use of artificial intelligence technologies has occupied a central place in military realities for collecting evidence of war crimes in digital forensics[41] . AI acts not only as a tool to speed up the expert's work, but also as a means of identifying hidden patterns inaccessible to human perception[42]. The use of artificial intelligence technologies has taken a central place in military realities, transforming digital forensics from the process of mechanical data collection into a system of intellectual analysis of large arrays of information (Big Data Forensics). In the conditions of war, the amount of digital data (video from drones, interceptions, satellite images) is so

[41] Dumchykov, M. O. Protsesy didzhytalizatsii i kryminalistyka: rektrospektyvnyi analiz. Kryminalistyka i sudova ekspertyza Forensics and forensic examination, 2020, 65, 100-108 in Ukrainian.

[42] Шевчук В. М., Авдєєва Г. К. Використання технологій штучного інтелекту та спеціальних знань у розслідуванні воєнних злочинів. *Правнича наука та законодавство України: європейський вектор розвитку в умовах воєнного стану* : монографія; Нац, акад. прав. наук України. Харків, 2023. С. 491–503.

colossal that traditional "manual" analysis becomes physically impossible. Therefore, the role of AI in collecting and analyzing digital evidence of war crimes is increasing[43].

It is believed that the process is a natural stage of development and formation of modern forensic knowledge[44] and involves the active implementation of digital technologies in various fields of criminalistics, forensic expertise and legal practice[45]. At the same time, it is important not to exaggerate the potential and advantages of artificial intelligence: it is worth considering its individual shortcomings. We see that the use of AI in judicial proceedings and law enforcement activities is permissible only under the condition of mandatory observance of the principles of the rule of law, basic human rights, respect for his honor and dignity, equality before the law and the court, proportionality, competition between the parties, transparency, impartiality and justice, etc[46].

The use of artificial intelligence is becoming especially relevant and important within the framework of the investigation of war crimes, in the course of criminal proceedings there is a possible violation of human rights (regarding the protection of the confidentiality of personal data and interference in private life), etc[47]. This requires intensifying the development and implementation of advanced technologies, methods and tools that are based on the application of forensic knowledge, adhering to the standards of evidence in criminal proceedings and the use of digital technologies and the capabilities of artificial intelligence[48].

Among the main areas of use of AI technologies in Ukraine today are the following: 1) analysis of: satellite images; video and photo materials, audio materials; social networks; data from medical institutions; text information; 2) facial recognition and identification of the offender in social networks and video recording cameras (including those of the Russian military); 3) ensuring road safety, identifying and

---

[43] Степанюк Р. Л. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 3 (99). С. 283-294. URL: DOI: 10.33766/2524-0323.99.283-294

[44] Шевчук В. М. Штучний інтелект в криміналістиці : проблеми, можливості, перспективи. *Інформаційне забезпечення розслідування злочинів* : матеріали X Міжнародного круглого столу (м. Одеса, 19 травня 2023 р.). Одеса: Видавництво «Юридика», 2023. С. 89–97.

[45] Shepitko V. Yu., Konovalova V. O., Shevchuk V. M. et. al. Scientific and technical support of investigative activities in the context of an adversarial criminal procedure. *Issues of Crime Prevention*, 2021, 1, 42, 92–102.

[46] Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 87-88.

[47] Шевчук В. М. Криміналістичне забезпечення розслідування кримінальних правопорушень в умовах цифрових технологій. *Інноваційні методи, засоби та технології в криміналістиці та судовій експертизі :* наук.-практ. посібник : електрон. наук. вид. ; за ред. В. Ю. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків: Право, 2023. С. 85–93.

[48] Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану*: матеріали всеукр. круг. столу (м. Харків, 16.12.22 р.); НДІ ВПЗ імені акад. В. В. Сташиса. Харків, 2022. С. 81.

recording violations of traffic rules; 4) the use of drones to combat the illegal circulation of firearms, drug crime, military operations and the collection of evidentiary information on the conditions of war and the conduct of active hostilities with the aim of recording war crimes; 5) prevention of criminal offenses using intelligent security systems with various information collection devices (sensors); 6) prediction of criminal offenses by the method of crime mapping, with the help of which forecasts are formed regarding local crime and individual criminal behavior[49], etc.

The use of AI in criminalistic activities is a promising innovative direction that opens up new opportunities for increasing the effectiveness of crime detection, automating routine tasks, predicting crime, and analyzing large volumes of data. In order to minimize risks and increase the effectiveness of the use of artificial intelligence in forensics, it is necessary to develop clear ethical and legal standards, ensure the transparency and accountability of algorithms, and improve the quality of training data. It is recommended to introduce AI into forensic practice gradually and cautiously, maintaining human control over final decision-making and taking into account the potential impact of technology on human rights and judicial justice[50].

Digital criminalistics is of particular importance for: obtaining information from mobile devices of seized phones of participants in criminal proceedings; obtaining information from personal computers of individuals and legal entities; obtaining information from servers and other information stores in organizations and institutions; obtaining information about radio frequency identifiers, GPS trackers, sensors, stationary and mobile measuring devices using geolocation, video surveillance and positioning systems; receiving information from network services that establish voice and video communication between computers via the Internet, such as ICQ, Skype, WhatsApp, Viber, Telegram and others; receiving information from banking systems on appropriate digital media (SD disks, flash cards, etc.); receiving information from cellular communication operators regarding the details of subscriber communication and establishing the location of the subscriber from geolocation; obtaining information from video surveillance cameras of various state structures; obtaining information from cameras and video cameras seized from participants in criminal proceedings.

Key areas of implementation of AI technologies in digital criminalistics:

1. *Automated recognition of objects and persons*. AI algorithms make it possible to process thousands of hours of video from surveillance cameras, chest recorders and drones for automatic identification of military equipment (by tactical signs), the type of weapons and the faces of combatants. This makes it possible to quickly establish the involvement of specific units in war crimes in populated areas.

2. *Audio data analysis and speech analytics*. In the investigation of war crimes, AI is used to automatically transcribe and translate intercepted radio or telephone conversations of the occupiers. AI-based systems are able to perform phonoscopic

[49] Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistikairteismo ekspertologija : mokslas, studijos, praktika: 18*, 2022, 18, 32.

