DOI https://doi.org/10.30525/978-9934-26-686-7-11

OSINT TECHNOLOGIES IN LAW ENFORCEMENT: INNOVATIONS AND AREAS OF APPLICATION DURING MARTIAL LAW AND THE COUNTRY'S POST-WAR RECOVERY

Nehrebetskyi V.V.

INTRODUCTION

Modern armed conflicts have radically transformed not only the conduct of hostilities but also the ways in which they are documented and proved in criminal proceedings. The digitalization of communications; the mass availability of mobile devices with cameras, livestreams, and geolocation services; the development of satellite observation; and the emergence of new data-sharing platforms have created an unprecedentedly dense information environment. In such an environment, open sources − social networks, video hosting platforms, web archives, satellite platforms, state registers, and other digital resources − become a fully-fledged basis for building the evidentiary record.

Since the start of the full-scale war, the intensity and diversity of digital traces of war crimes have increased sharply. Videos and photos of the aftermath of shelling, fragments of live broadcasts from the scene, eyewitness accounts on social media, Telegram channels, and arrays of satellite observation have, in near-real time, formed a new evidentiary base for law enforcement agencies. The search for reliable tools to identify those involved in war crimes, to localize the places where they were committed, and to verify causal links naturally directed domestic law enforcement agencies to OSINT as a practice-tested, systematized approach to working with open digital data.

A key advantage of OSINT is the speed and scalability of event capture. This is not only about the 'first alert' from social networks, but also about the ability to build spatio-temporal reconstructions: geolocating frames by distinctive terrain features; comparing them with before/after satellite series; overlaying them with air-raid chronicles or systematic time stamps to narrow the 'time window' to procedurally acceptable limits. Given the limited access to crime scenes in active combat zones, these methods have become a bridge between operational response and subsequent 'classic' investigative and procedural actions.

OSINT has catalyzed interagency interaction and international cooperation. Joint analytical projects, consolidation of verified geolocations in open databases, and the exchange of methodologies and tools with civic initiatives and academic centers have created an 'ecosystem of trust' in which quality standards are gradually being unified[1]. Thus, the turn to OSINT has not been a situational response to the lack of access to scenes, but an element of the structural modernization of law enforcement

[1] OSINT-розвідка у роботі журналістів. URL: https://youcontrol.com.ua/articles/osint-in-journalists-work/

in the digital era, ensuring both promptness and legal viability of evidence during wartime and the post-war period.

The use of modern information technologies, including open-source information gathering, in criminal proceedings has been the focus of academic events and the works of many legal scholars as G. K. Avdeeva, V. S. Batyrgareeva, V. I. Borisov, T. Ya.Gnidets, O. M. Borshchevskaya, S. S. Voznyuk, V. I. Grishko, Yu. I. Dmitrik, I. V. Zhukevich, I. O. Osnova, K. V. Dubonos, N. M. Dyachenko, V. A. Zhuravel, V. P. Zakharov, A. O. Ignatovich, O. Ya. Kovalchuk, R. S. Kozyakov, V. O. Konovalova, T. M. Lemekha, a.m. Lysenko, O. A. Lokhmatov, T. V. Ognevyuk, O. S. Mel-nik, A. O. Moroz, I. V. Oleshko, Yu.V.Osadchaya, O. V. Plahotnik, Yu. S. Razmetaeva, O. V. Rybalsky, V. I. Rudeshko, V. I. Solovyov, L. I. Sopilnik, A.V. Stolitny, I. O. Suprun, E. A. Timoshenko, V. I. Teremetsky, V. V. Topchy, A. O. Fesenko, V. G. Khakhanovsky, L. M. Khmelnichy, R. Yu. Tsarev, V. A. Shvets, V. M. Shevchuk, V. Yu. Shepitko, and others[2].

It should be noted that OSINT technologies for detecting and collecting evidentiary information have been covered in the literature from different angles. However, in our view, it is crucial and timely to comprehensively explore the possibilities of implementing OSINT technologies into the procedural activities of criminal justice bodies, considering their innovative potential, functional capabilities, and application areas specifically under the conditions of war in Ukraine. Therefore, studying the trends and potential of OSINT technologies in the applied aspect for the activities of criminal justice authorities and the security and defense sector of Ukraine in investigating and preventing criminal offenses requires further consideration. Given the war, the use of OSINT in investigative units to increase the effectiveness of investigating war crimes and crimes of aggression is particularly urgent.

Accordingly, examining international experience in using OSINT is relevant and, given the need to improve regulatory frameworks in Ukraine, fully justified.

1. Challenges of Regulating the Use of Digital Evidence Technologies During Wartime

From the outset of the full-scale war against Ukraine, the search for tools to identify the perpetrators of war crimes, the locations of such crimes, and information that had surfaced online led domestic law enforcement to OSINT.

The efforts of the Prosecutor General's Office, the Security Service of Ukraine, the National Police of Ukraine, as well as scholars and human rights defenders aimed at

[2] Трансформація завдань криміналістики в умовах воєнного стану та євроінтеграційних процесів : зб. матеріалів наук.-практ. конф. присвяч. пам'яті д-ра юрид. наук, проф. В.О. Коновалової,м. Харків, 28 берез. 2024 р. Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2024; *Методологічні засади криміналістики: традиції та новації* : зб. матеріалів Криміналістичних читань, присвяч.пам'яті акад. В. О. Коновалової, м. Харків, 28 берез. 2025 р. Нац. юрид. ун-т ім. Ярослава Мудрого,Каф. криміналістики; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В.Сташиса Нац. акад. прав. наук України. Харків: Право, 2025; *Роль OSINT-досліджень у підвищенні рівня національної безпеки України* : матеріали круглого столу (м. Львів,7 травня 2025 р.) Львів: ЛьвДУВС, 2025.

introducing OSINT into the practice of detecting and investigating war crimes deserve positive assessment. On 12–13 January 2026, in cooperation with the Training Center for Prosecutors of Ukraine and the National School of Judges, with the support of the Council of Europe's CyberUA project, a specialized training on the use of open sources (OSINT) and electronic evidence in criminal proceedings − focused on cases concerning war crimes and gross human rights violations − was held[3].

