It is noted that the successful conduct of interrogations in criminal proceedings regarding criminal offenses committed by organized groups or criminal organizations largely depends on proper preparation. Some features of preparation for interrogation of members of an organized group or criminal organization are shown. The most important tactical techniques are given, the use of which reduces the ability of persons who have committed a crime to resist, contributes to the destruction of a conspiracy between suspects, ensures the concealment of the true intentions and goals of the investigation until a certain moment etc.

The need to use video recording of absolutely all interrogations of members of organized groups or criminal organizations in addition to drawing up an interrogation protocol is emphasized

Keywords: forensic provision, forensic tactics, interrogation, interrogation planning, suspect, organized group, criminal organization.

DOI: 10.33766/2786-9156.106.1.180-191
UDC: 342.95

Kovalchuk O., *PhD in Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Theory of Law and Constitutionalism, West Ukrainian National University (Ternopil, Ukraine)*
e-mail: olhakov@gmail.com
ORCID iD: https://orcid.org/0000-0001-6490-9633

MODERN IT SOLUTIONS FOR ENSURING RUSSIA'S ACCOUNTABILITY FOR IT MILITARY AGGRESSION AGAINST UKRAINE

The article examines the information and legal aspects of using information technologies to ensure Russia's accountability for war crimes committed in Ukraine. The advantages and dangers of applying the latest technological solutions and tools actively used by Ukrainian law enforcement agencies to document crimes of Russian aggression are explored. It is noted that innovative solutions based on artificial intelligence, big data analysis, cryptography, and blockchain technologies can significantly increase the efficiency of recording evidence, its authenticity, integrity, and admissibility in litigation. The main challenges regarding the legal force of digital evidence, and the processes of its verification and preservation while respecting human rights have been clarified.

Directions for improving information and legal mechanisms for engaging the latest information technologies solutions to ensure the inevitability of punishment for Russia's war crimes are proposed: creating a national repository of digital evidence; forming a unified information system of electronic evidence of war crimes; developing specialized software systems for identifying perpetrators of crimes. The urgent need to develop, with the participation of international experts, unified standards for the use of IT in trials of war criminals is substantiated.

It is emphasized that only coherent interaction between the legal and technological spheres will ensure the full use of the advantages of modern information technologies for the inevitable punishment of violators of international humanitarian law and for bringing

to justice the highest military and political leadership of the Russian Federation as the organizers of crimes in Ukraine. At the same time, fundamental human rights must not be restricted in any way. A comprehensive approach involving a wide range of experts in the fields of law and IT will help to most effectively employ the latest technological solutions in the interests of justice.

Keywords: information technologies, war crimes, trial, international court, digitalization of justice, information and legal mechanisms, digital evidence, analytical system, accountability.

Problem Statement. With the start of Russia's full-scale invasion of Ukraine on February 24, 2022, the world community was faced with the challenge of documenting numerous war crimes and crimes against humanity committed by Russian troops on the territory of Ukraine. The systematic destruction of civilian infrastructure, illegal deportations, torture of prisoners of war and civilians, and deliberate shelling of residential areas – these and other criminal actions require thorough investigation and recording to bring the perpetrators to justice. However, the scale of hostilities, the vast territory covered by the crimes, and the active phase of combat operations create unprecedented challenges for traditional methods of documenting war crimes. There is an urgent need to engage modern information technologies (IT) such as satellite imagery, video analytics, artificial intelligence (AI), blockchain, etc., which open up new opportunities for rapidly documenting, analyzing, and systematizing various evidence of war crimes, overcoming limitations of physical access. The proper application of these technologies can ensure impartial recording of evidence and create a strong evidence base for future trials.

The article addresses the important scientific issue of developing a methodology for applying the latest IT in the investigation of war crimes. This will optimize the documentation process, increase the reliability of evidence, and ensure compliance with international trial standards. The research results will be of practical significance for the activities of national and international law enforcement and judicial bodies involved in investigating and prosecuting Russia's crimes against Ukraine. They will help develop effective mechanisms for using the latest technologies to bring perpetrators to justice. The relevance lies in the need to systematize knowledge about modern IT methods and tools used to document Russia's war crimes in Ukraine and to study the regulatory and legal mechanisms for their use to hold the aggressor accountable.