[50] Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики**.** *Аналітично-порівняльне правознавство*. 2025. Т. 3. № 3. С. 211-115.URL: https://app-journal.in.ua/wp-content/uploads/2025/06/33-2.pdf

identification (identification of a person by voice) and detect key words-markers in speech that indicate the provision of criminal orders.

3. *Detection of manipulations and Deepfakes*. Countering disinformation is a strategic task of AI in digital forensics. Specialized neural networks analyze video and photo materials for digital anomalies, allowing experts to distinguish real footage of war crimes from enemy-generated or edited propaganda materials.

4. *Correlation analysis and construction of networks of connections*. Artificial intelligence allows you to combine disparate digital traces (geotags of photos, billing data, mentions in social networks) into a single logical scheme. This makes it possible to reconstruct the hierarchy of command and establish specific perpetrators and masterminds of crimes, revealing connections that at first glance seem random.

5. *Predictive analytics and event modeling*. AI helps reproduce 3D models of artillery strikes by analyzing the shape of cavities and damage to buildings, which allows you to calculate the trajectory of the projectile with high accuracy and identify the positions of enemy artillery even in the absence of direct video surveillance.

Therefore, the investigation of war crimes committed in conditions of full-scale armed aggression requires the use of high-tech tools to document massive violations of international humanitarian law. The use of these tools allows for the completeness of the investigation in cases where a traditional examination of the scene is impossible due to hostilities or landmines, making digital evidence the basis for future convictions in national and international courts[51].

In the realities of today's war, the digital toolkit of modern criminalistics is considered not just as an auxiliary tool, but as a technological foundation for proving war crimes, genocide and aggression in the conditions of a full-scale armed conflict. Intellectualization of digital forensics provides Ukraine with a strategic advantage in the legal field. AI technologies transform a chaotic set of digital data into a structured evidence base that meets the standards of international justice. This allows not only to scale the investigation process, but also to ensure its objectivity, minimizing the impact of the human factor when processing evidence of war crimes committed in Ukraine.

CONCLUSIONS

Summarizing the results of research on digital criminalistics as a strategic direction for the development of modern forensic science, some conclusions can be formulated: 1) a change in the scientific paradigm can be traced, since the digital transformation of forensics led to the transition from the study of purely material traces to the study of informational and digital patterns of the emergence, preservation and transmission of evidentiary information. This allows us to consider digital criminalistics as the intellectual core of a modern criminalistic strategy based on the principles of projectivity and intellectualization; 2) a transformation of the research object and methodology took place, that is, the object of strategic planning in criminalistics is not only the physical place of the event, but the digital

[51] Shevchuk V.M., Konovalova V.O., Sokolenko M.O. Digital criminalistics: formation and role in the fight against crime in wartime conditions in Ukraine. *The use of digital information in the investigation of criminal offenses*: materials of the international science and practice round table, Kharkiv, December 12. 2022; Scientific Research Institute crime problems named after Acad. V. V. Stashis. Kharkiv: Pravo, 2021. Pp. 97-102.

environment and digital traces; 3) the methodological basis of modern criminalistics is expanded due to the introduction of cryptographic methods (hashing), blockchain technologies to ensure the "Chain of Custody" and artificial intelligence algorithms to process Big Data arrays; 4) digital criminalistics acquires strategic importance in the conditions of a hybrid war, acts as a key tool for overcoming anonymity and solving the problem of legal attribution of the aggressor's actions. In modern conditions, it provides verification of facts in a distorted information field, allowing to separate objective digital evidence from products of disinformation and manipulation (Deepfakes); 5) digital criminalistics determines innovative areas of investigation of war crimes, among which the use of Drone Forensics tools and remote sensing of the Earth is an irreplaceable way of recording war crimes in occupied territories and in combat zones, which allows for the formation of a reliable evidence base for international judicial authorities; 6) further development of criminalistic science and digital forensics should be aimed at normative legitimization of remote methods of evidence collection and implementation of "Criminalistics by Design" standards. Therefore, in today's realities, it is necessary to update the development of the issues of digital criminalistics in modern conditions. At the same time, special attention should be paid to increasing the role of forensic didactics, in particular, forensic training of investigators, prosecutors, courts, detectives, forensic investigators, forensic experts in the field of digital technologies. Starting a new profession and training a digital criminologist is relevant today. Under such circumstances, the modern paradigm of criminology should be aimed at the further development and formation of digital criminalistics in order to effectively solve new tasks in the conditions of martial law.

SUMMARY

Actual problems of digital criminalistics as a strategic direction of development of modern criminalistics are studied. It has been proven that digitalization in criminalistics is manifested in the integration of digital technologies in criminalistic activities, which includes the development and use of special methods, techniques and tools for working with digital evidence and investigating crimes in the digital sphere. The processes of digital transformation of criminalistics as a scientific prerequisite and the methodological basis of the formation of new criminalistic knowledge are analyzed. It is noted that the methodological basis of the formation of new knowledge in the context of digital criminalistics research is structured according to three vectors: epistemological; systemic and structural; axiomatic The value of digital criminalistics for the formation of a criminalistic strategy lies in the transition from a tactical response to individual episodes to the creation of a comprehensive model of anticipatory documentation and investigation of criminal activity. A modern understanding of digital criminalistics is offered, its role and significance in the formation of evidentiary information in the conditions of hybrid warfare is analyzed. It is indicated that digital criminalistics is of key importance in the formation of evidentiary information in the conditions of hybrid warfare. It becomes a kind of digital tool that allows you to translate virtual and online acts of Russian military aggression into the realm of criminal procedural evidence. The most promising directions of research in this field of knowledge have been identified and considered.

Key words: digital technologies, special knowledge, criminalistic methodics, evidence collection, criminal proceedings, criminal activity, digital assets, criminalistic strategic, criminalistic innovations, forensic examination, digital criminalistics.

References:

1. Avdeeva G. Technological breakthrough in criminalistics and forensic examination : new horizons. *Archive of Criminology and Forensic Sciences*, 2025, 11(1), 100–110. https://doi.org/10.32353/acfs.11.2025.06

2. Aharkova O. I., Korosteleva L. A., Krasnopolskyi, V. E. The Use of Innovative Soft-ware Packages in Digital Forensics to Combat Crime in Ukraine. Sci. innov., 2025, 21(6), 60–67. https://doi.org/10.15407/scine21.06.060

2. Baranyak V. Digital forensics in the context of digitalisation of modern society. *Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки"*. № 2 (42), 2024. С. 7-11. http://doi.org/10.23939/law2024.42.007

3. Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану*: матеріали всеукр. круг. столу (Харків, 16.12.22 р.); НДІ ВПЗ імені акад. В. В. Сташиса. Харків, 2022. С. 81-83.

