DOI: 10.18372/2307-9061.73.19470
УДК 343.98(045)

N. O. Holdberh,
PhD (Law), Associate Professor
ORCID ID: https://orcid.org/0000-0003-1624-1944

V. M. Kolonska,
student of the first (bachelor's) level of higher education

DIGITAL FORENSICS IN MARTIAL LAW

State Non-Commercial Company «State University «Kyiv Aviation Institute»
Lubomyr Huzar Avenue, 1, 03058, Kyiv, Ukraine
E-mails: natalia.holdberh@npp.nau.edu.ua, 7545177@stud.nau.edu.ua

The purpose *of the article is to study a new area of forensics - digital forensics.* ***Research methods:*** *the article uses the hermeneutic method, the method of classification, logical methods (analysis, synthesis, induction, deduction, generalization, etc.), and the method of systematization.* ***Results:*** *the article explores a new branch of forensics, namely digital forensics. Digital forensics is becoming increasingly important and is becoming one of the main components of traditional forensics. Knowledge of digital forensics is used in many investigative actions and in the process of appointing relevant forensic examinations not only in relation to offenses in the field of information technology, but also in the investigation of a wide range of crimes committed during the war and occupation.* ***Discussion:*** *the author analyzes the views of leading scholars on the concept of digital forensics in the system of forensic science. The author assesses the trends in the development of digital forensics at the present stage and predicts the further development of this area in Ukraine, and conducts a legal analysis of the use of digital forensics. The existing model of forensic science in Ukraine urgently requires the formation of a separate branch of forensic technology, which includes means and methods of digital evidence investigation. The article also examines the peculiarities of digital forensics application under martial law. In particular, new challenges and opportunities arising from the active use of digital technologies in modern conflicts are analyzed.*

Key words: *digital forensics; forensics; evidence; digital technologies; criminal offenses; war crimes; digital evidence; cybercrime.*

Statement of the problem and its relevance. Today, almost everyone uses multiple digital devices and accesses various digital services on a daily basis. As a result, a large number of digital traces are created in everyday life and there is a high probability that digital traces are left by criminal activity. Therefore, the number of cases when law enforcement agencies need to detect and investigate digital traces, use tools to search and record information in cyberspace, and use digital data in the process of proving criminal proceedings is increasing every year.

Every year, more and more innovative technologies are being introduced into various spheres of public life. Criminalistics is no exception and has entered a new stage of development thanks to the latest technologies. In particular, a new branch of forensics - digital forensics - has emerged thanks to the latest technologies.

The increase in the number of cyberattacks related to armed conflicts poses new challenges to digital forensics.

Analysis of research and publications with problems. In Ukraine, very few researchers work in the field of digital forensics. This is due to the fact that digital forensics is a relatively new field of science and emerged only in the 1980s. Among the authors who touch upon certain issues of digital forensics are Kolodina A., Fedorova T., Shepitko V., Shepitko M., etc.

The purpose of the article is to study a new area of criminalistics - digital forensics.

Summary of the main research material. The introduction of martial law in Ukraine has had a significant impact on the development of forensic science. In this context, there is a need to develop new approaches to countering modern military challenges, as well as to create and implement effective systems to counter current threats.

In today's military reality, the effectiveness of using digital technologies to investigate modern crimes, including cybercrime and war crimes, is becoming increasingly important. In this context, we can talk about the emergence of a new field - digital forensics. Other terms used to refer to this field include electronic forensics, computer forensics and computer systems forensics.

In the legal literature, scholars express different opinions on the definition of digital forensics and its role in the system of forensic science. A. Kolodina and T. Fedorova note that digital forensics is an applied science of solving crimes related to computer information, the study of digital evidence, methods of searching, obtaining and securing such evidence [1, p. 283].