Analysis of recent research and publications. To date, there are no substantive scientific works that explore the use of the latest IT solutions as a mechanism to ensure Russia's accountability for military aggression against Ukraine. The full-scale war is ongoing. Moreover, a certain amount of time is needed for an in-depth scientific understanding of this issue. However, several publications and studies partially touch upon this topic. The authors M. Kapustina et al. analyzed the potential of using advanced IT as a tool for effectively investigating war crimes [1]. Researchers Yu. Tymoshenko et al. studied the latest technological solutions in the field of crime investigation with the aim of their pilot implementation and practical testing in the conditions of Ukraine [2]. M. Kostenko and V. Shmyga investigated the state and prospects of applying IT in criminalistics [3]. R. Blahuta examined the current state and problems

of using the latest technologies in crime investigation [4]. S. Luchyk explored the possibilities of applying digital technologies in recording war crimes [5]. Russia's war against Ukraine is unique in world history in terms of the scale of application of the latest technologies, including for recording and investigating crimes. There are no established methods and cases for studying this issue. Therefore, research on the opportunities and limitations of using innovative IT to guarantee the inevitability of Russia's accountability for war crimes in Ukraine is relevant.

Statement of goals. The article aims to explore the advantages and challenges of using innovative technological solutions for recording and investigating Russia's war crimes in Ukraine and to outline the legislative framework and regulations regarding the use of IT to ensure Russia's accountability for the crime of aggression.

Main part. The full-scale war launched by Russia against Ukraine on February 24, 2022, has been accompanied by unprecedented war crimes and violations of international humanitarian law for the third year now. Ukrainian law enforcement agencies are making tremendous efforts to record, investigate and document the criminal actions of Russian troops on the territory of our state. Careful collection of evidence and establishing an objective picture of events is critically important to ensure the inevitable accountability of the Russian Federation for aggression and terror against the civilian population.

Investigators of the National Police of Ukraine have already documented nearly 125,000 war crimes committed by the Russian Federation over the 2 years of full-scale war. These include deliberate killings of civilians; torture, inhumane treatment, rape, sexual violence; deliberate shelling of residential areas, civilian infrastructure; use of prohibited weapons; hostage-taking, unlawful deprivation of liberty of civilians; deportation of civilians to Frssia; looting, destruction of private property, cultural values; use of human shields (using civilians as living cover); deliberate attacks on sites marked with UN and other humanitarian organizations' emblems; looting, robbery, violence against the civilian population; war crimes against prisoners of war (torture, insulting treatment); deliberate obstruction of civilian evacuation from dangerous areas. These various war crimes are systematically documented to bring the guilty Russian military and political leadership to justice [6]. War crimes are the most serious violations of international humanitarian law, for the commission of which not only the direct perpetrators but also their commanders are held responsible [7].

The number of cases regarding war crimes is constantly increasing, as law enforcement officers continue to record new episodes of Russia's military aggression in the de-occupied territories. Investigating these crimes requires a colossal amount of work in collecting evidence, interviewing witnesses, and analyzing video and photo materials. Conducting such large-scale investigations is unprecedented and requires the engagement of the latest IT, international cooperation, and financial assistance. To identify individuals involved in committing war crimes on the territory of Ukraine, employees of the National Police are using a wide range of advanced innovative technological solutions and tools. Among them [8]:

1. Facial recognition systems contain giant databases with over 30 billion images collected from open sources on the internet. These software systems allow identifying potential perpetrators by comparing their photographs with arrays of visual data.

2. Specialized software tools for searching and verifying the accounts of suspected criminals on popular social networks. In particular, tools such as Clearview for identifying accounts by photos and Artellence for verifying social media profiles are used.

3. Satellite communication technologies, as well as analytical systems for processing video and photo materials obtained from seized mobile devices, video surveillance cameras, including the "Safe City" system, etc.

4. OSINT (Open Source Intelligence) methods for collecting, analyzing, and using open photo, video, and text data from the internet to detect signs of criminal activity.

5. The interagency unified database "War Crime", was created by specialists of the National Police. It contains information about over 550,000 potential war criminals, details of offenses committed by them, and collected evidence related to Russia's armed aggression against Ukraine.