4. Баранов Р. О. Протидія легалізації злочинних доходів та фінансуванню тероризму з використанням віртуальних валют. *Державне управління: удосконалення та розвиток.* 2016, 6. URL: http://www.dy.nayka.com.ua/?op=1&z=978 (дата звернення: 19.02.2026).

5. Борисова К. Є., Світличний, В. А. Застосування цифрової криміналістики. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану*: тези доп. Міжнар. наук.-практ. конф.(м. Харків, 25 листоп. 2022 р.). Харків : ХНУВС, 2022. С. 83-84.

6. Демидова Є.Є. Тенденції розвитку цифрової криміналістики: виклики та перспективи для органів кримінальної юстиції. *Проблеми законності.* 2025. № 168. С. 164–182.

7. Домашенко О. М. Проблемні питання використання цифрових доказів у криміналістиці. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці:* матеріали міжнар. «круглого столу» (Харків, 12.12.2019) / В. Шепітько, В. Журавель, В. Шевчук. Х. : Право, 2019. С. 52–55.

8. Dumchykov M. O. Protsesy didzhytalizatsii i kryminalistyka: rektrospektyvnyi analiz. *Kryminalistyka i sudova ekspertyza Forensics and forensic examination*, issue 65, 2020. P. 100-108.

9. Заєць І. С. Перспективи криміналістики в умовах інформатизації суспільства. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід* : матеріали Міжнар. наук.-практ. круглого столу (Київ, 19 лют. 2020 р.). Київ : НАВСУ, 2020. С. 77-81.

10. Затенацький Д.В. Роль криміналістичної стратегії в розслідуванні воєнних злочинів в Україні. *Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє*: матеріали панельної дискусії VII Харківського Міжн. юрид. форуму 25 вересня 2023 року. Київ : Алерта, 2023. С. 33-38.

11. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 208 с.

12. Kohutych I. I. Zastosuvannia tsyfrovykh tekhnolohii – novyi napriam kryminalistyky. *Naukovi chytannia pamiati Hansa Hrossa: zbirnyk tez mizhnarodnoi naukovo-praktychnoi konferentsii* (m. Chernivtsi, 09 hrudnia 2021 r.) – Scientific readings in memory of Hans Gross: collection of theses of the international scientific conference (Chernivtsi, December 9, 2021). Chernivtsi: Tekhno-druk, 2021. P. 79-84.

13. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал*. 2022. № 4. С. 378–380.

14. Kolodina A. S., Fedorova T. S. Tsyfrova kryminalistyka: problemy teorii i praktyky. *Kyivskyi chasopys prava – Kyiv Journal of Law*, issue 1, 2022. P.176-180.

15. Konovalova V.O., Shevchuk V.M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries of modern science: experience, approaches and innovations*: III International Scientific and Theoretical Conference, January 20, 2023. Amsterdam: European Scientific Platform. Pp. 73-77.

16. Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: Proceedings of the 5th International scientific and practical conference (August7-9, 2022). Sci-conf.com.ua‖. Lviv, Ukraine. 2022. Pp. 896–903. https://sci-conf.com.ua/wp-content/uploads/2022/08/MODERN-RESEARCH-IN-WORLD-SCIENCE-7-9.08.2022.pdf

17. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistikairteismo ekspertologija : mokslas, studijos, praktika: 18,* 2022, 18, 32.

18. Maras M.-H. Computer Forensic: Cybercriminals, Laws, and Evidence. Second Edition, 2014. 408 p.

19. Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики,* 4 (29), 2023, 6-39.

20. Полотай О.І. Комп'ютерна криміналістика: основні завдання та проблеми. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*": матеріали Міжн. наук. інтернет-конф. Тернопіль. Вип. 68. 2022. С. 29-30.

21. Степанюк Р. Л. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 3 (99). С. 283-294. URL: DOI: 10.33766/2524-0323.99.283-294

22. Цифрова криміналістика та її роль у формуванні доказової інформації в умовах воєнних дій : монографія / [В. Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова] ; за ред. В. Ю. Шепітька ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2025. 200 с.

23. Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики**.** *Аналітично-порівняльне правознавство*. 2025. Т. 3. № 3. С. 211-115.

24. Шевчук В. М. Діджиталізація, цифровізація та технологізація криміналістики: проблеми сьогодення та перспективи майбутього. *Діджиталізація судово-експертної науки в умовах воєнного стану:* матеріали міжн. наукю-практ. конф. (8 листопада 2024 р., м. Харків). Харків: Право, 2024. С. 324-327.

25. Шевчук В. М. Криміналістика: традиції, новації, перспективи : добірка наук. пр. Харків : Право. 2020. 1280 с. с. 778. URL: http://library.nlu.edu.ua/POLN_TEXT/POSIBNIKI_2020/Kriminalistika_Shevchu k_2020.pdf.

26. Шевчук В. М. Криміналістичне забезпечення розслідування кримінальних правопорушень в умовах цифрових технологій. *Інноваційні методи, засоби та технології в криміналістиці та судовій експертизі :* наук.-практ. посібник : електрон. наук. вид. ; за ред. В. Ю. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків: Право, 2023. С. 85–93.

27. Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки і обороноздатності України. *Юридичний науковий електронний журнал.* № 6. 2024. С. 356 – 361.

28. Шевчук В. М. Штучний інтелект в криміналістиці : проблеми, можливості, перспективи. *Інформаційне забезпечення розслідування злочинів*: матеріали X Міжнародного круглого столу (м. Одеса, 19 травня 2023 р.). Одеса: Видавництво «Юридика», 2023. С. 89–97.

29. Шевчук В. М., Авдєєва Г. К. Використання технологій штучного інтелекту та спеціальних знань у розслідуванні воєнних злочинів. *Правнича наука та законодавство України: європейський вектор розвитку в умовах воєнного стану* : монографія; Нац, акад. прав. наук України. Харків, 2023. С. 491–503.

