

determination of the range of possible sources of information about the crime; improvement of detection, fixation and removal of material traces of a crime during initial investigative (search) actions.

Keywords: *investigation method, forensic characteristics, criminal offenses against property, investigator, object of encroachment, methods of commission and setting of the crime, traces, identity of the criminal and the victim.*

UDC 343.985

DOI 10.31733/2078-3566-2023-5-205-212



Serhii ROZUMNY ©

Director

*(Dnipropetrovsk scientific research
Institute of Forensic Examinations
of the Ministry of Justice of Ukraine,
Dnipro, Ukraine)*

THE USE OF SPECIAL KNOWLEDGE IN THE INVESTIGATION OF CYBERCRIMES

Сергій Розумний. ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАТЬ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ. В статті на основі аналізу думок науковців та правоохоронної практики розглянуто поняття та ознаки спеціальних знань, під якими треба розуміти сукупність теоретичних знань і практичних умінь та навичок у галузі науки, техніки, мистецтва чи ремесла, набутих у результаті спеціальної теоретичної підготовки або професійного досвіду роботи, що використовуються при розслідуванні кримінальних правопорушень. Наголошується, що загальною метою використання спеціальних знань є вирішення завдань кримінального провадження, визначених ст. 2 Кримінального процесуального кодексу України, а саме забезпечення швидкого, повного та неупередженого розслідування. Використання спеціальних знань, сприяє формування доказової бази шляхом виявлення нової інформації, яку неможливо отримати використанням тільки юридичних знань.

Приділяється увага формам використання спеціальних знань. Зазначається, що вони є нічим іншим як способом реалізації теоретичних положень науки в практиці розслідування злочинів. Розглянуто окремі питання використання спеціальних знань у процесуальній та непроцесуальній формах при розслідуванні кіберзлочинів. Зосереджено увагу на процесуальних формах використання спеціальних знань, а саме залученні спеціаліста до проведення слідчих (розшукових) дій та призначення та проведення експертизи. Визначено спеціалістів, що приймають участь у розслідуванні визначеної категорії кримінальних проваджень, зазначено основні дії, що ними виконуються та зосереджено увагу на об'єктах, що вилучаються при огляді місця події. Розглянуто об'єкти та предмет експертиз: комп'ютерної техніки та програмних продуктів та експертизи електронних комунікацій, що частіше за все призначаються при розслідуванні кримінальних правопорушень, учинених в умовах воєнного часу та визначено об'єкти та предмет їх дослідження.

Ключові слова: *кримінальне провадження, розслідування, кіберзлочини, комп'ютерні технології, слідчі (розшукові) дії, огляд місця події, експертиза, спеціаліст, експерт.*

Relevance of the study. One of the main tasks of criminal proceedings is to ensure a quick, complete and impartial investigation (Art. 2 of the Criminal Procedure Code of Ukraine) [1]. In order to solve this task, the inquirer, investigator, and prosecutor, within the limits of their authority, carry out pre-trial investigation of criminal offenses, using all their professional knowledge, skills and abilities for this purpose. Despite the efforts of law enforcement agencies, crime is improving today: its organized forms are increasingly developing, new types of crimes are appearing, methods of their commission are being improved, the latest technical means of committing crimes are being used, etc. To counter modern criminal activity, it is not

enough for an investigator to have only professional legal knowledge. Taking into account the improvement of the technical equipment of crime, the involvement of modern computer technologies for the commission of crimes, the investigator, accordingly, needs to acquire new knowledge or use the knowledge of various types of specialists during the investigation.

Positive trends in the development of innovative technologies and computer equipment in modern society led to the emergence of a completely new negative phenomenon, namely the so-called computer or cybercrime. According to statistical data of the Office of the Prosecutor General of Ukraine, in 2022, 3,415 criminal offenses were registered in the field of use of electronic computing machines, systems and computer networks and telecommunication networks, of which a notice of suspicion was served in 2,643 cases [2]. Criminal offenses in the field of computer technologies are characterized by high latency due to the complexity of their detection and investigation. The virtual or digital traces inherent in these crimes can be destroyed in an instant, while it is usually very difficult to identify the computer that was used to gain unauthorized access to a particular network. That is why it is necessary to use not only professional legal, but also special knowledge to carry out a quick and complete investigation. Today, in the theory of criminology and the practice of investigating criminal offenses, there are certain difficulties in determining the types and forms of special knowledge in general, and, in particular, when investigating such a latent and complex category as crimes in the field of computer technologies. Therefore, the relevance of the issues investigated in this article is beyond doubt.