Access to the "War Crime" subsystem has been provided to all Ukrainian security forces and defense agencies. This is an unprecedented case of interagency consolidation to administer justice over the aggressor country in national and international judicial instances. There is also an active exchange of relevant data with Europol, Eurojust, and other international partners assisting Ukraine in investigating war crimes [8].

In addition to the technological tools mentioned above, Ukrainian criminologists, together with their foreign colleagues, are also using other advanced means: unmanned aerial vehicles to record the consequences of missile strikes, modern 3D scanners to create detailed spatial models of crime scenes, rapid DNA analyzers for quick identification of individuals by genetic material.

During the investigation of Russia's war crimes in Ukraine, law enforcement agencies have conducted hundreds of thousands of site inspections, searches, investigative experiments, interrogations, and other necessary procedural actions. Combined with the use of the latest technologies, evidence has been collected to bring over 2,400 charges, about half of which have already been sent to court [8]. Ensuring that all collected evidence meets international standards is a priority, so that it can be used in the future to convict Russian war criminals in national courts, as well as to bring the highest political and military leadership of the Russian Federation to criminal responsibility in international courts and ensure payment of reparations to Ukraine for the damage caused [9, 10].

Ukraine is actively implementing and using advanced technological solutions for the systematic documentation, investigation, and accountability of war crimes committed by Russian forces. Unlike previous armed conflicts, where attention was focused mainly on crimes against the physical integrity of people – killings, injuries, attacks, and humiliations, in the context of modern warfare, the Office of the Prosecutor General of Ukraine considers a wider range of war crimes. In particular, cases of

sexual violence, and crimes against the environment, such as damage to nuclear facilities, destruction and pollution of the environment, which will have long-term negative consequences for the health of Ukrainians for many generations, are being actively investigated. Cyber attacks are also being studied in the context of their qualification as war crimes.

One of the most difficult tasks is identifying specific individuals who committed crimes. In such cases, the latest IT is often the only effective tool. During investigations, technological solutions from Palantir for big data analysis, as well as Microsoft tools for voice recognition, are actively used, for example, in cases of incitement to genocide or aggression. These are unique tools that help comprehensively analyze and properly record the evidence base. AI-based technologies are involved in processing hundreds of terabytes of video and photo materials. The use of the latest technologies makes it possible to identify perpetrators and collect all the necessary evidence for subsequent fair trials. The development of such technological tools is important not only for identifying criminals but also for preventing the loss of evidence on which charges can be based [11].

The Ministry of Digital Transformation of Ukraine has created a series of chatbots for crowdsourcing and corroborating evidence of probable war crimes. Digital tools have been developed to enable citizens to document damage to their homes. Facial recognition software is being used to identify Russian soldiers in photographs. New tools have been introduced that help users add geotags and timestamps to videos, which can help authorities hold the perpetrators accountable. Official chatbots and websites classify different types of war crimes and human rights violations. All information is stored in a centralized database created by the Office of the Prosecutor General of Ukraine [12].

The use of digital tools in the combat zone has great potential for quickly collecting evidence of war crimes, ensuring their authenticity and integrity through cryptographic methods. The availability of powerful smartphones and other gadgets to many civilians allows them to record photo and video evidence of violations directly at the scene. These materials can be promptly transmitted to human rights organizations and investigators for investigating crimes. The use of specialized software makes it possible to overlay digital timestamps, geolocation metadata, and cryptographic hashes on the collected files. This increases the reliability of evidence and protects it from further changes or manipulation. Digital blockchains can be used to create an immutable timestamped ledger that records and stores all evidence in a distributed repository. This prevents the loss or substitution of evidentiary information. Advanced public-key cryptographic technologies enable the formation of secure digital signatures for authenticating the source of evidentiary materials. Cloud services and distributed networks provide backup storage of digital evidence in different locations, minimizing the risk of its loss or destruction. Digital tools help avoid chain of custody issues typical for physical materials. Cryptographically proven authenticity and transparency of origin significantly increase the legal force of digital evidence when prosecuting war crimes [13, 14].

The use of IT for documenting war crimes is regulated by several international and domestic legislative acts. The Geneva Conventions of 1949 [15] and the Additional Protocols to them of 1977 [16] establish general norms for the protection of victims of armed conflicts and regulate the use of certain methods and means of warfare. The Statute of the International Criminal Court defines the jurisdiction and powers of the ICC to investigate and prosecute war crimes [17]. Some UN Security Council resolutions call on states to use appropriate technologies to record violations of international humanitarian law [18]. The UN Guiding Principles on Collecting Digital Evidence provide recommendations on the proper collection, storage, and exchange of digital data in investigations [19].