30. Шевчук В. М., Тищенко О. І. Технологізація криміналістики, судової експертизи і кримінального провадження в сучасних умовах цифровізації. *Юридичний науковий електронний журнал.* № 12. 2024. С. 375-380. URL: http://www.lsej.org.ua/12_2024/88.pdf

31. Шевчук В. М., Латиш К. В. Криміналістичне дослідження цифрових слідів / Криміналістика: підручник / [В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін.]; за ред. В. М. Шевчука; Нац. юрд. ун-т ім. Ярослава Мудрого. Харків: Право, 2024. С. 388–410. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20592

32. Shevchuk V. M. Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*. 2020, 27, 2, 170–183. URL: http://visnyk.kh.ua/en/article/metodologichni-problemi-formuvannya-ponyatiynogo-aparatu-kriminalistichnoyi-innovatiki

33. Shevchuk V. The role of digital criminalistics tools in the documentation of war crimes in Ukraine. Актуальні проблеми національного законодавства :

зб. тез Всеукр. наук.-практ. конф. (м. Кропивницький, 20 квітня, 2023 р.). Кропивницький: Юрайт, 2023. С. 46-50.

34. Shevchuk, V., Zhuravel, V., Yevdokimenko, S., Yevdokimenko, S., Myshkov, Y. Forensic Examination and Criminalistics in Investigating War Crimes: European and Ukrainian Experiences. *Jurnal Media Hukum*, 2025, 32(1), 59-77. DOI: https://doi.org/10.18196/jmh.v32i1.25056

35. Shevchuk, V., Bululukov, O., Chornyi, H., Tyshchenko, O., & Baranchuk, V. Latest Criminalistic Tools and Technologies in the Investigation of Cybercrimes: International and Ukrainian Experience. *Law, State & Telecommunications Review*, 2025, *17.*

36. Shevchuk, V., Morozova T., Chornyi, H., Nehrebetskyi V., and Slobodeniuk, I. Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues. *International Annals of Criminology*, 2025. Pp. 1-19. DOI: https://doi.org/10.1017/cri.2025.10090

37. Shevchuk V. Criminalistics Means and Methods of Combating Ecocide in the Modern Conditions of Military Threats. *Journal of Environmental Law and Policy*, 2024, 04 (03), 82-120. DOI: https://doi.org/10.33002/jelp040304

38. Shevchuk V.M., Konovalova V.O., Sokolenko M.O. Digital criminalistics: formation and role in the fight against crime in wartime conditions in Ukraine. *The use of digital information in the investigation of criminal offenses*: materials of the international science and practice round table, Kharkiv, December 12. 2022. Kharkiv: Pravo, 2021. Pp. 97-102.

39. Шепітько В.Ю. Теоретико-методологічна модель криміналістики та її нові напрями. *Теорія та практика судової експертизи і криміналістики*. 2021. Вип. 3 (25). С. 10–20.

40. Shepitko V., Shepitko, M. Doktryna kryminalistyky ta sudovoi ekspertyzy: formuvannia, suchasnyi stan i rozvytok v Ukraini. *Pravo Ukrainy – Law of Ukraine*, 2021, 8. P. 12-27.

41. Shepitko V., Shepitko M. The Formation of Digital Criminalistics as a Strategic Direction for the Development of Science. *XVII Criminalistics and Forensic Expertology: Science, Studies, Practice*. Abstracts of the XVII International Congress (September 16-17, 2021). Bratislava, Slovak Republic, 2021. P. 187-198.

42. Shepitko V. Yu., Konovalova V.O., Shevchuk V.M. et. al. Scientific and technical support of investigative activities in the context of an adversarial criminal procedure. *Issues of Crime Prevention*. Vol. 1. №. 42. 2021. Pp. 92-102.

Information about the author:
Shevchuk Viktor Mykhailovych,
Doctor of Legal Sciences, Professor,
Head of the Department of Criminalistics
Yaroslav Mudryi National Law University,
leading researcher Academician Stashis Scientific
Research Institute for the Study of Crime Problems
77, Hryhoriia Skovorody Str., 61024, Kharkiv, Ukraine
https://orcid.org/0000-0001-8058-3071

Zatenatskyi Dmytro Viktorovich,
PhD in Law, Associate Professor
Department of Criminalistics
Yaroslav Mudryi National Law University,
77, Hryhoriia Skovorody Str., 61024, Kharkiv, Ukraine
https://orcid.org/0000-0001-5430-4649

Kolesnikova Inna Anatoliivna
PhD in Law, Assistant
Yaroslav Mudryi National Law University
77, Pushkinska Str., Kharkiv, 61024, Ukraine
https://orcid.org/0000-0002-6138-8569

DOI https://doi.org/10.30525/978-9934-26-686-7-20

ЦИФРОВІ ДОКАЗИ У ПРОТИДІЇ КІБЕРПРАВОПОРУШЕННЯМ: ПРАВОВІ, ТЕХНІЧНІ ТА ЕКСПЕРТОЛОГІЧНІ АСПЕКТИ

Гомон В. О., Мірошник Р. О., Хівренко Д. В.

ВСТУП

Динамічний розвиток інформаційних технологій та їх інтеграція у всі сфери суспільного життя зумовили появу якісно нових форм правопорушень, які потребують переосмислення установлених підходів до правозастосування. Кіберправопорушення, що охоплюють широкий спектр протиправних діянь від несанкціонованого доступу до комп'ютерних систем до складних схем легалізації злочинних доходів із використанням криптовалютних активів, становлять одну з найбільш гострих проблем сучасного правопорядку[1].

Центральним елементом будь-якого провадження, пов'язаного з кіберправопорушеннями, є цифрові докази – інформація в електронній формі, що має значення для встановлення обставин справи. Специфіка цифрових доказів полягає у їхній нематеріальній природі, легкості модифікації, потенційній масштабності обсягів даних та необхідності застосування спеціальних технічних знань для їх виявлення, фіксації та дослідження[2]. Ці характеристики створюють суттєві виклики для правової практики, оскільки традиційні процесуальні механізми не завжди адекватно враховують технічну специфіку цифрового середовища.

Стрімкий розвиток технологій блокчейну та криптовалют додає окремий вимір до цієї проблематики. Використання криптовалют у злочинній діяльності вимагає від експертного середовища володіння принципово новими інструментами – блокчейн-аналізаторами та системами на базі штучного інтелекту. Водночас результати застосування цих інструментів мають ймовірнісний характер, що потребує розробки методологічних стандартів.