First of all, the requirements for electronic evidence under national criminal procedure law and international standards − particularly the Berkeley Protocol − were discussed. The participants reviewed typical categories of open sources and types of electronic evidence and examined procedures for ensuring the chain of custody for electronic evidence in detail.

In 2020, the Office of the UN High Commissioner for Human Rights and the Human Rights Center at UC Berkeley presented a «practical guide on the effective use of digital open-source information for investigating violations of international criminal, human rights, and humanitarian law» that sets out standards and methodological approaches for the collection, preservation, and analysis of open-source information that may be presented as evidence in criminal proceedings[4]. Unfortunately, Ukraine's Criminal Procedure Code does not provide a separate category of digital evidence. It lacks a definition of «digital evidence» and a detailed procedure for its seizure, examination, recording, and storage. Investigators and judges often face difficulties collecting and assessing digital evidence due to the absence of definitions and procedures in Ukrainian law, which may lead to errors and inadmissibility in court[5].

Therefore, leveraging the experience of leading European countries − engaging specialized research institutions and legal experts − to align current criminal procedure law with the demands of the digital era is essential.

The participants also discussed the role of a specialist in OSINT investigations: from proper acquisition and recording of data to explaining technical aspects to the court (metadata, hash values, file validation, detection of editing, etc.). It was emphasized that proper documentation of specialist involvement during inspection when using OSINT in criminal proceedings is important.

Of particular interest was the block on expedited preservation of data under Articles 16–17 of the Budapest Convention on Cybercrime, which allows electronic data to be preserved prior to obtaining proper procedural access. The network of 24/7 contact points, drafting preservation requests, and using mutual legal assistance mechanisms (MLA) to obtain electronic evidence were also discussed.

---

[3] OSINT та електронні докази: юридичні вимоги та практика застосування у кримінальних провадженнях щодо воєнних злочинів в Україні. 14.01.2026. URL: https://www.coe.int/uk/web/kyiv/-/osint-and-electronic-evidence-legal-requirements-and-practical-application-in-criminal-proceedings-on-war-crimes-in-ukraine

[4] Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

[5] Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США (2023). URL: https://khrife-journal.org/index.php/journal/article/download/564/633.

Practice-oriented trainings were also conducted within the Ministry of Internal Affairs system. In October 2025, investigators and operatives of the National Police of Ukraine were trained to master the skills of collecting and using information from publicly available sources in proving war crimes[6]. As part of implementing the UN–Ukraine framework to prevent and combat conflict-related sexual violence, the MIA Human Rights Monitoring Office organized two two-day offline trainings for investigators and operatives on «Using OSINT to Prove Command Responsibility for International Crimes: Theory and Practice».

OSINT not only enables the collection of evidence under conditions of limited access, but also creates the foundation for building evidentiary records in cases concerning war crimes and crimes against humanity, consistent with national and international investigative standards.

The training was organized by the Human Rights Monitoring Department of the Ministry of Internal Affairs of Ukraine and the National Police of Ukraine with the support of the United Nations Development Programme (UNDP) within the framework of the UNDP project «Joint Programme for Ukraine on conflict-related sexual violence Issues», which is funded by the European Union.

During war, the arsenal of traditional forensic tools and forms of collecting evidence of war crimes in Ukraine is significantly limited due to danger to all participants in investigative actions and the impossibility of direct access to the scene[7], necessitating the use of artificial intelligence technologies. Moreover, the European vector of development of forensics and forensic examination in Ukraine is evidenced by the application of European standards of proof during criminal proceedings[8].

By Presidential Decree No. 273/2023 of 11 May 2023, a Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as part of the Security and Defense Sector for 2023–2027 was approved[9]. «Every element of the state system – law enforcement agencies, first of all – must work so that people really feel safe and secure, so that people really feel justice, so that it is guaranteed at the level of institutions, at the level of the everyday work of those by whom people judge the state. Trust in the state, trust in the state are formed from trust in those who act on behalf of the state. Law enforcement officers, the prosecutor's office system are key

[6] Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: навчання НПУ. 08.10.2025.URL: https://npu.gov.ua/news/vykorystannia-osint-u-dokazuvanni-komandnoi-vidpovidalnosti-za-mizhnarodni-zlochyny-navchannia-npu

[7] Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374. DOI: 10.32782/2524–0374/2022–4/88

[8] Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України.* 2022. № 2. С. 87.

[9] Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

in this. Of course, together with everyone else who works in the state apparatus,» emphasized President Volodymyr Zelenskyy[10].

The document was jointly developed by an interagency group, which included the heads of the Prosecutor General's Office, the Ministry of Internal Affairs, the Ministry of Justice, the Security Service of Ukraine, the State Bureau of Investigation, the National Police, the State Border Service, the Border Guard Service, the State Customs Service, as well as representatives of the Office of the President of Ukraine, the Cabinet of Ministers of Ukraine, international experts from the Council of Europe Office in Ukraine, the EUAM, the EU project «PRAVO-JUSTICE», the Law Enforcement Affairs Department of the US Embassy in Ukraine, and the International Development Law Organization (IDLO).