Recent publications review. Considerable attention was paid to the methodology of investigating certain types of criminal offenses and the use of special knowledge by such domestic scientists as V. Areshonkov, L. Arotsker, V. Bakhin, A. Vinberg, A. Volobuev, V. Goncharenko, I. Hora, H. Granovskyi, S. Yevdokimenko, A. Ishchenko, N. Klymenko, V. Konovalova, V. Kuzmichev, V. Lysychenko, V. Lukashevich, E. Lukyanchikov, I. Petrova, I. Pyrih, M. Saltevsykyi, M. Segai, E. Simakova-Efremyan, R. Stepaniuk, I. Fridman, K. Chaplinskyi, Y. Chornous, V. Shevchuk, V. Shepitko, M. Scherbakovskiy, and others.

Recently, there have been enough scientific works investigating the use of special knowledge in the investigation of certain types of crimes. Among them, the following can be noted: I. Pyrih "Theory and practice of the use of special knowledge in the investigation of theft of goods on railway transport" (2006), P. Kravchuk "The use of special knowledge during the investigation of robberies and robberies" (2015), M. Bidniak "Use of special knowledge in the investigation of fraud" (2018), N. Timofeeva "Use of special knowledge in the investigation of crimes against production safety", A. Taranova "Use of special knowledge in the investigation of improper performance of professional duties by a medical or pharmaceutical worker" (2020), S. Borysov "Use of special knowledge in the investigation of illegal handling of weapons, ammunition or explosives" (2020), A. Lisitskyi "Use of special knowledge in the investigation of criminal offenses committed by arson" (2023). However, in the works of scientists, not enough attention was paid to the use of special knowledge in the investigation of cybercrimes.

The research paper's objective. The purpose of the article is to determine the specifics of the use of special knowledge in the investigation of cybercrimes.

Discussion. Regarding the definition of the concept of "special" knowledge, we consider it inappropriate to dwell on it, since the above-mentioned scientists have sufficiently developed this issue. At the same time, it should be noted that certain concepts used in jurisprudence in general and in criminal proceedings in particular are not clear enough, which leads to significant shortcomings during the investigation and making of procedural decisions. Concepts formulated by scientists, subject to the laws of dialectics, are clarified, changed, and improved over time. Separate concepts formed in science become the basis of their legislative consolidation and further use in practice, which, in our opinion, is natural.

Despite the fact that the concept of special knowledge is sufficiently developed in science, it is not legally established. In normative documents regulating expert activities in Ukraine, such as the Law of Ukraine "On Forensic Expertise" [3], the Instruction on Appointment and Conduct of Forensic Expertises and Expert Research dated October 8, 1998 No. 53/5 [4] and other interpretations there is no such concept, which sometimes leads to errors when appointing an expert or involving specialists in the investigation. There is no concept of special knowledge in Art. 3 "Definition of the main terms of the Code" of the Criminal Procedure Code of Ukraine. In Art. 69 of this Code states that "an expert in criminal proceedings is a person who possesses scientific, technical or other special knowledge", and

Art. 71 defines a specialist as a person who "has special knowledge". At the same time, the meaning of the concept of "special knowledge" is not clarified. Therefore, when controversial issues arise regarding the use of special knowledge, investigators use scientific interpretation, which sometimes does not lead to positive results during proof.

One of the fundamental scientific works summarizing the problems of the use of special knowledge in criminal proceedings is a monograph reflecting the results of M. Scherbakovsky's doctoral dissertation "Conducting and using forensic examinations in criminal proceedings" [5]. The author, summarizing the achievements of scientists, defines the controversial issues that are the basis of the discussion of scientists regarding the definition of the essence of special knowledge and their characteristic features. Let's dwell separately on their characteristics.