Особливої актуальності набуває міжгалузевий характер проблематики цифрових доказів. Питання їх допустимості, достовірності та доказової сили виникають не лише у кримінальному провадженні, а й у цивільному та адміністративному судочинстві, господарському процесі та інших правових процедурах. Кожна з цих галузей встановлює власні вимоги до доказів та стандарти оцінки, що зумовлює необхідність формування цілісного міжгалузевого підходу до регламентації роботи з цифровими доказами.

Ця монографія присвячена комплексному дослідженню міжгалузевих викликів та перспектив, пов'язаних із кіберправопорушеннями та цифровими

[1] Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. Рада Європи. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[2] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

доказами. Метою роботи є системний аналіз правових, технічних та методологічних аспектів роботи з цифровими доказами, виявлення основних проблем їх допустимості та оцінки, а також формулювання пропозицій щодо вдосконалення нормативного регулювання та експертної практики. Особлива увага приділяється застосуванню блокчейн-аналізаторів та штучного інтелекту у криміналістичних дослідженнях криптовалют, процесуальним аспектам забезпечення цілісності цифрових доказів, а також перспективам розвитку правового регулювання у сфері протидії кіберправопорушенням.

1. Цифрові докази як міжгалузева правова категорія

1.1. Поняття та правова природа цифрових доказів

Цифровий доказ у найбільш загальному розумінні являє собою будь-яку інформацію, що зберігається або передається у цифровій формі та має доказове значення для встановлення обставин справи. Правова природа цифрових доказів характеризується низкою специфічних ознак: нематеріальністю, тобто існуванням доказової інформації у вигляді послідовності бітів, що потребує спеціальних засобів для відображення у доступній формі; легкою відтворюваністю, що породжує проблему розмежування оригіналу та копії; а також летючістю – здатністю до швидкої зміни або знищення внаслідок як цілеспрямованих дій, так і автоматичних процесів функціонування систем.

Чинне процесуальне законодавство України не містить окремого визначення цифрових доказів, натомість оперує поняттям електронних доказів. Кримінальний процесуальний кодекс розглядає електронні документи та дані в електронній формі у контексті загальної класифікації доказів. Цивільний процесуальний кодекс та Кодекс адміністративного судочинства визначають електронні докази як інформацію в електронній формі, що містить дані про обставини справи, зокрема електронні документи, вебсайти, повідомлення, метадані, бази[3] даних[4]. Таке регулювання, хоча й створює правову основу для використання цифрових доказів, залишає відкритими питання щодо процедур їх вилучення, зберігання та дослідження у справах про складні кіберправопорушення.

За джерелом походження цифрові докази охоплюють дані з комп'ютерних систем та мобільних пристроїв, мережевий трафік, журнали подій, дані з хмарних сервісів, інформацію з блокчейн-мереж, метадані файлів, а також дані з пристроїв Інтернету речей. Кожна з цих категорій має технічну специфіку, що впливає на процедури вилучення та критерії оцінки достовірності. Зокрема, дані з блокчейн-мереж мають принципову відмінність: вони є публічно-доступними, проте псевдонімними за природою, створюючи специфічні виклики для їх інтерпретації у доказуванні.

[3] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/1618-15

[4] Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/2747-15

1.2. Специфіка цифрових доказів у різних видах судочинства

У кримінальному процесі, де діє стандарт доказування «поза розумним сумнівом», вимоги до цифрових доказів є найсуворішими. Процедура вилучення має відповідати вимогам КПК щодо обшуку, тимчасового вилучення майна або інших слідчих дій, а порушення процедури може стати підставою для визнання доказу недопустимим. Особливого значення набуває забезпечення безперервного ланцюга зберігання цифрових доказів із документуванням кожного етапу роботи з доказом та криптографічною верифікацією цілісності даних.

У цивільному та адміністративному судочинстві стандарти допустимості є менш формалізованими, проте суди стикаються з проблемою оцінки автентичності цифрових доказів, оскільки можливість їх модифікації та фальсифікації значно вища, ніж для паперових документів. Відсутність єдиних стандартів подання цифрових доказів у цивільному процесі створює ситуацію правової невизначеності, коли прийняття або відхилення доказу значною мірою залежить від дискреції конкретного судді та його обізнаності у технічних питаннях. Особливу складність становить використання цифрових доказів у справах міжгалузевого характеру, коли одні й ті ж дані одночасно використовуються у кримінальному провадженні, цивільному позові та адміністративному провадженні, що порушує питання взаємної допустимості доказів та узгодження різних стандартів оцінки.

Забезпечення автентичності та цілісності цифрових доказів є фундаментальною передумовою їх використання у будь-якому провадженні. На відміну від матеріальних об'єктів, цифрові дані можуть бути модифіковані без залишення видимих слідів втручання, що робить питання верифікації критично важливим. Основним технічним інструментом є криптографічне хешування – обчислення унікального цифрового відбитку за допомогою алгоритмів SHA-256[5] або MD5, де будь-яка зміна у вихідних даних призводить до кардинальної зміни хеш-значення. Практична реалізація цих механізмів стикається з проблемами: хешування має відбуватися безпосередньо при вилученні, саме хеш-значення не захищає від підміни усього доказу, а зростання обсягів даних ускладнює верифікацію у справах із терабайтами інформації з множини пристроїв.

2. Кіберправопорушення та особливості їх доказування

2.1. Систематизація кіберправопорушень та збирання цифрових доказів

Кіберправопорушення поділяються на три основні групи: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних систем (несанкціонований доступ, шкідливе програмне забезпечення, DDoS-атаки); правопорушення з використанням комп'ютерних систем як засобу вчинення традиційних злочинів (шахрайство, легалізація доходів через криптовалюти, ransomware); та правопорушення, пов'язані зі змістом комп'ютерних даних.

[5] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

Кожна категорія характеризується принципово відмінними механізмами вчинення, картиною слідства та вимогами до збирання доказів.

Доказування у першій групі вимагає дослідження журналів подій операційних систем та мережевого обладнання, слідів шкідливого програмного забезпечення та мережевого трафіку. Складність полягає у тому, що кваліфіковані зловмисники використовують VPN-сервіси, проксі-сервери та мережу Tor для маскування слідів. Друга група, що включає криптовалютні злочини, потребує комбінованого підходу – традиційних криміналістичних методів разом із блокчейн-аналізом та дослідженням цифрових артефактів на пристроях підозрюваних.