V. Shepitko and M. Shepitko note that digital forensics can be considered a strategic direction of development of forensic science and law enforcement practice. In turn, the development of digital forensics itself takes place in three main areas: the formation of a separate scientific field in forensics; application of special knowledge when working with digital evidence; and forensic examinations (mainly computer and technical) [7, p. 21].

The full-scale military aggression of the Russian Federation and the introduction of martial law in Ukraine had a significant impact on the development of forensics and society. Obviously, the dynamics and trends of crime in Ukraine during the war had a significant impact on the change in the priorities of forensic science and the activities of the criminal justice system.

In this context, there is a need to develop new approaches to counteracting modern military challenges, modernise and update law enforcement and judicial bodies in accordance with martial law, and create and implement effective systems to counteract existing threats by forensic means.

The subject matter of digital forensics is the patterns of detection, recording, preliminary research, use of computer information, digital traces and means of their processing in order to solve the problems of detection, disclosure, investigation and prevention of criminal offences, as well as the development of patterns of technical means, techniques, methodological recommendations aimed at optimising activities to counter criminal offences in the digital space based on this knowledge [5, p. 36].

It is necessary to distinguish between digital forensics, on the one hand, as an independent branch of forensic knowledge for the study of digital traces, and, on the other hand, as the use of digital technologies in investigation and trial, i.e. the process of digitalisation 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, up to the pre-trial investigation process.

The following modern areas of digital forensics are distinguished: 1) research of cloud storage; 2) research of mobile devices (phones); 3) research of programs (messengers and other smartphone applications used for information exchange); 4) research of Internet of Things (IoT); 5) network research; 6) research of the latest devices and applications (Alexa from Amazon, Google Assistant, Siri from Apple, etc.); 7) research of applications not for the phone (research of databases, Spotlight, America online instant messaging, drones, volatile memory, Darknet, anti-criminalistics tools, deleted and fragmented files, images, flash memory, cryptocurrencies); 8) digital analysis of the behaviour of individuals, groups of people and their interconnections and relationships; 9) digital forensic intelligence and intelligence based on open sources, etc.

The rapid development of digitalisation and communications has increased the challenges and risks of cybersecurity, making society more vulnerable to cyber threats. This has contributed to the emergence of new types of modern crime, such as information fraud, cyberattacks on critical infrastructure, copyright and related rights infringement, fraud, illegal activities using transfer documents, payment cards and other means of accessing bank

accounts, tax evasion, sale and distribution of pornography.

The collection, storage, use and verification of digital evidence in criminal proceedings requires a modern approach. It is important to develop developments by Ukrainian scientists in the methodology of investigating cybercrime and to use their professional knowledge and expertise in the investigation of such crimes. Digital forensics develops methods, hardware and software for collecting and examining evidence of computer crimes and conducts tactical and operational countermeasures and investigative actions using computer information to determine the forensic nature of crimes in cyberspace.

The international standard ISO/IEC 27037 on the handling of digital evidence provides for four stages of digital evidence handling: 1) identification (searching for and documenting relevant evidence); 2) collection (gathering data from various sources, including computers, servers and mobile devices, using special tools); 3) retrieval (copying digital data using record blockers to preserve data integrity. Checking the accuracy of the copy using hash functions); 4) preservation (protection and preservation of digital evidence, creation of copies to ensure consistency throughout the investigation) [3, p. 288].

Digital forensics tools play an important role in the investigation of war crimes, providing valuable data and evidence to establish the truth. One important tool is the search for information on social media and forums. This can help to locate witnesses, victims and perpetrators, as well as determine the scale and circumstances of the crime. Satellite imagery can document destruction and troop movements and help identify crimes and those involved.

Big data and geolocation are other important tools that analyse data from phones, social media, finances and other sources to help identify patterns of crime-related behaviour. Geolocation helps to locate people and devices, as well as track criminals, victims and crime scenes. Photographs and videos document crimes, and facial recognition and image analysis software helps to identify victims and criminals. In addition, analyses of telephone conversations, digital images, and gaming systems can provide valuable information for investigations. These tools enable digital forensics investigators to effectively investigate and solve war crimes and ensure justice and fairness.