Ukrainian legislation also provides for legal norms regarding the use of IT for building an evidentiary base of war crimes. The Criminal Procedural Code of Ukraine regulates the procedure for collecting, recording, and using evidence, including that obtained through information technologies [20]. The Law "On Combating Terrorism" provides for the use of the latest information and telecommunication systems to counter terrorism [21]. Order No. 298 of the Office of the Prosecutor General of Ukraine defines the procedure for documenting war crimes committed by the Russian Federation, including the use of geoinformation systems and other IT tools [22]. In addition, Ukraine is actively cooperating with international organizations and private IT companies to involve the latest digital solutions based on AI, big data analysis, etc. Standards and protocols for collecting and using digital evidence in investigations are being developed.

Ukrainian legislation provides for comprehensive measures for the wide involvement of the latest IT in the processes of investigating and documenting Russian aggression, which is part of the overall digitalization of justice:

– creation of the Unified Register of Pre-Trial Investigations of War Crimes – a centralized electronic database to accumulate all information about the facts, locations, participants, and circumstances of war crimes committed by the Russian Federation on the territory of Ukraine [22];

– formation of the Unified Information System of Electronic Evidence of War Crimes, which should ensure the collection, processing, storage, and exchange of digital data between all involved law enforcement agencies [23];

– development and implementation of specialized software systems and databases for automated identification of perpetrators of war crimes based on analysis of video, photo, audio, and biometric data;

– regulation of the use of the latest geoinformation systems, unmanned aerial vehicles, and high-resolution satellite imagery to record the destruction of civilian infrastructure;

– establishment of interagency and international cooperation in the exchange of digital evidence of war crimes, ensuring its proper preservation and protection from unauthorized access;

– creation of a national repository of digital evidence of war crimes with a high level of protection for their long-term storage and use in future trials;

– expanding the capabilities of expert institutions to conduct various types of information technology expertise of digital materials in cases of war crimes.

The application of digital technologies for recording and investigating war crimes undoubtedly opens up new opportunities, but it also poses certain challenges related to the legal force of such evidence, its proper recording and verification, as well as ensuring the right to a fair trial. In particular, digital evidence collected using the latest technologies may raise doubts about its authenticity, integrity, and reliability of origin. Clear standards are needed to ensure a proper chain of custody and the ability to confirm the authenticity of each piece of evidence [11].

The development of transparent and unified protocols for methods of collecting, processing, storing, and transferring digital evidence is necessary. This will minimize the risk of accidental or intentional damage or forgery. The verification process must guarantee the absence of manipulation with evidence.

The use of digital technologies must not violate fundamental human rights, in particular the right to a fair trial. It is necessary to ensure compliance with the principles of impartiality, equality of parties, the right to privacy, etc. when using IT tools for collecting evidence.

Considering these challenges, it is extremely important to develop unified international standards and regulations for the use of IT in judicial proceedings for the prosecution of war crimes. Such standards should cover: 1) requirements for the collection, recording, storage, and transfer of digital evidence using cryptographic protection and means of authentication; 2) procedures for verifying evidence and establishing its reliability and proper origin; 3) regulations for the submission of digital materials in courts, adhering to the principles of a fair trial; 4) issues of personal data protection and confidentiality when using IT systems for evidence; 5) unified requirements for software and hardware involved in the processing of digital evidence. The development of such international standards should involve experts from IT, forensics, judicial bodies, and human rights organizations. Only a comprehensive approach will ensure the proper use of the advantages of modern technologies in the process of prosecuting the most serious crimes without violating human rights.

Against the backdrop of unprecedented use of cutting-edge technologies for committing and concealing war crimes, improving information and legal mechanisms becomes a guarantee of the inevitability of punishment for violators of international law. Only coordinated interaction between the legal and IT spheres will ensure adherence to the principles of justice and human rights.