Фундаментальним принципом цифрової криміналістики є мінімізація впливу на досліджуваний об'єкт через створення побітових криміналістичних образів носіїв із подальшим проведенням усіх досліджень на копії. Для мобільних пристроїв використовуються спеціалізовані криміналістичні комплекси – Cellebrite (Inseyets), Oxygen Forensic Detective та інші, що забезпечують різні рівні доступу від логічного вилучення до повного фізичного образу. У контексті криптовалютних злочинів дані блокчейну є публічно доступними та не потребують спеціальних процесуальних дій для отримання, проте їх інтерпретація вимагає складних аналітичних досліджень з використанням блокчейн-аналізаторів.

Окрему проблему становить збирання летючих даних – інформації з оперативної пам'яті, що знищується при вимкненні живлення. Такі дані можуть містити сліди активних з'єднань зі зловмисниками, ключі шифрування або дані авторизації на криптовалютних сервісах. Вилучення летючих даних має здійснюватися за принципом порядку летючості, починаючи з найбільш нестабільних джерел, і потребує спеціалізованих інструментів та високої кваліфікації, оскільки будь-яка взаємодія з працюючою системою неминуче змінює її стан.

Зростаюча роль шифрування – BitLocker, LUKS, VeraCrypt, TrueCrypt, FileVault, повнодискове шифрування мобільних пристроїв – також створює суттєві перешкоди для отримання доступу до релевантних даних. Методи подолання шифрування включають пошук ключів у оперативній пам'яті або файлах гібернації, використання вразливостей конкретних реалізацій, а також залучення спеціалізованих апаратних засобів для обходу захисту. Фіксація цифрових доказів у процесуальних документах має відображати технічні параметри процедури вилучення, хеш-значення образів, серійні номери пристроїв та будь-які обставини, що можуть вплинути на цілісність даних.

3. Блокчейн-аналізатори та штучний інтелект у криміналістичних дослідженнях крипто валют

3.1. Технічні можливості блокчейн-аналізаторів та роль штучного інтелекту

Стрімке зростання використання криптовалют у злочинній діяльності, зокрема у схемах відмивання коштів, фінансування тероризму, ransomware-атаках та порушенні санкційних режимів, актуалізує питання застосування

спеціалізованих блокчейн-аналізаторів у рамках судової експертизи. Водночас виникає принципова методологічна проблема: трансформація технічної інформації з блокчейн-мереж у судовий доказ вимагає критичного переосмислення традиційних підходів до формулювання експертних висновків, оскільки результати автоматизованого аналізу часто мають ймовірнісний, а не категоричний характер.

Сучасні платформи блокчейн-аналізу – Global Ledger, Crystal Blockchain, CipherTrace, Chainalysis, Elliptic – використовують комплексний підхід до дослідження криптовалютних транзакцій: кластеризацію (поєднання адрес в один пул), графовий аналіз транзакційних ланцюгів (адреси – вузли, транзакції – зв'язки), атрибуцію гаманців до конкретних сервісів чи осіб та оцінку ризиків на основі машинного навчання. Ці системи здатні обробляти мільйони транзакцій у режимі реального часу, виявляти складні багаторівневі схеми переміщення коштів, ідентифікувати використання міксерів та встановлювати зв'язки між адресами на основі поведінкових патернів та евристичних правил.

Кожна з платформ має свої сильні сторони. Chainalysis відзначається найширшим покриттям блокчейнів та найбільшою базою атрибуційних даних, що робить її переважним інструментом для правоохоронних органів. Crystal Blockchain пропонує зручний графовий інтерфейс для візуалізації транзакційних ланцюгів. Global Ledger спеціалізується на глибокому аналізі з акцентом на точності кластеризації. Elliptic фокусується на аналізі ризиків та комплаєнсі. Обрання інструменту для експертного дослідження залежить від характеру завдання, типу блокчейну та необхідної глибини аналізу.

Штучний інтелект у блокчейн-аналізі застосовується для розв'язання декількох критичних завдань. Алгоритми машинного навчання дозволяють кластеризувати адреси одного власника навіть за відсутності явних зв'язків, базуючись на часових патернах, обсягах транзакцій та поведінкових характеристиках. Нейронні мережі розпізнають типові схеми відмивання: layering (створення множинних проміжних адрес), peel chain (створення видимості легітимної активності), використання cross-chain мостів (переміщення криптоактивів між різними блокчейнами) для ускладнення трасування. Системи на базі штучного інтелекту здійснюють автоматичну атрибуцію адрес до конкретних бірж, платіжних сервісів та міксерів на основі аналізу величезних датасетів історій транзакцій.

3.2. Виявлення схем відмивання криптовалютних активів та технічні обмеження аналізу

Легалізація злочинних доходів через криптовалюти має специфічні технічні ознаки, виявлені блокчейн-аналізом. Типові патерни включають структурування транзакцій для уникнення порогів моніторингу фінансових установ, швидке переміщення коштів між множинними адресами та блокчейнами, конвертацію у стейблкоїни, використання анонімних бірж без KYC та P2P-платформ з низькими вимогами до ідентифікації. Блокчейн-аналізатори застосовують графовий аналіз для виявлення складних транзакційних структур, характерних для layering-фази відмивання.

Однак дослідження стикається з принциповими технічними обмеженнями. Використання міксерів, де кошти множинних користувачів об'єднуються у загальний пул з подальшим розподілом на нові адреси, робить встановлення прямого зв'язку між конкретними вхідними та вихідними транзакціями математично неможливим. Privacy-орієнтовані криптовалюти – Monero з кільцевими підписами та конфіденційними транзакціями, Zcash з протоколом ZK-SNARK – унеможливлюють трасування коштів на рівні протоколу блокчейну. Децентралізовані міксери, cross-chain atomic swaps та інші технології обфускації створюють додаткові виклики для аналізу.

3.3. Ймовірнісна природа експертних висновків у блокчейн-експертизі

Принципова відмінність блокчейн-експертизи від традиційних криміналістичних досліджень полягає у ймовірнісному характері висновків, особливо коли кошти проходять через міксери або множинні етапи обфускації. Результати варіюються від високого рівня достовірності для прямих транзакцій без обфускаційних сервісів до повної неможливості встановлення зв'язку для коштів, що пройшли через міксери чи privacy-coins (Monero, Zcash, Dash). Категоричні твердження можливі лише для простих ланцюжків між ідентифікованими адресами без сервісів анонімізації.