Difficulties include the need for investigators to have high computer competence; the need to prove evidence as authentic; significant costs for the production and storage of electronic records; the use of incompatible tools, which can lead to the rejection of evidence by the court [3, p. 289].

Digital forensics is a science with a technical component, but it goes beyond technical aspects. In recent years, the technical examination of digital evidence has been increasingly integrated into the entire process of detecting and investigating cybercrime, which requires the involvement of experts at every stage of the investigation.

Digital forensics tools and methods are widely used in operational and investigative activities, pretrial investigation, forensic examination and digital evidence research.

Digital forensics developments are used in the investigation of cybercrime, such as hacking, identity theft, fraud, and in corporate investigations (analysing computer logs or emails to identify security breaches or employee misconduct); civil litigation (collecting evidence to support or refute claims, for example, in cases of intellectual property theft); incident response (investigating cyber incidents and determining the source of the attack); regulatory compliance (ensuring compliance with rules and proper).

In particular, the role of forensic information in improving and ensuring a safe environment in our country is becoming increasingly important, and the optimisation and efficiency of combating modern crime (including war crimes and cybercrime) through the active use of digital technologies is being addressed. The most well-known areas of this process are Digital Forensic Imaging, which involves creating an exact copy of a digital device for further analysis without changing the original data; Deleted Data Recovery, which is used to recover lost information from digital devices; computer and mobile forensics capabilities, including the collection, analysis and interpretation of data from computers, mobile devices such as smartphones and tablets for use in criminal cases; research on the In addition, digital media analysis (Digital Media

Analysis) is gaining momentum, which includes the analysis of images, video and audio files to detect fakes, manipulations or other evidence; digital steganography (Digital Steganography) - the study and disclosure of hidden information in digital images, video or audio files [2, p. 218-219].

In the realities of war, artificial intelligence has become essential for ensuring the country's security and collecting evidence of criminal behaviour in the digital sphere. Today, in the modern military environment, the following areas of digital forensics are important: obtaining information from mobile devices, phones seized from the defendants; obtaining information from personal computers; obtaining information from servers and other storage media of institutions and organisations; obtaining information from radio frequency identifiers, GPS trackers, sensors, video surveillance and positioning; information, as well as from networked snrvis.

Before digital evidence can be presented in court as direct or indirect evidence, it must be recognised (i.e., it must be shown to be relevant to the intended purpose). To illustrate the practice of authentication, the following examples of digital evidence can be cited: 1) content generated by one or more persons (for example, the text of an email or instant message and documents in a text editor such as Microsoft Word); 2) content generated by a computer or digital device without the user's participation (for example, data logs); 3) content generated simultaneously by the user and the device (for example, dynamic tables in programs such as Microsoft Excel, which include data entered by the user and calculations performed by the program) [4, p. 372].

However, digital forensics has certain disadvantages: 1) digital evidence is admissible in court. However, it must be proved that there has been no tampering; 2) the production of electronic records and their storage is extremely expensive; 3) investigators must have extensive computer knowledge; 4) reliable and convincing evidence must be provided; 5) if the tool used for digital forensics does not meet the specified standards, the evidence may be rejected by the court; 6) the lack of technical knowledge of the investigator may not give the desired result [4, p. 374].

At the present stage, the main direction of development of forensic science is the creation and development of the field of technical and forensic investigation of digital data. As a result, the relevant tools and methods have not yet found their place in the national forensic system. Therefore, there is an urgent need to create a separate section of forensic technology dedicated to the forensic examination of digital evidence, with scientific provisions of digital forensics as a branch of forensic science adapted to the realities of domestic law enforcement practice and forensic theory.