The main goal of the developers of the Plan was to put the focus of the law enforcement, security and defense sectors on the person, his life, health, honor and dignity, rights and legally protected interests. Every Ukrainian should be sure that he lives in safety, has freedom and can count on the mechanisms of justice.

The plan identifies six strategic priorities that will allow modernizing the security sector and bringing it into line with the standards that Ukraine must achieve on its path to EU membership, including:

1. Effectiveness and efficiency of law enforcement agencies and the prosecutor's office as an integral part of the security and defense sector, within which they ensure the national security of Ukraine, including public safety and order, and combat crime, taking into account strategic goals and in accordance with the standards of human rights and fundamental freedoms, including ensuring gender equality.

2. Consistent criminal policy, the priority of which is the prevention of crime, the inevitability of liability, the protection of the individual, society and the state from criminal offenses, and the protection of the interests of the victim.

3. Efficiency of criminal proceedings in compliance with international standards and the rule of law.

4. A result-oriented management system in accordance with established priorities.

5. Comprehensive digital transformation.

6. Openness, transparency, accountability and independence.

The plan provides for a comprehensive digital transformation, in particular:

1. Implementation of a consolidated phased digital transformation of law enforcement agencies and the prosecutor's office based on strategic management tools that comply with EU best practices.

2. Further introduction of innovative technological achievements into the activities of law enforcement agencies and the prosecutor's office that ensure flexibility of operational processes, IT solutions, digital ability to respond promptly to events and changes and achieve results focused on the interests of society.

3. Phased implementation of an electronic system for managing criminal proceedings through comprehensive replacement and modernization of equipment,

[10] Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku.

ensuring compatibility of IT systems, uninterrupted operation, access of all participants in criminal proceedings and interoperability.

4. Increasing the efficiency of law enforcement agencies and the prosecutor's office by ensuring greater accessibility and completeness of information, development and implementation of services on the Unified State Web Portal of Electronic Services.

5. Implementation of security and personal data protection measures in accordance with EU standards.

6. Improvement and implementation of more secure, flexible, capable and accessible communication systems between all law enforcement agencies and other emergency services (including digital radio: voice communication and broadband data transmission).

7. Implementation of a unified personal authentication system and biometric matching system in all law enforcement agencies and prosecutors' offices, gradually ensuring its compatibility with European systems. Widespread use of artificial intelligence, blockchain, cloud computing and other innovative solutions in pre-trial investigations, as well as for data processing and analytical activities of law enforcement agencies and prosecutors' offices.

8. Updating operational processes using IT systems suitable for data exchange with EU institutions in accordance with EU standards.

9. Granting law enforcement agencies and prosecutors the right to direct shared access to automated information and reference systems, registers and databases, the holder (administrator) of which is other state bodies, to ensure the performance of their functions[11].

2. Using Digital Technologies and Open-Source Data in Investigating War Crimes

In today's realities of war and global threats, all practitioners in the field of international criminal justice must improve their technical understanding of cutting-edge AI technologies and cultivate a deeper, up-to-date understanding of how social networks, geolocations, mobile communications, computer information, and other digital traces and communications are used in conflict zones[12]. Given the aggressor state's actions in Ukraine − mass killings, rapes, looting − the problem of collecting evidence of war crimes is acute and requires greater use of AI technologies in detecting, documenting, and investigating war crimes, crimes against humanity, and genocide.

The investigation and documentation of war crimes in Ukraine is the most important line of work for criminal justice bodies. Decisive factors include professional, high-quality, complete, comprehensive, admissible, timely, and proper

[11] Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 – 2027 роки: Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

[12] Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності:* мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

documentation of all elements of a war crime. As of 20 January 2026, the Prosecutor General's Office has registered over 216,000 instances of crimes of aggression and war crimes committed during the full-scale invasion, with numerous cases of destruction of residential infrastructure, killings of civilians, looting, and violence documented[13]. The collected evidence will later make it possible not only to prove that these crimes were committed, but also to connect them to specific individuals, bring well-founded charges, and hold perpetrators accountable. Personal accounts of people who suffered violence and inhuman treatment, widely documented and disseminated, draw public attention to the intolerable armed conflict and enable the development of new recommendations and mechanisms for human rights protection.

OSINT plays a major role in documenting gross human rights violations and war crimes. Non-governmental organizations such as Bellingcat[14], Amnesty International, and Human Rights Watch have become pioneers in using open data to investigate events in conflict zones where access for official investigators is limited or impossible. By analyzing satellite imagery, social media videos, and public registers, these organizations have debunked official narratives and provided evidence for international courts.

A milestone that legitimized OSINT as an evidentiary tool was the judgment of the European Court of Human Rights in Ukraine and the Netherlands v. Russia (2022). In this decision, the Court for the first time recognized data obtained from open sources (in particular, Bellingcat's investigation of the downing of flight MH17) as full-fledged and reliable evidence.

The court formulated three key criteria for assessing such evidence:

– the authority and experience of the source (the research team must have recognized competence in the relevant1 field);

– transparency of the methodology (a clear description of how the information was collected, verified and stored);

– consistency with other evidence (coincidence of OSINT data with official investigation results, eyewitness accounts or other materials)[15].