Conclusions. The paper explores the advantages of using the latest IT for effective documentation and investigation of war crimes committed by Russia in Ukraine. The application of innovative AI-based solutions, big data analysis, cryptography, blockchain technologies, etc. significantly increases the efficiency of evidence recording, its authenticity, and integrity. This creates a strong evidentiary base for future trials. The main challenges regarding the legal force of digital evidence, and the processes of its verification and preservation while respecting human rights are outlined. The urgent need to develop international standards and regulations for the use of IT

in documenting war crimes is identified. The current international and national legislation regulating the use of IT in the processes of investigation and prosecution of crimes of aggression is analyzed. The set of measures for the digitalization of judicial proceedings implemented in Ukraine is highlighted. Directions for improving information and legal mechanisms for engaging the latest IT solutions to ensure the inevitability of punishment for Russia's war crimes are proposed. Among the key proposals: are the creation of a national repository of digital evidence, the formation of a unified information system of electronic evidence of war crimes, development of specialized software systems for identifying perpetrators of crimes. It is established that only close cooperation between the legal and IT environments, and comprehensive implementation of technological innovations in compliance with international standards, will be able to ensure effective prosecution of the Russian Federation for military aggression against Ukraine. Further improvement is required for the legal acts regulating the use of IT for documenting war crimes. This will provide proper legal guarantees for holding the aggressor country accountable for crimes committed during the war against Ukraine.

Further directions of our research will be to study the issues of introducing possible amendments to the procedural codes (criminal, civil, etc.) to clearly define the procedure for collecting, recording, storing, and using digital evidence in court proceedings; develop special legislative acts that will regulate the admissibility of various types of digital evidence, requirements for their authenticity and integrity; implementation of international standards and best practices for using IT in the processes of documenting war crimes into national legislation.

References:

1. Kapustina, M. V., Demydova, Ye. Ye., & Latysh, K. V. (2023). The Use of Modern Information Technologies in the Investigation of War Crimes. *Legal Scientific Electronic Journal*, *4, 544–546*. DOI : https://doi.org/10.32782/2524-0374/2023-4/134. [in English].

2. Tymoshenko, Y. P., Kozachenko, O. I., Kyslenko, D. P., Horodetska, M. S., Chubata, M. V., & Barhan, S. S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). Amazonia Investiga, *11(51), 149–160*. DOI : https://doi.org/10.34069/AI/2022.51.03.14. [in English].

3. Kostenko, M. V., & Shmyga, V. O. (2022). Innovatsiini tekhnolohii u kryminalistytsi: suchasnyi stan ta perspektyvy. *Yurydychnyi naukovyi elektronnyi zhurnal – Legal Scientific Electronic Journal*, *9*, *316–318*. URL: http://lsej.org.ua/9_ 2022/76.pdf. [in Ukrainian].

4. Blaguta, R. I. (2020). Novitni tekhnolohii u rozsliduvanni zlochyniv: suchasnyi stan i problemy vykorystannia : monohrafiia / Blahuta R. I., Movchan A. V. (Eds.) Lviv. URL : https://library.megu.edu.ua:9443/jspui/handle/123456789/2449. [in Ukrainian].

5. Luchyk, S. D., & Stolyk, D. (2023) Zastosuvannia tsyfrovykh tekhnolohii u fiksatsii voiennykh zlochyniv. *Mizhnarodna naukovo-praktychna konferentsiia "Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia"(Odesa, 17 lystop. 2023 roku). – International Scientific and Practical Conference "Cybersecurity in Ukraine: Legal and Organizational Issues" (Odesa, November, 17, 2023 roku)*. N. p. URL: https:// dspace.univd.edu.ua/handle/123456789/19915. [in Ukrainian].

6. Ofitsiinyi vebportal – Ofis Heneralnoho Prokurora. (N. d.) N. p. URL : https:// www.gp.gov.ua. [in Ukrainian].

7. Ofitsiinyi veb-portal – Ofis Heneralnoho Prokurora. (N. d.) N. p. URL : https://zakon.rada.gov.ua/laws/show/995_588#Text. [in Ukrainian].

8. Ofitsiinyi veb-portal – Natsionalna politsiia Ukrainy. (N. d.) N. p. URL : https://www.npu.gov.ua/news/politseiski-predstavyly-rezultaty-rozsliduvannia-voien nykh-zlochyniv-v-ukraini-na-shchorichnomu-zasidanni-ekspertiv-v-haazi. [in Ukrainian].