Conclusions. An analysis of the development of digital forensics shows that the rapid spread of digital technologies in all spheres of life has significantly changed the way crimes are committed, including in cyberspace. Digital forensics, as a new field of science, responds to these challenges by providing effective investigation of digital traces to detect, investigate and prevent crimes.

The imposition of martial law in Ukraine and the aggression of the Russian Federation have significantly affected the development of forensic science, highlighting the need for innovative approaches to countering military and cyber threats. In this context, digital forensics is becoming a strategic direction in the criminal justice system, especially in the study of war crimes and cybercrime.

Література

1. Братішко Н. Напрями використання цифрової криміналістики в умовах воєнного стану. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2023. № 2. С. 282-288. DOI: https://doi.org/10.31733/2078-3566-2023-6-282-288

2. Грекова Л.Ю., Павроз Д.О. Цифрова криміналістика: формування та роль у забезпеченні безпекового середовища України. *VII Міжнародний молодіжний науковий юридичний форум:* матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 трав. 2024 р. С. 217-220. URL: http://dspace.nau.edu.ua: 8080/handle/NAU/63863

3. Редька Я.О. Цифрова криміналістика: виклики, методи та перпективи в сучасних умовах. *VII Міжнародний молодіжний науковий юридичний форум:* матеріали форуму, м. Київ, Національний авіаційний університет,

16-17 трав. 2024 р. С. 287-290. URL: https://er.nau.edu.ua/handle/NAU/63857

4. Світличний В.А. Цифрова криміналістика: особливості, можливості та перспективи. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану:* матеріали Міжнар. наук.-практ. конф. (м. Харків, 25 лист. 2022 р.). Харків: Харківський нац. ун-т внутріш. справ, 2022. С. 371-375.

5. Шевчук В.М. Цифрова криміналістика: воєнні виклики сьогодення та нові завдання у сучасних умовах. *Правові виклики сучасності:* матеріали всеукраїнського круглого столу (м. Харків, 20 груд. 2022 р.). Харків: Державний біотехнологічний університет, 2022. С. 35-39. URL: http://btu.kharkov.ua/wp-content/uploads/2023/01/mater-kr-stil-20-12-22.pdf

6. Шевчук В.М. Цифрова криміналістика: формування та роль у забезпеченні безпекового середовища України. *Нова архітектура безпекового середовища України:* зб. тез Всеукр. наук.-практ. конф. (м. Харків, 23 груд. 2022 р.). Харків: Юрайт, 2022. С. 146-150.

7. Шепітько В.Ю., Шепітько М.В. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 2021. № 8. С. 12–27. DOI: https://doi.org/10.33498/louu-2021-08-012

References

1. Bratishko N. Napryamy vykorystannya tsyfrovoyi kryminalistyky v umovakh voyennoho stanu. *Naukovyy visnyk Dniprovskoho derzhavnoho universytetu vnutrishnikh sprav.* 2023. № 2. S. 282-288. DOI: https://doi.org/10.31733/2078-3566-2023-6-282-288

2. Hrekova L.Yu., Pavroz D.O. Tsyfrova kryminalistyka: formuvannya ta rol u zabezpechenni bezpekovoho seredovyshcha Ukrayiny. *VII Mizhnarodnyy molodizhnyy naukovyy yurydychnyy forum:* materialy forumu, m. Kyiv, Natsionalnyy aviatsiynyy universytet, 16-17 trav. 2024 r. S. 217-220. URL: http://dspace.nau.edu.ua:8080/handle/NAU/63863

3. Redka Ya.O. Tsyfrova kryminalistyka: vyklyky, metody ta perpektyvy v suchasnykh umovakh. *VII Mizhnarodnyy molodizhnyy naukovyy yurydychnyy forum:* materialy forumu, m. Kyiv, Natsionalnyy aviatsiynyy universytet, 16-17 trav. 2024 r. S. 287-290. URL: https://er.nau.edu.ua/handle/NAU/63857

4. Svitlychnyy V.A. Tsyfrova kryminalistyka: osoblyvosti, mozhlyvosti ta perspektyvy. *Suchasni tendentsiyi rozvytku kryminalistyky ta kryminalnoho protsesu v umovakh voyennoho stanu:* materialy Mizhnar. nauk.-prakt. konf. (m. Kharkiv, 25 lyst. 2022 r.). Kharkiv: Kharkivskyy nats. un-t vnutrish. sprav, 2022. S. 371-375.