Коли криптовалютні кошти надходять у загальний пул міксера, де змішуються з коштами інших користувачів, блокчейн-аналізатор може визначити лише ймовірнісний зв'язок між вхідними та вихідними транзакціями на основі часових збігів, статистичного аналізу обсягів та поведінкових патернів. Категорично стверджувати, що конкретні кошти, внесені певною особою, опинилися на певній вихідній адресі, технічно неможливо через архітектуру міксерів, спрямовану на розрив транзакційних зв'язків.

Використання блокчейн-аналізаторів у розслідуваннях вимагає дотримання науково обґрунтованої методології, що забезпечує відтворюваність результатів та можливість верифікації. Експерт не може обмежуватися представленням висновків програмного забезпечення як остаточних результатів дослідження. Необхідною є верифікація ключових висновків через аналіз первинних даних блокчейну з використанням альтернативних інструментів, перевірка коректності кластеризації через аналіз спільних входів транзакцій та документування всього ланцюга транзакцій з поясненням логіки встановлення зв'язків. Експертний висновок має містити інформацію про використані програмні засоби із зазначенням версій, методологію кластеризації та атрибуції, альтернативні сценарії переміщення коштів та рівень достовірності кожного встановленого зв'язку.

4. Процесуальні та методологічні аспекти роботи з цифровими доказами

4.1. Ланцюгзберігання та криптографічна верифікація цифрових доказів

Ланцюг зберігання цифрових доказів (chain of custody) являє собою безперервну документовану послідовність дій з доказом від моменту виявлення до представлення у суді. На етапі вилучення це включає фіксацію первинного стану об'єкта, реєстрацію технічних характеристик, обчислення хеш-значень та

створення криміналістичного образу з використанням апаратних блокувальників запису. Подальші етапи передбачають контрольоване зберігання в умовах, що виключають несанкціонований доступ, із документуванням кожної передачі доказу.

Криптографічне хешування є фундаментом забезпечення цілісності. Алгоритм SHA-256 вважається криптографічно стійким, тоді як MD5 має відомі вразливості до колізійних атак[6]. Практика передбачає обчислення хеш-значень на кількох рівнях – для носія загалом, окремих розділів та файлів – з використанням множинних алгоритмів одночасно. Кваліфікований електронний підпис та довірені позначки часу забезпечують додаткові гарантії цілісності та хронологічної прив'язки доказу.

У контексті блокчейн-експертизи ланцюг зберігання має особливості: дані блокчейну публічно доступні, а їх цілісність гарантована архітектурою розподіленого реєстру. Проте необхідно документувати джерела даних, конкретні вузли або API-сервіси, версії блокчейн-аналізаторів та дату аналізу, оскільки атрибуційні бази оновлюються і результати можуть дещо відрізнятися з часом.

4.2. Методологічні вимоги до експертного висновку та верифікація результатів

Експертний висновок у справах про кіберправопорушення має включати детальний опис об'єктів дослідження, перелік питань, опис методів та програмних засобів із зазначенням версій, послідовний виклад ходу дослідження та висновки з чітким зазначенням їхнього характеру – категоричного чи ймовірнісного. Особливу увагу слід приділяти обмеженням дослідження та альтернативним версіям, які не можуть бути виключені.

Для верифікації результатів автоматизованого аналізу рекомендується підхід перехресної верифікації – проведення аналізу одних і тих же даних кількома незалежними інструментами[7]. У блокчейн-аналізі це означає використання щонайменше двох платформ для кластеризації та трасування, а також перевірку висновків через ручний аналіз первинних даних за допомогою блокчейн-експлорерів. Збіг результатів, отриманих різними інструментами, суттєво підвищує достовірність висновків, тоді як розбіжності вимагають додаткового дослідження та пояснення.

Забезпечення відтворюваності вимагає фіксації версій програмного забезпечення, дати аналізу, параметрів налаштування та проміжних результатів. Водночас повна відтворюваність результатів блокчейн-аналізу може бути обмежена об'єктивними факторами – оновленням атрибуційних баз, зміною алгоритмів кластеризації та появою нових транзакцій, що змінюють контекст аналізу. Цей фактор має бути відображений у дослідницькій частині експертного висновку як об'єктивне обмеження даного виду дослідження, а не як недолік конкретної експертизи.

---

[6] MD5 Collision Demo, Peter Selinger Published Feb 22, 2006. Last updated Oct 11, 2011. URL: https://www.mscs.dal.ca/~selinger/md5collision/

[7] ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization, 2015.

5. Перспективи розвитку

Розвиток технологій підвищення конфіденційності криптовалютних транзакцій випереджає можливості аналітичних систем, що створює постійну необхідність адаптації експертних методик. Децентралізовані міксери, атомарні свопи, блокчейни з обмеженою прозорістю вимагають нових підходів до трасування коштів. Інтеграція штучного інтелекту відкриває нові можливості, проте високі показники точності на тренувальних даних не гарантують абсолютної достовірності, особливо за умови застосування контрзаходів.

Водночас застосування блокчейн-аналізаторів є абсолютно необхідним для розслідування криптовалютних злочинів, оскільки альтернативні методи фактично відсутні. Ручний аналіз мільйонів транзакцій технічно неможливий, а практика розслідування ransomware-атак та схем шахрайства демонструє, що саме ці технології забезпечили викриття злочинців. Відсутність категоричної достовірності у окремих висновках не применшує критичної важливості інструментів, а лише вимагає коректного відображення рівня достовірності.

Ключовими напрямами розвитку є формування єдиних методологічних стандартів експертиз у сфері кіберправопорушень, розробка стандартизованих шкал ймовірності для блокчейн-аналізу, підвищення кваліфікації експертів та суддів у цифрових технологіях, а також розвиток міжвідомчої взаємодії між правоохоронними органами, експертними установами та регуляторами фінансового ринку. Створення спеціалізованих підрозділів, що поєднують правову та технічну експертизу, забезпечення доступу до сучасних аналітичних інструментів та систематичне підвищення кваліфікації є необхідними умовами ефективної протидії кіберзлочинності.

Перспективними технологічними напрямами є застосування великих мовних моделей для аналізу текстових артефактів у кіберрозслідуваннях, розвиток предиктивного аналізу для прогнозування кіберзлочинів та інтеграція різнорідних джерел даних у єдині аналітичні платформи. Впровадження цих технологій у судово-експертну практику потребує ретельного наукового обґрунтування, валідації та формування чітких методологічних рамок, що забезпечують прозорість та верифікованість результатів.