9. Teremetskyi, V., Zhuravlov, D., Boiko, V., Stratonov, V., Ilchenko, O., Glukh, M., & Chudyk, N. (2023). Organization of courts operation in Ukraine in the period of martial law: comparative and legal research. *Revista de Gestão e Secretariado. Management and Administrative Professional Review*, *14(10), 18976–18991*. DOI: https://doi.org/10.7769/gesec. v14i10.2945. [in English].

10. Onishchenko, N., Teremetskyi, V., Bila, V., Chechil, Yu., & Kostenko, M. (2023). Judicial and extrajudicial proceedings to compensate for damages caused by armed conflicts: experience of Ukraine. *Lex Humana*, *15(3), 522–537*. URL: https://seer.ucp.br/seer/index.php/LexHumana/article/view/2663/3585. [in English].

11. Bergengruen, V. (2023). How Ukraine is Pioneering New Ways to Prosecute War Crimes. *Time*. N. p. URL : https://time.com/ 6331902/ukraine-war-crimes-prosecutor. [in English].

12. Bergengruen, V. (2022). How Ukraine Is Crowdsourcing Digital Evidence of War Crimes. *Time*. N. p. URL : https://time.com/6166781/ukraine-crowdsourcing-war-crimes/. [in English].

13. Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & Miranda, F. P. d. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. *J. Risk Financial Manag*, *16*, *360*. DOI : https://doi.org/10.3390/jrfm16080360. [in English].

14. Ali, M., Ismail, A., Elgohary, H., Darwish, S., & Mesbah, S. (2022). A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. *Symmetry*, *14*, *334*. DOI: https://doi.org/10.3390/sym 14020334. [in English].

15. Zhenevski konventsii pro zakhyst zhertv viiny 1949 roku. *Obudsman Ukrainy*. (N. d.) N. p. URL : https://www.ombudsman.gov. ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku. [in Ukrainian].

16. Dodatkovyi protokol do Zhenevskykh konventsii vid 12 serpnia 1949 roku, shcho stosuietsia zakhystu zhertv mizhnarodnykh zbroinykh konfliktiv (Protokol I), vid 8 chervnia 1977 r. *Verkhovna Rada Ukrainy*. (N. d.) N. p. URL : https://zakon. rada.gov.ua/laws/show/995_199#Text. [in Ukrainian].

17. Rymskyi statut mizhnarodnoho kryminalnoho sudu. *Verkhovna Rada Ukrainy*. (N. d.) N. p. URL : https://zakon.rada.gov.ua/laws/show/995_588#Text. [in Ukrainian].

18. Rezoliutsii. Rada bezpeky OON. (N. d.) N. p. URL : https://www.un.org/ securitycouncil/ru/content/resolutions. [in Ukra-inian].

19. Guidelines First Responders on the Collection of Digital Devices in the Battlefield. (2023) UNCCT. New York. URL : https://www.un.org/counterterrorism/sites/www.un.org. counterterrorism/files/guide-first_responders-digital_devices_in_battlefield.pdf. [in English].

20. Kryminalnyi kodeks Ukrainy: Zakon Ukrainy vid 05.04.2001 No. 2341-III. (2001) N. p. URL: https://zakon.rada.gov.ua/laws/ show/2341-14#Text. [in Ukrainian].

21. Pro borotbu z teroryzmom: Zakon Ukrainy vid 20.03.2003 No. 638-IV. (2003) N. p. URL: https://zakon.rada.gov.ua/laws/show/ 638-15#Text. [in Ukrainian].

22. Pro zatverdzhennia Polozhennia pro Yedynyi reiestr dosudovykh rozsliduvan, poriadok yoho formuvannia ta vedennia: Nakaz OHP Ukrainy vid 30.06.2020 No. 298. (2020) N. p. URL : https://zakon.rada.gov.ua/laws/show/v029 8905-20#Text. [in Ukrainian].

23. Deiaki pytannia zabezpechennia funktsionuvannia Derzhavnoho reiestru maina, poshkodzhenoho ta znyshchenoho vnaslidok boiovykh dii, terorystychnykh aktiv, dyversii, sprychynenykh zbroinoiu ahresiieiu Rosiiskoi Federatsii proty Ukrainy: Postanova Kabinetu Ministriv Ukrainy vid 13 chervnia 2023 r. No. 624. (2023) N. p. URL: https://zakon.rada.gov.ua/laws/show/624-2023-%D0 %BF#Text. [in Ukrainian].

