modern model of service that meets the requirements of wartime and Ukraine's international obligations.

References:

1. Медведєв В., Д. Горбенко. Сучасний стан і проблеми гендерної рівності в діяльності сектору безпеки України. *Юридична психологія*. 2020. С. 7-16. URL: https://psychped.navs.edu.ua/index.php/psychped/article/view/1358

2. Скиба Е.К., Комих Н.Г. Гендерна дискримінація: інструменти виявлення та протидії в секторі безпеки та оборони. Дніпро: ДДУВС, 2023. 34 с. URL: https://www.er.dduvs.edu.ua/bitstream/123456789/13111/1/pdf

3. Коба М. Гендерна інтеграція в секторі безпеки: український та міжнародний досвід. *Матеріали Міжнародної науково-практичної конференції.* Дніпро: ДДУВС. 2025. С. 101-103. URL: https://er.dduvs.edu.ua/bitstream/123456789/16236/5/101

4. Романова Н.В. Забезпечення гендерної рівності в секторі безпеки і оборони: імплементація міжнародно-правових стандартів у законодавство України. Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 – Право. Інститут держави і права імені В.М. Корецького Національної академії наук України, Київ, 2024. 235 с. URL: https://constitutionalist.com.ua/wp-content/uploads/2024/09/pdf

Третяк С.,
здобувач ступеня вищої освіти бакалавра
Донецького державного
університету внутрішніх справ
Консультант з мови: **Снісаренко І.**

DIGITAL INFORMATION AS A NEW TOOL OF EVIDENCE IN CRIMINAL PROCEEDINGS

Digital information is increasingly used in criminal investigations. This is due to scientific and technological progress and new ways of committing offenses. The widespread use of computers, software, smartphones and the Internet by criminals has raised a number

of questions regarding the admissibility and use of digital data as evidence. The scientific literature draws attention to the fact that "the use of digital sources of evidentiary information remains almost unregulated in national criminal procedural legislation, which complicates the effective use of modern technologies and sources of information." Despite legislative gaps, digital data is increasingly being used as evidence in criminal cases.

Investigation practice shows that electronic devices — phones, smartphones, computers, portable geolocation devices (GPS, GLONASS), digital photo and video cameras, webcams, network routers, payment systems, etc. — are increasingly used by criminals, as a result of which traces of their illegal actions are stored in the information space. These digital traces are detected during investigative (search) actions on specific information carriers. In our opinion, digital information can be used in an investigation in different ways. In particular, when investigating certain types of criminal offenses, the investigative situation can change under the influence of forensic tactics — through the adoption and implementation of various tactical decisions. Such measures help to obtain evidentiary information, in particular regarding: a) sources of its origin; b) overcoming resistance from interested parties; c) cases of its concealment; d) risks of further concealment; e) difficulties with recalling or interpreting information by individuals, etc.

It is digital data that often determines the direction of tactical decisions in these situations. Digital evidence requires the implementation of modern approaches to its collection, storage, use and research in the process of proving in criminal proceedings. When working with such evidence, it is important to adhere to a number of principles, in particular, ensuring proper professional training, attracting expert support and observing reasonable caution [1, p. 14-15].

The US Federal Code of Criminal Procedure provides for the possibility for a magistrate judge to accept complaints, issue warrants (resolutions) or execute subpoenas using reliable electronic means of communication (clause 4.1). In accordance with paragraph "a" of part 2 of rule 41, the procedure for conducting a search and seizure of property is determined, which means documents, books, business papers, any material objects and information.

Digital evidence is recognized as evidentiary information that is stored or transmitted in digital form and can be used by a party to the proceedings during the trial. Such information consists of two components:

1. content — that is, direct data (text documents, images, databases, etc.);

2. metadata — information about this data, containing information about the creation, modification or access to them. Metadata describes who, when and how a file or data set was created or modified, as well as under what conditions access took place.

Procedural aspects of working with electronic evidence in the United States are regulated by the Guidelines for the Search and Collection of Electronic Evidence. Before accepting electronic evidence in court, a party must prove its authenticity through a standard procedure for verifying an electronic document or by describing the process of its creation or the system by which the corresponding result was obtained. In this case, it is necessary to confirm that the system or process ensures the accuracy and reliability of the data.

The authenticity of computer records in US law is based on two principles:

• first, the absence of specific evidence of interference, even if there is a theoretical possibility of such interference, does not affect the reliability of the record;

• secondly, the rule of "best evidence" (Article 1002) applies, according to which there is no obligation to submit the original recording to the court.

The current direction of development of digital forensics in the USA is the study of electronic databases (Data Mining), which accumulate information about the activities of a person, including his possible criminal behavior. The essence of Data Mining in forensic activities is the systematic analysis of large amounts of information - collection, filtering, extraction and intellectual processing of data to identify forensically significant information. For example, through the use of geographic information systems, it is possible to establish the location of a person or other important circumstances.

In the UK, the key regulatory act regulating work with electronic evidence is the Computer Use for Unlawful Purposes Statute. It contains criminal law provisions on computer crimes, as well as

procedural provisions on conducting a search, seizing electronic evidence and determining the powers of law enforcement agencies.

In addition, the Association of Chiefs of Police of England, Wales and Northern Ireland has developed a Handbook on Working with Digital Evidence, which details the practical aspects of their detection, preservation and analysis [2, p. 223]. In conclusion, we note that the legislation of leading countries of the world is gradually becoming "technological" in nature: modern terms, technologies and approaches to the use of electronic evidence in criminal proceedings are being integrated into legal norms. In the USA, where the judicial procedure for forming evidence allows the parties to provide the court with information in any form, electronic evidence has a wider application. This is due to the fact that the concept of evidence in the US legal system is broader than in Ukraine, and does not require a mandatory indication of the specific source of its origin.

References:

1. Використання цифрової інформації в розслідуванні кримінальних правопо рушень: матеріали міжнар. наук.-практ. круглого столу. м. Харків, 12 груд. 2022 р. Харків: Право, 2022. 104 с. URL: https://ivpz.kh.ua/wp-content/uploads/2023/2022.pdf

2. Ахтирська Н.М. Міжнародний досвід використання цифров інформації у кримінальному судочинстві. *Юридичний науковий електронний журнал*. № 4. 2019. С. 221-224. URL: http://lsej.org.ua/4_2019/61.pdf

Тринога Т.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Романов І.**

EFFECTIVE DCIME REDUCTION STRATEGIES: INTERNATIONAL CASE STUDIES

Today, crime knows no borders, creating complex challenges for law enforcement agencies and politicians. Together with the development of crime, strategies to combat it must also develop. By