National courts have repeatedly referred to OSINT materials as a means of obtaining information necessary for investigating criminal offenses.Thus, in the Ivano-Frankivsk City Court, OSINT was used to prove guilt in collaboration activities (case No. 344/19008/24). The court referred to the report of the operational officer, which indicated the analysis of information from open sources, in particular the social network «Vkontakte», to establish the fact of cooperation of a person with the occupation authorities. The verdict noted: "…during the implementation of counterintelligence activities, information was obtained regarding the unlawful actions of a citizen of Ukraine PERSON_7… acting to the detriment of sovereignty… went over to the enemy's side under martial law… according to the OSINT analysis of materials about the individual N 4/1-2350 dated 09/29/2022, she

[13] Злочини, вчинені в період повномасштабного вторгнення рф станом на 20.02.26. URL: https://www.gp.gov.ua/

[14] Bellingcat. URL: https://www.bellingcat.com/

[15] Радейко Р. І. Інструментарії OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400–410. DOI: https://doi.org/10.5281/zenodo.15648723

was a cadet of the Luhansk State University of Internal Affairs, worked as a police officer in the response sector of the patrol police at ADDRESS_2" (Verdict dated 05/12/2024 No. 344/19008/24 Ivano-Frankivsk City Court)[16].

2. In the Osnovyanskyi District Court of Kharkiv, the term OSINT was directly used to designate a method of identifying a person who transmitted the coordinates of the Armed Forces of Ukraine to the enemy (case No. 643/6925/24). The verdict states: "…who is registered to the number of the Ukrainian mobile operator NUMBER_Z and belongs to a citizen of Ukraine PERSON_5... whose identity was established using the capabilities of OSINT analytics" (Verdict of the Osnovyanskyi District Court of Kharkiv dated June 10, 2025 in case No. 643/6925/24)[17].

Analysis of these decisions shows that OSINT results are presented in criminal proceedings as OSINT-analysis memos, extracts from open-source intelligence, OSINT dossiers on individuals, and protocols of computer data inspection. In most decisions, references are made not to a document as the source of OSINT data, but to the results or sources gathered through OSINT[18]. This practice arises from the lack of a definition of OSINT as a tool for obtaining information on the circumstances of a criminal offense in current legislation, which, in our view, contradicts the principle of legal certainty in criminal procedure and in the activities of authorized bodies for detecting and investigating criminal offenses.

In today's realities of war and global threats, all practitioners in international criminal justice must improve their technical understanding of emerging artificial intelligence technologies and must cultivate a deeper contemporary understanding of the applications of how social media, geolocation, mobile phone conversations, computer information, and other digital traces and communications are used in war zones[19]. Given the military aggression on the territory of Ukraine and the commission of mass murders, rapes, and looting, the problem of collecting evidence of war crimes is acute today. This requires the activation and expansion of the use of artificial intelligence technologies in the detection, documentation, and investigation of war crimes, crimes against humanity, and genocide.

The use of OSINT technologies in the investigation of war crimes in Ukraine can be useful in many aspects. The main areas in which this technology can be used are as follows:

---

[16] Вирок Івано-Франківського міського суду Івано-Франківської області від 05 грудня 2024 року у справі № 344/19008/24. URL: https://reyestr.court.gov.ua/Review/123535737

[17] Вирок Основ'янського районного суду міста Харкова від 10 червня 2025 року у справі № 643/6925/24. URL: https://reyestr.court.gov.ua/Review/127999232.

[18] Кудінов С. С., Шехавцов Р. М. Правове регулювання використання osint та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126–133. URL: https://doi.org/10.32782/2311-8040/2025-3-14. http://journals.lvduvs.lviv.ua/index.php/law/article/view/1013

[19] Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності:* мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

Satellite imagery analysis. Artificial intelligence can help analyze large volumes of satellite imagery to identify changes in the landscape, including buildings, roads, and infrastructure, that may be linked to war crimes, as well as help identify locations where the bodies of war crimes victims may be buried[20];

Video and photo analysis. Artificial intelligence can be used to analyze large volumes of video and photo materials that were filmed at war crimes sites, which, in turn, can help identify suspects and witnesses, as well as determine whether they depict objects that may contain forensically significant information for investigating such crimes[21];

Audio processing. In telephone recordings and during the processing of audio materials for war crimes investigations, artificial intelligence can help identify voices contained in such media, as well as determine the places where these conversations took place;

Social media analysis[22]. By analyzing social media, AI can help uncover connections between suspects who may be involved in war crimes and identify individuals who may have witnessed or had information about war crimes[23];

analysis of data from medical institutions. Artificial intelligence can help in identifying the bodies of war crime victims, establishing the cause of death, identifying prisoners of war, war criminals and searching for them based on disease data and information about their identification features that help in identifying a specific person[24];

Facial recognition. Artificial intelligence can be used to recognize faces in photos and videos from war crimes scenes. This can help identify suspects involved in committing such crimes and identify witnesses who can provide important information about the war crime event under investigation;

Textual information analysis. Artificial intelligence analysis of textual information (e.g., social media posts and other sources) related to war crimes will

---

[20] Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

[21] Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, – LIGA.net URL: https://tech.liga.net/ua/ukraine/novosti/iskusstvennyy-intellekt-mintsifry-razoblachil-okkupanta-popavshego-v-gospitalv-krivom-roge

[22] Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

[23] Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С.142–146.

[24] Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL:. https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogiluukrayinskih-vijskovih-ta-ponad-460-novih-mogil-foto

help identify suspects and witnesses and uncover forensically significant information about war crimes under investigation[25].