Використані джерела:

1. Капустіна М. В., Демидова Є. Є., Латиш К. В. Використання сучасних інформаційних технологій при розслідуванні воєнних злочинів. *Юридичний науковий електронний журнал*. 2023. № 4. С. 544–546.

2. Tymoshenko Y. P., Kozachenko, O. I., Kyslenko D. P., Horodetska M. S., Chubata M.V., Barhan S. S. Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga*. 2022. Vol. 11(51). Pp. 149–160.

3. Костенко М. В, Шмига В. О. Інноваційні технології у криміналістиці: сучасний стан та перспективи. *Юридичний науковий електронний журнал*. 2022. Вип. 9. С. 316–318.

4. Благута Р. І. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія / Благута Р. І., Мовчан А. В. Львів. 2020. 256 с.

5. Лучик С. Д., Столик Д. Застосування цифрових технологій у фіксації воєнних злочинів. Міжнародна науково-практична конференція "Кібербезпека в Україні: правові та організаційні питання" (м. Одеса, 17 листоп. 2023 року). С. 45–47.

6. Офіційний вебпортал – Офіс Генерального Прокурора. URL: https://www.gp. gov.ua. (дата звернення: 05.05.2024)

7. Римський статут Міжнародного кримінального суду. URL : https://zakon.rada.gov.ua/laws/show/995_588#Text. (дата звернення: 05.05.2024)

8. Офіційний вебпортал – Національна поліція України. URL : https://www.npu.gov.ua/news/politseiski-predstavyly-rezultaty-rozsliduvannia-voiennykh-zlochy niv-v-ukraini-na-shchorichnomu-zasidanni-ekspertiv-v-haazi. (дата звернення: 05.05. 2024)

9. Teremetskyi V., Zhuravlov D., Boiko V., Stratonov V., Ilchenko O., Glukh M., Chudyk N. Organization of courts operation in Ukraine in the period of martial law: comparative and legal research. *Revista de Gestão e Secretariado. Management and Administrative Professional Review*. 2023. Vol. 14(10). Pp. 18976–18991.

10. Onishchenko N., Teremetskyi V., Bila V., Chechil Yu., Kostenko M. Judicial and extrajudicial proceedings to compensate for damages caused by armed conflicts: experience of Ukraine. *Lex Humana*. 2023. Vol. 15(3). Pp. 522–537.

11. Bergengruen V. How Ukraine is Pioneering New Ways to Prosecute War Crimes. Time (2023, April 19). URL : https://time.com/ 6331902/ukraine-war-crimes-prosecutor.

12. Bergengruen, V. How Ukraine Is Crowdsourcing Digital Evidence of War Crimes. Time (2022, April 18). URL: https://time.com/6166781/ukraine-crowd sourcing-war-crimes/.

13. Batista D., Mangeth A. L., Frajhof I., Alves P. H., Nasser R., Robichez G., Silva G. M., Miranda F. P. d. Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. *J. Risk Financial Manag*. 2023. Vol. 16. Art. 360.

14. Ali M., Ismail A., Elgohary H., Darwish S., Mesbah S. A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. *Symmetry*. 2022. Vol. 14. Art. 334.

15. Женевські конвенції про захист жертв війни 1949 року. *Обудсман України*. URL : https://www.ombudsman.gov.ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku. (дата звернення: 05.05.2024)

16. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text. (дата звернення: 05.05.2024)

17. Римський статут міжнародного кримінального суду. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text. (дата звернення: 05.05.2024)

18. Резолюції. Рада безпеки ООН. URL : https://www.un.org/securitycouncil/ru/content/resolutions. (дата звернення: 05.05.2024)

19. Guidelines First Responders on the Collection of Digital Devices in the Battlefield. UNCCT. New York, 2023. 60 p. URL: https:// www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/guide-first_responders-digital_devices_ in_battlefield.pdf.