ВИСНОВКИ

Цифрові докази як міжгалузева правова категорія потребують формування єдиного комплексного підходу до регламентації, що враховує технічну специфіку цифрової інформації та забезпечує баланс між ефективністю доказування й дотриманням процесуальних гарантій. Чинне законодавство, хоча й визнає електронні докази повноцінним засобом доказування, не містить достатньо детальних положень щодо процедур їх вилучення та дослідження у справах про складні кіберправопорушення. Класифікація кіберправопорушень демонструє значну різноманітність способів вчинення, що зумовлює необхідність диференційованого підходу до збирання та оцінки доказів у кожній категорії справ.

Застосування блокчейн-аналізаторів та штучного інтелекту є безальтернативним інструментом розслідування криптовалютних злочинів. Ймовірнісний характер окремих висновків не применшує їхньої доказової

цінності, а лише потребує адекватного відображення у процесуальних документах та відповідного тлумачення при судовому розгляді. Ланцюг зберігання, криптографічне хешування та інші механізми забезпечення цілісності є обов'язковими елементами роботи з цифровими доказами, без яких їх допустимість може бути поставлена під сумнів.

Актуальними завданнями залишаються розробка єдиних методологічних стандартів судової експертизи у сфері кіберправопорушень, впровадження стандартизованих шкал ймовірності для блокчейн-аналізу, підвищення кваліфікації експертів та суддів у сфері цифрових технологій, а також удосконалення нормативно-правової бази з урахуванням стрімкого технологічного розвитку. Вирішення цих завдань потребує консолідації зусиль правової науки, експертного середовища та правоохоронних органів.

АНОТАЦІЯ

Монографія присвячена комплексному дослідженню правових, технічних та методологічних аспектів використання цифрових доказів у протидії кіберправопорушенням в умовах динамічного розвитку інформаційних технологій. Авторами проаналізовано правову природу цифрових доказів як міжгалузевої категорії та виявлено системні прогалини чинного процесуального законодавства України щодо процедур їх вилучення, зберігання та дослідження у складних кіберсправах. Досліджено специфіку збирання цифрових доказів у різних видах судочинства з урахуванням відмінних стандартів допустимості та достовірності, притаманних кримінальному, цивільному й адміністративному процесам. Окрему увагу приділено застосуванню сучасних блокчейн-аналізаторів – Chainalysis, Crystal Blockchain, Global Ledger, Elliptic – та систем штучного інтелекту для виявлення схем легалізації криптовалютних активів і атрибуції транзакцій. Обґрунтовано, що результати автоматизованого блокчейн-аналізу мають ймовірнісний характер, що зумовлює необхідність розробки стандартизованих шкал достовірності та відповідного відображення рівня висновків у процесуальних документах. Розглянуто методологічні вимоги до забезпечення ланцюга зберігання цифрових доказів, криптографічної верифікації їх цілісності та відтворюваності результатів експертного дослідження. Визначено перспективні напрями розвитку судово-експертної практики, зокрема інтеграцію великих мовних моделей, предиктивного аналізу та уніфікованих аналітичних платформ у розслідування кіберзлочинів. Результати дослідження можуть бути використані для вдосконалення нормативно-правової бази, підвищення кваліфікації судових експертів і суддів, а також розбудови міжвідомчої взаємодії у сфері протидії кіберзлочинності.

Література

1. Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. Рада Європи. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

2. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/1618-15

3. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/2747-15

4. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

5. NIST Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. Gaithersburg, 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

6. MD5 Collision Demo, Peter Selinger Published Feb 22, 2006. Last updated Oct 11, 2011. URL: https://www.mscs.dal.ca/~selinger/md5collision/

7. ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization, 2015.

Information about the authors:
Homon Volodymyr Oleksiyovych,
Forensic expert (digital evidence)
Scientific research center for forensic science of information technologies and intellectual property
26, L. Ukrainky blvd, Kyiv, 01133, Ukraine
https://orcid.org/0000-0001-6326-9590

Miroshnyk Ruslan Oleksandrovych,
Forensic expert (digital evidence)
Scientific research center for forensic science of information technologies and intellectual property,
26, L. Ukrainky blvd, Kyiv, 01133, Ukraine
https://orcid.org/0009-0004-8504-0489

Khivrenko Dmytro Volodymyrovych,
Forensic expert (digital evidence)
Scientific research center for forensic science of information technologies and intellectual property,
26, L. Ukrainky blvd, Kyiv, 01133, Ukraine

NOTES

NOTES

The project was implemented with the support of

CUESC

The Center for Ukrainian and European Scientific Cooperation is a non-governmental organization, which was established in 2010 with a view to ensuring the development of international science and education in Ukraine by organizing different scientific events for Ukrainian academic community.

The priority guidelines of the Centre for Ukrainian and European Scientific Cooperation

1. International scientific events in the EU

Assistance to Ukrainian scientists in participating in international scientific events that take place within the territory of the EU countries, in particular, participation in academic conferences and internships, elaboration of collective monographs.

2. Scientific analytical research

Implementation of scientific analytical research aimed at studying best practices of higher education establishments, research institutions, and subjects of public administration in the sphere of education and science of the EU countries towards the organization of educational process and scientific activities, as well as the state certification of academic staff.

3. International institutions study visits

The organisation of institutional visits for domestic students, postgraduates, young lecturers and scientists to international and European institutes, government authorities of the European Union countries.

4. International scientific events in Ukraine with the involvement of EU speakers

The organisation of academic conferences, trainings, workshops, and round tables in picturesque Ukrainian cities for domestic scholars with the involvement of leading scholars, coaches, government leaders of domestic and neighbouring EU countries as main speakers.

Contacts:
Head Office of the Center for Ukrainian and European Scientific Cooperation:
88000, Uzhhorod, 25, Mytraka str.
+38 (099) 733 42 54
info@cuesc.org.ua

www.cuesc.org.ua

Izdevniecība “Baltija Publishing”
Avotu iela 8 k-1 – 25, Rīga, LV-1011
E-mail: office@baltijapublishing.lv

Iespiests tipogrāfijā SIA “Izdevniecība “Baltija Publishing”
Parakstīts iespiešanai: 2026. gada 30. aprīlis
Tirāža 150 eks.