Modern approaches to the investigation of war crimes make it possible to identify sources of digital information that determine the directions of collecting and studying digital traces to obtain information: from mobile devices, phones seized from participants in criminal proceedings; from personal computers of individuals and legal entities; from servers and other information storage devices in organizations and institutions; from radio frequency identifiers, GPS trackers, sensors, stationary and mobile measuring devices using geolocation, video surveillance and positioning systems; from network services that provide voice and video communication between computers via the Internet (ICQ, Skype, WhatsApp, Viber, Telegram, etc.); from banking systems on digital media (HDD, SSD, flash cards, etc.); from cellular operators regarding the detailing of subscriber communication and determining the location of the subscriber using geolocation; from recordings of video surveillance cameras of commercial and government structures; from the cameras and video cameras seized from the participants in the criminal proceedings.

By the same algorithm, OSINT debunks myths about the so-called «special operation» and «invincible» soldiers. Technologies recognize the faces of deceased occupiers and locate their social media profiles; autodialers inform relatives of their deaths. Ukraine's Ministry of Defense has also begun using Clearview AI facial recognition to identify Russian attackers, combat disinformation, and identify the dead and war criminals[26]. In the military realities of a full-scale war on the territory of Ukraine, digital forensics tools significantly assist in the detection, disclosure, and investigation of war crimes.

Geo-OSINT is a subtype of open-source intelligence that specializes in collecting, processing, analyzing, and interpreting geospatial data obtained from open sources. In contemporary forensics, security, intelligence work, and investigative journalism, Geo-OSINT is gaining strategic importance as a tool for obtaining evidence, verifying information, and building situational awareness. Unlike «classic» OSINT, which covers a wide spectrum of open information, Geo-OSINT focuses on data with a geographic reference.

Sources include:

– satellite imagery (Sentinel, Landsat, Maxar);
– digital maps (Google Maps, OpenStreetMap, Bing Maps);
– image/video geotags (EXIF);
– route data (GPS tracks, AIS, ADS-B);
– geolocated social media (Twitter, Instagram, TikTok);
– crowdsourcing platforms (Mapillary, Wikimapia);

[25] Шевчук В.М. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі*: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2024. 208 с. С. 89.

[26] Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі ? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

– open GIS databases [27].

Geo-OSINT consists in identifying spatial relationships among objects, events, and actions based on location, time of capture, and context. For example, combining a satellite image with a geotagged social media video allows one to confirm an event or track the movement of equipment, people, and weapons. Scientifically, Geo-OSINT combines elements of geoinformatics, forensics, digital forensics, information analytics, and law.

With Geo-OSINT, investigators can:

- track routes of suspects and vehicles;
- identify crime scenes;
- establish links among locations, events, and objects;
- reconstruct chronologies from geolocation data;
- monitor changes in terrain using satellite imagery over time[28].

In forensics, Geo-OSINT can:

- verify testimony (e.g., confirming a person's presence at a specific place);
- track criminal groups via their digital footprints in public space;
- create crime maps to analyze hot spots;
- model scenarios in space and time[29].

Geo-OSINT commonly uses:

- satellite visualization services (Sentinel Hub, Google Earth Pro, Zoom Earth);
- geoanalytical platforms (ArcGIS, QGIS, MapInfo);
- tools for extracting coordinates from images (ExifTool, FotoForensics);
- social media monitoring systems with geotag filtering (GeoSocial Footprint, Hootsuite, Maltego)[30].

Geo-OSINT has become popular among military analysts, investigators and detectives, and the State Border Guard Service, particularly in war-crimes investigations. For example, geolocation analysis of social media photos allowed Bellingcat investigators to confirm movements of military equipment during armed conflicts.

---

[27] Батанов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану : дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. С.7.

[28] Кисельов А. О. Тактика спілкування поліцейського з особами. The Top Actual Researches in Modern

Science: Proceedings of the IInd International Scientific and Practical Conference (Ajman, July 28- 29, 2016,

UAE). International Scientific and Practical Conference «World Science». 2016. № 8 (12). P. 23.

[29] Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики: матеріали Всеукр. наук.-практ. конф. : у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро: Дніпроп.держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

[30] Москаленко Я. , Кривошея Д. , Дейкун О, Кисельов А. Гео-OSINT в кримінальному аналізі. Collection of Scientific Papers «SCIENTIA», (May 30, 2025; Glasgow, Scotland, UK). С.89.

3. Ensuring Authenticity and Admissibility of Digital Open-Source Evidence in Criminal Justice

Proper handling of the evidentiary base − detection, collection, documentation, and investigation of war crimes − must be carried out with due regard to international experience and European standards of proof[31]. At the same time, one problem in using OSINT during pre-trial investigation is the risk of human-rights infringements (privacy and data protection). We should not overstate the potential and advantages of these technologies and must pay attention to their drawbacks. OSINT is acceptable in law enforcement and justice only if fundamental rights and rule-of-law principles are strictly respected − human dignity, equality before the law and the court, adversarial process, transparency, proportionality, fairness, and impartiality.

Using open sources in investigating war crimes is accompanied by complex ethical, legal, and procedural challenges that demand a particularly cautious approach. Unlike traditional methods, OSINT relies on data created, disseminated, or collected beyond state procedural control − by private individuals, journalists, volunteers, or even actors pursuing propaganda goals. This increases evidentiary potential but simultaneously creates risks of privacy breaches, exposure of witnesses, dissemination of traumatic content, and the spread of unverified or manipulative materials. For this reason, the Berkeley Protocol emphasizes the need to adhere to professional, methodological, and ethical principles when working with open sources, especially in the context of international crimes.