20. Кримінальний кодекс України: Закон України від 05.04.2001 No 2341-III. URL: https://zakon.rada.gov.ua/laws/show/ 2341-14#Text. (дата звернення: 05.05.2024)

21. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV. URL : https://zakon.rada.gov.ua/laws/show/638-15#Text. (дата звернення: 05.05. 2024)

22. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: Наказ ОГП України від 30.06.2020 № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text. (дата звернення: 05.05.2024)

23. Деякі питання забезпечення функціонування Державного реєстру майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України: Постанова Кабінету Міністрів України від 13 червня 2023 р. № 624. URL: https://zakon.rada.gov.ua/laws/show/624-2023-%D0%BF#Text. (дата звернення: 05.05.2024)

Стаття надійшла до редколегії 06.05.2024

Ковальчук О. Я., *кандидат фізико-математичних наук, доцент, доцент кафедри теорії права та конституціоналізму Західноукраїнського національного університету (м. Тернопіль, Україна)*

СУЧАСНІ ІТ-РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАЛЬНОСТІ РОСІЇ ЗА ЇЇ ВІЙСЬКОВУ АГРЕСІЮ ПРОТИ УКРАЇНИ

У статті досліджено інформаційно-правовий аспект використання інформаційних технологій для забезпечення відповідальності росії за воєнні злочини, скоєні в Україні. Досліджено переваги та небезпеки застосування новітніх технологічних рішень та інструментів, що активно використовуються українськими правоохоронними органами для документування злочинів російської агресії. Зазначено, що інноваційні рішення на основі штучного інтелекту, аналізу великих даних, криптографії та технологій блокчейн можуть значно підвищити оперативність фіксації доказів, їх автентичність, цілісність та допустимість у судочинстві. З'ясовано основні виклики

щодо юридичної сили цифрових доказів, процесів їх верифікації та збереження в умовах дотримання прав людини.

Запропоновано напрями вдосконалення інформаційно-правових механізмів залучення новітніх ІТ-рішень для забезпечення невідворотності покарання за воєнні злочини росії: створення національного сховища цифрових доказів; формування єдиної інформаційної системи електронних доказів воєнних злочинів; розробка спеціалізованих програмних комплексів для ідентифікації виконавців злочинів. Обґрунтовано нагальну необхідність розробки за участі міжнародних експертів уніфікованих стандартів застосування ІТ у судових процесах над воєнними злочинцями. Наголошено, що лише злагоджена взаємодія правової і технологічної сфер забезпечить повноцінне використання переваг новітніх ІТ для невідворотного покарання порушників норм міжнародного гуманітарного права та притягнення до відповідальності вищого військового й політичного керівництва рф як організаторів злочинів в Україні. При всьому жодним чином не повинні бути обмежені основоположні права людини. Комплексний підхід із залученням широкого кола фахівців галузей права та ІТ допоможе максимально ефективно задіяти новітні технологічні рішення в інтересах правосуддя.

Ключові слова: інформаційні технології, воєнні злочини, судовий процес, міжнародний суд, цифровізація судочинства, інформаційно-правові механізми, цифрові докази, аналітична система, притягнення до відповідальності.

DOI: 10.33766/2786-9156.106.1.191-203
УДК: 343.98

Степанюк Р. Л., *доктор юридичних наук, професор, професор кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ (м. Харків, Україна)*
e-mail: stepanuk2@ukr.net
ORCID iD: https://orcid.org/0000-0002-8201-4013

РОЗВІДКА У КРИМІНАЛІСТИЦІ Й ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Статтю присвячено аналізу сучасного стану адаптації зарубіжної термінології щодо кримінальної розвідки до вітчизняної наукової доктрини криміналістики й оперативно-розшукової діяльності. Визначено основні напрями впровадження деяких галузей кримінальної розвідки в теорію і практику кримінального розслідування. Зауважено, що в нинішніх умовах значення методів пошуку й аналізу інформації в різних її джерелах і масивах постійно зростає. Широкомасштабна військова агресія проти України, яка досі триває, ще більше актуалізувала потребу застосування новітніх пошукових засобів і методів задля розслідування пов'язаних із війною кримінальних правопорушень, встановлення жертв війни, розшуку осіб, які вчинили тяжкі злочини в умовах конфлікту. Зазначено, що у вітчизняній системі наук кримінально-правового циклу виникають труднощі, пов'язані з теоретичним обґрунтуванням і практичним впровадженням розвідувальних інструментів у практику кримінa-