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