A single key postulate for the admissibility of open-source data is the protection of the accused's rights and a fair trial (para. 55 of the Berkeley Protocol)[32]. The Protocol is a practical guide developed by UC Berkeley School of Law together with the UN, setting international standards for online investigations into alleged violations of international human rights, humanitarian, and criminal law, and providing guidance on methodologies and procedures for the collection, analysis, and preservation of digital information in a professional, legal, and ethical manner. The Berkeley Protocol was developed with input from individuals with diverse professional perspectives, legal and cultural backgrounds, gender and nationality, and involved over 150 expert consultations and input from key stakeholders, including UN human rights investigators. Building on this collaborative approach, the Berkeley Protocol includes international standards for conducting online investigations into alleged violations of international human rights law, international humanitarian law and criminal law. It also provides guidance on methodologies and procedures for collecting, analyzing and preserving digital information in a professional, legal and ethical manner.

[31] Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. *Використання цифрових технологій у криміналістиці та судовій експертизі :* матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К . Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. С ташиса НАПрН України. Харків: Право, 2024. С. 133–136.

[32] Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

In this context, Articles 6(2) and 8 of the European Convention on Human Rights are fundamental[33]. Одним із ключових етичних вимірів є питання *приватності* та *пропорційності*. One key ethical dimension is privacy and proportionality. An OSINT researcher inevitably deals with data that may contain personal information: faces, voices, locations, household details, behaviors, and social ties. The use of such material must be necessary to achieve a specific procedural purpose, and the intrusion must be proportionate. If identifying a person is not critical, it is appropriate to limit oneself to group or role attribution; if content contains data that may endanger an individual, depersonalization, blurring, or partial redaction should be used. These approaches are reflected in the Berkeley Protocol, which underscores that safeguarding the digital, physical, and psychological security of all involved must prevail over research interests.

An equally important aspect is the *vulnerability of victims and witnesses*. Open-source materials often depict violence, the aftermath of attacks, and the dead or injured. Such content can retraumatize not only victims' relatives but also analysts who process large volumes of imagery. The Protocol therefore calls for ethical filters: limiting access to graphic material, providing psychological support, labeling content, and using procedures that minimize harm. Researchers should refrain from copying and storing unnecessary files lacking evidentiary value to reduce leakage and unauthorized access risks.

Legal aspects include ensuring *authenticity*, *integrity*, and *admissibility*. Evidence must have established provenance, be obtained by a proper subject or in a manner not contrary to law, and remain unchanged from discovery to presentation in court. Documenting the chain of custody − time of receipt, source, technical parameters, software versions, and any transformations − is crucial. The Berkeley Protocol provides a structure for such procedures, and technical transparency is a condition of judicial acceptability.

Authorial context and intent also matter. Social media materials may be created by civilians, military personnel, journalists, or hostile information structures. It is important to assess whether the author had access to the scene, whether third-party rights are violated, and whether the content is part of an influence operation. The fact that material was published by a private person does not preclude its procedural use − provided proper verification and compliance with international standards. However, courts often evaluate not only the content, but also the method of obtaining evidence – therefore, procedural discipline becomes no less important than the content of the material itself.

A separate legal challenge is the problem of *manipulation* and *disinformation.* The digital space is saturated with fakes, edited videos, fake metadata, and content taken out of context. That is why triangulation of independent sources, analysis of the history of content appearance, reverse image search, installation of early copies, and work with primary files are mandatory components of OSINT investigation. The Berkeley Protocol defines procedures for working with digital evidence from

[33] Convention for the Protection of Human Rights and Fundamental Freedoms : Council of Europe Convention of 04.11.1950 : as of 1 August 2021. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

open sources as basic methodological standards that ensure reproducibility and independent verification of the reliability of materials[34].

Ethical dilemmas also arise in public communication of results. OSINT investigations often unfold with interim results being actively disseminated in the media or on social networks. Premature disclosures can hinder official investigations, endanger witnesses, or jeopardize procedural steps. Researchers must balance the public interest in access to information with the interests of justice and adhere to a principle of minimum sufficiency − publishing only what will not harm the proceedings or persons involved. These requirements resonate with the ethical principles for the safe use of digital resources contained in the Berkeley Protocol.

Legal assessment of OSINT materials occurs within international humanitarian and criminal law. To qualify an event as a war crime, one must establish not only the fact of attack or destruction but also the status of the object (civilian or military), proportionality of force, mens rea or gross negligence, and causation. Digital evidence may be necessary but insufficient; it must be aligned with other evidence: witness testimony, expert examinations, crime scene inspections, and official sources. Properly collected and verified OSINT materials, however, can uniquely reconstruct events where direct access is limited or dangerous.

In conclusion, we would like to emphasize that the legal and ethical aspects of using OSINT are not limited to the technical quality of the files. They cover issues of privacy, security, reliability, legal status of the material, balance of intervention, responsibility for the consequences of publication, and methodological transparency. It is precisely adherence to these principles, formulated in the *Berkeley Protocol on Digital Open Source Investigations*, that allows turning digital open sources into a full-fledged evidentiary base in the investigation of war crimes and ensuring the compatibility of the results with international standards of justice.

CONCLUSIONS

Systematic integration of OSINT into war-crimes investigations has demonstrated the ability of open digital sources to ensure rapid event detection, construct spatio-temporal narratives, and produce persuasive analytical findings compatible with procedural standards. Practice has confirmed that it is the combination of various OSINT technologies that gives the highest evidentiary return: imagery, satellite images, geospatial layers, and the content of social networks mutually reinforce each other, making it possible to narrow the «time windows», increase the accuracy of geolocation, and identify the object by unique features.