5. Shevchuk V.M. Tsyfrova kryminalistyka: voyenni vyklyky sohodennya ta novi zavdannya u suchasnykh umovakh. *Pravovi vyklyky suchasnosti:* materialy vseukrayinskoho kruhloho stolu (m. Kharkiv, 20 hrud. 2022 r.). Kharkiv: Derzhavnyy biotekhnolohichnyy universytet, 2022. S. 35-39. URL: http://btu.kharkov.ua/wp-content/uploads/2023/01/mater-kr-stil-20-12-22.pdf

6. Shevchuk V.M. Tsyfrova kryminalistyka: formuvannya ta rol u zabezpechenni bezpekovoho seredovyshcha Ukrayiny. *Nova arkhitektura bezpekovoho seredovyshcha Ukrayiny:* zb. tez Vseukr. nauk.-prakt. konf. (m. Kharkiv, 23 hrud. 2022 r.). Kharkiv: Yurayt, 2022. S. 146-150.

7. Shepitko V.Yu., Shepitko M.V. Doktryna kryminalistyky ta sudovoyi ekspertyzy: formuvannya, suchasnyy stan i rozvytok v Ukrayini. *Pravo Ukrayiny.* 2021. № 8. S. 12–27. DOI: https://doi.org/10.33498/louu-2021-08-012

Наталя Гольдберг, Вікторія Колонська

ЦИФРОВА КРИМІНАЛІСТИКА В УМОВАХ ВОЄННОГО СТАНУ

Державне некомерційне підприємство
«Державний університет «Київський авіаційний інститут»
проспект Любомира Гузара, 1, 03058, Київ, Україна
E-mails: natalia.holdberh@npp.nau.edu.ua, 7545177@stud.nau.edu.ua

***Метою с**татті є дослідження нової сфери криміналістики – цифрової криміналістки. **Методи дослідження:** у статті використані герменевтичний метод, метод класифікації, логічні прийоми (аналізу, синтезу, індукції, дедукції, узагальнення тощо), метод систематизації. **Результати:** у статті досліджено нову галузь криміналістики, а саме цифрову криміналістику. Цифрова криміналістика набуває все більшого значення і стає однією з основних складових традиційної криміналістики. Знання з цифрової криміналістики використовуються при проведенні багатьох слідчих дій та в процесі призначення відповідних судових експертиз не лише щодо правопорушень у сфері інформаційних технологій, а й при розслідуванні широкого кола злочинів, вчинених під час війни та окупації. **Обговорення:** проаналізовано погляди провідних вчених щодо поняття цифрової криміналістики в системі криміналістичної науки. Оцінено тенденції розвитку цифрової криміналістики на сучасному етапі та спрогнозовано подальший розвиток цього напряму в Україні, проведено правовий аналіз стосовно того, що цифрова криміналістика може використовуватися. Існуюча модель криміналістики в Україні нагально потребує формування окремої галузі криміналістичної техніки, що включає засоби і методи дослідження цифрових доказів. Також досліджуються особливості застосування цифрової криміналістики в умовах воєнного стану. Зокрема, аналізуються нові виклики та можливості, які виникають у зв'язку з активним використанням цифрових технологій у сучасних конфліктах.*

***Ключові слова:** цифрова криміналістика; криміналістика; докази; цифрові технології; злочини; воєнні виклики; воєнний стан; цифрові докази; слідчі; кіберзлочини.*

Стаття на дійшла до редакції 04.12.2024