Correct work with the evidence base, in particular, detection, collection, documentation, investigation of war criminal offenses, must be carried out taking into account international experience and European standards of evidence. Technologies for working with open data impose requirements for ethical prudence on law enforcement officers: protection of privacy, minimization of harm to victims and witnesses, careful work with traumatic content, responsible public

[34] Главюк І.В Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*, 2025. Вип. 91. Т. 4. С. 251-259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35

communication of intermediate results. Given the influence of digital data, it is the balance between probative value and people's safety that should determine the limits of information processing and disclosure.

The Berkeley Protocol emphasizes the need to observe professional, methodological and ethical principles when working with open sources, especially in the context of international crimes. The only key postulate for the admissibility of data from open sources in evidence is the protection of the rights of the accused and a fair trial (clause 55 of the Berkeley Protocol). One of the key ethical dimensions is the issue of privacy and proportionality. The provisions of the Berkeley Protocol emphasize that the protection of the digital, physical and psychological safety of all persons involved must take precedence over research interests.

A separate legal challenge is the problem of manipulation and disinformation. The Berkeley Protocol defines procedures for working with digital evidence from open sources as basic methodological standards that ensure reproducibility and independent verification of the reliability of materials. At the same time, the methodological requirement − triangulation (verification) of sources, work with primary copies, description of tools and software versions, conducting an «audit track» – is an indispensable condition for the admissibility and reliability of digital evidence.

From the standpoint of the strategic development of criminal justice, the priorities are the institutionalization of uniform national protocols for working with digital open sources, the development of an interdepartmental OSINT ecosystem, the training of investigators, prosecutors and judges to work with digital evidence, as well as the integration of tools and procedures compatible with international practice. In such a configuration, OSINT ceases to be an «auxiliary» tool and becomes a full-fledged technology for collecting digital evidence, capable of significantly increasing the effectiveness of the investigation of war crimes in the war and post-war periods and strengthening public confidence in justice.

SUMMARY

The article is devoted to the study of the possibilities of using OSINT technologies for the investigation of war crimes and crimes of aggression in the conditions of modern armed conflicts in the activities of law enforcement agencies of Ukraine. Emphasis is placed on innovative possibilities of technologies for working with open digital sources and methods of their practical use in procedural proof of violations of international humanitarian law. The theoretical and legal principles of OSINT application are revealed and algorithms for working with visual materials, satellite images, geospatial data, social networks and other public digital resources are given. Considerable attention is paid to the peculiarities of recording digital traces during investigative (search) actions, issues of authenticity and admissibility of digital evidence, documentation of the chain of preservation, use of professional approaches to geolocation and chronology of events, as well as methods of identification of involved persons and military equipment. Ethical and legal aspects of technologies for working with open data are separately covered. Emphasis is placed on protecting privacy, minimizing the risks of retraumatization, preventing manipulation, and ensuring compliance with international standards, including the Berkeley Protocol on Digital Open Source Investigations. First of all, such

technologies expand the possibilities of timely notification of offenses, search and identification of criminals. Based on the analysis of global trends in the digital transformation of the activities of criminal justice bodies, a systematic approach to the implementation of the use of OSINT technologies in this direction in the war and post-war periods is proposed. The work pays attention to the issue of consistency of the process with the trends of European integration. The author came to the conclusion that the complex use of digital technologies for working with open data in the investigation of war crimes contributes to increasing the efficiency of law enforcement activities and the judicial process, expands evidentiary possibilities and provides more complete documentation of the circumstances of criminal offenses.

Key words: OSINT, technologization, innovations, war crimes, criminal justice, digital evidence, open sources of information, Budapest Convention on Cybercrime, satellite images, geolocation, chronology, verification, chain of preservation, Berkeley Protocol, propaganda, procedural proof.

References

1. OSINT-розвідка у роботі журналістів. URL: https://youcontrol.com.ua/articles/osint-in-journalists-work/.

2. Трансформація завдань криміналістики в умовах воєнного стану та євроінтеграційних процесів : зб. матеріалів наук.-практ. конф. присвяч. пам'яті д-ра юрид. наук, проф. В.О. Коновалової,м. Харків, 28 берез. 2024 р. / [редкол.: А. П. Гетьман, В. М. Шевчук, Є. Є. Демидова] ; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків: Право, 2024. 148 с. URL: https://ivpz.kh.ua/wp-content/uploads/2024/09/Трансформація-завдань-криміналістики-28.06.2024.pdf

3. Методологічні засади криміналістики: традиції та новації : зб. матеріалів Криміналістичних читань, присвяч.пам'яті акад. В. О. Коновалової, м. Харків, 28 берез. 2025 р. Нац. юрид. ун-т ім. Ярослава Мудрого,Каф. криміналістики; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В.Сташиса Нац. акад. прав. наук України. Харків: Право, 2025. 276 с. URL: https://ivpz.kh.ua/wp-content/uploads/2025/04/Kryminalistychni_chytannia_Konovalova_28.03.2025.pdf.

4. Роль OSINT-досліджень у підвищенні рівня національної безпеки України : матеріали круглого столу (м. Львів, 7 травня 2025 р.) / укладач І. О. Ревак. Львів : ЛьвДУВС, 2025. 249 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8875/1/07_05_2025.pdf.

5. OSINT та електронні докази: юридичні вимоги та практика застосування у кримінальних провадженнях щодо воєнних злочинів в Україні. 14.01.2026. URL: https://www.coe.int/uk/web/kyiv/-/osint-and-electronic-evidence-legal-requirements-and-practical-application-in-criminal-proceedings-on-war-crimes-in-ukraine.

6. Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

7. Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США (2023). URL: https://khrife-journal.org/index.php/journal/article/download/564/633.

8. Використання OSINT у доказуванні командної відповідальності за міжнародні злочини: навчання НПУ. 08.10.2025. URL: https://npu.gov.ua/news/vykorystannia-osint-u-dokazuvanni-komandnoi-vidpovidalnosti-za-mizhnarodni-zlochyny-navchannia-npu.

9. Дуфенюк О. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374. DOI: 10.32782/2524–0374/2022–4/88.

10. Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України.* 2022. № 2. С. 87-90.

11. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733.

12. Президент України схвалив Комплексний стратегічний план реформування органів правопорядку (12.05.2023). URL: https://www.gp.gov.ua/ua/posts/prezident-ukrayini-sxvaliv-kompleksnii-strategicnii-plan-reformuvannya-organiv-pravoporyadku.

13. Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності:* мат-ли наук.-практ. онлайн-семінару (Харків, 05.11.2020). Харків, 2020. С. 6–10.

14. Злочини, вчинені в період повномасштабного вторгнення рф станом на 22.12.23. URL: https://www.gp.gov.ua.

15. Bellingcat. URL: https://www.bellingcat.com/

16. Радейко Р. І. Інструментарії OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400–410. DOI: https://doi.org/10.5281/zenodo.15648723.

17. Вирок Івано-Франківського міського суду Івано-Франківської області від 05 грудня 2024 року у справі № 344/19008/24. URL: https://reyestr.court.gov.ua/Review/123535737.

18. Вирок Основ'янського районного суду міста Харкова від 10 червня 2025 року у справі № 643/6925/24. URL: https://reyestr.court.gov.ua/Review/127999232.

19. Кудінов С. С., Шехавцов Р. М. Правове регулювання використання osint та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126–133. DOI: https://doi.org/10.32782/2311-8040/2025-3-14

20. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yakcifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

21. Штучний інтелект Мінцифри викрив окупанта, який потрапив у госпіталь в Кривому Розі – новини України, LIGA.net URL: https://tech.liga.net/ua/ukraine/ novosti/iskusstvennyy-intellekt-mintsifry-razoblachil-okkupanta-popavshego-v-gospitalv-krivom-roge.

22. Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Кримінальне та кримінальне процесуальне законодавство у контексті реформи кримінальної юстиції*: матеріали науково-практичного семінару (22 травня 2020 р.). Львів: ЛьвДУВС, 2020. С. 56–61.

23. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С. 142–146.

24. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. *Military offences and war crimes: background, theory and practice*: Scientific monograph. Riga, Latvia: «Baltija Publishing», 2023. С. 795-823. URL: http://www.baltijapublishing.lv/omp/ index.php/bp/catalog/download/322/8791/18392-1.

25. Під Ізюмом знайшли братську могилу українських військових та понад 460 нових поховань. URL:. https://hromadske.ua/posts/pid-izyumom-znajshli-bratsku-mogiluukrayinskih-vijskovih-ta-ponad-460-novih-mogil-foto.

26. *Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі*: монографія / В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін. ; за заг. ред. В. Ю. Шепітька ; Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2024. 208 с. С. 89.

27. Батанов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану: дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. 205 с.

28. Кисельов А. О. Тактика спілкування поліцейського з особами. The Top Actual Researches in Modern Science: Proceedings of the IInd International Scientific and Practical Conference (Ajman, July 28- 29, 2016, UAE). International Scientific and Practical Conference «World Science». 2016. № 8 (12). P. 25–28.

29. Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф.: у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро: Дніпроп.держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

30. Москаленко Я. , Кривошея Д. , Дейкун О, Кисельов А. Гео-OSINT в кримінальному аналізі. Collection of Scientific Papers «SCIENTIA», (May 30, 2025; Glasgow, Scotland, UK). С. 85–91.

31. Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. *Використання цифрових технологій у криміналістиці та судовій експертизі:* матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К . Авдєєва]; Нац. акад. прав. наук України ; НДІ вивч.

проблем злочинності ім. акад. В. В. С ташиса НАПрН України. Харків: Право, 2024. С.133–136.

22. Shevchuk, V., Morozova, T., Chornyi, H., Nehrebetskyi, V., and Slobodeniuk, I. Artificial Intelligence in Criminal Proceedings: Criminalistics, Criminal Procedure and Psychology Issues / V. Shevchuk та ін. *International Annals of Criminology*. 2025. С. 1–19. URL: https://doi.org/10.1017/cri.2025.10090.

23. Shevchuk, V., Dunaev, O., Tyshchenko, O., Biletska, G., and Nehrebetskyi, V. Innovative Methods in the Identification of Deceased Persons during Armed Conflicts and Disasters: Criminalistic and Forensic Medical Issues / V. Shevchuk et al. *International Annals of Criminology*. 2025. С. 1–20. URL: https://doi.org/10.1017/cri.2025.10094.

24. Гловюк І.В Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*, 2025. Вип. 91. Т. 4. С.251-259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35 URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/37-3.pdf

Information about the author:
Nehrebetskyi Vladyslav Valerevych,
Ph. D. in Law,
Associate Professor at the Department of Criminalistics
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., Kharkiv, 61024, Ukraine,
Researcher at Academician Stashis Scientific Research Institute
for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
49, Hryhoriia Skovorody str., Kharkiv, 61002, Ukraine