The first criterion that characterizes special knowledge is its lack of general knowledge and lack of general availability. At the current stage of informatization of society, the presence of the worldwide Internet, where you can get any information, "public access" as a term loses its meaning. Indeed, today there cannot be such knowledge that cannot be obtained, that is, which is not freely available. But this only applies to knowledge. If we talk about skills and abilities that are part of the definition of special knowledge, then it is impossible to get them quickly. Investigating cybercrimes requires computer knowledge. Any educated person today has this knowledge as a user, but to deal with issues related to, for example, network intrusion and the nature of hacker activity, more in-depth knowledge is required. The limit of general availability of knowledge is a dynamic concept and changes over time.

As fields of special knowledge, most scientists define science, technology, art and craft, with which we agree. Any kind of special knowledge belongs to the fields of science, technology, art or craft. Individual scientists note such fields of knowledge as physics, chemistry, natural science, etc. as independent, but the named fields are covered by the concept of science.

The ratio of special and legal knowledge is the most controversial among scientists. We believe that for an investigator who investigates criminal offenses, knowledge in the fields of criminal law, criminal procedural law and criminology is professional. Knowledge from other branches of law: civil, agrarian, administrative, etc., are special for him, and the investigator can involve in the investigation a specialist in the field, for example, financial or economic law, as a specialist. We also join those scientists who consider knowledge in the field of forensic technology to be special, since it is, in fact, knowledge in the field of technology or natural science [6, pp. 155–158].

Analyzing the relationship of special knowledge with abilities and skills, M. Scherbakovskiy notes that these concepts are, although interrelated, but different, and including "special knowledge" in the definition of abilities and skills does not correspond to the provisions adopted in psychology and pedagogy [5, p. 60]. In our opinion, knowledge, ability and skills are three interdependent and mutually determined concepts that fully characterize the concept of "special knowledge".

When determining the goals of using special knowledge in criminal proceedings, we agree with the opinion of V. Kuzmichev and I. Pyrih that "the use of special knowledge in investigative and judicial practice is always purposeful. A clear definition of the purpose of their application at each stage of the criminal process is important for a correct understanding of the functions and powers of persons who use certain types of knowledge in procedural forms provided for by law" [7, pp. 11-12]. The general purpose of using special knowledge is to solve the tasks of criminal proceedings, defined in Art. 2 of the Criminal Procedure Code of Ukraine. Solving the goal presents the investigator with a large number of tasks, which we consider impractical to enumerate within the scope of this publication. The use of special knowledge, in our opinion, contributes to the formation of the evidence base by revealing new information that cannot be obtained using only legal knowledge.

Above, we drew attention to insufficiently clear regulation of the process of using special knowledge by procedural law. Considering the variety of types and forms of special knowledge, as well as their dynamism, in our opinion, it is legally impossible to list all types of special knowledge and fix all possible cases of their use. However, the basic concepts, principles of use, forms, subjects of use, their rights, obligations, etc. must be enshrined in the Criminal Procedure Code of Ukraine and other legal acts.

Having considered the criteria that separate "special" knowledge from others, we will give a definition of special knowledge, which we consider to be more justified: "special

knowledge is a set of theoretical knowledge and practical abilities and skills in the field of science, technology, art or craft, acquired as a result of a special theoretical training or professional work experience used for the purpose of detection, investigation and prevention of crimes" [7, p. 14].

Understanding the concept of special knowledge and its types is of great importance for the theory of criminology. But in the investigation of criminal offenses, the concept of forms of using special knowledge is more essential, in our opinion. Forms of using special knowledge are nothing more than a way of implementing the theoretical provisions of science in the practice of crime investigation. Despite the sufficiently developed forms of use of special knowledge among scientists, there are still discussions on this issue. Changes in legislation and the lack of a clear list of forms of using special knowledge also contribute to scientific controversy.

Most scientists distinguish procedural and non-procedural forms of using special knowledge. Procedural should be considered those that are directly provided by the legislation, namely: the participation of a specialist during investigative (search) actions and conducting forensic examinations with the relevant subjects: a specialist (Article 69 of the Criminal Procedure Code of Ukraine) and an expert (Article 71 of the Criminal of the Procedural Code of Ukraine) [5, p. 65; 8, p. 14; 9, p. 81]. The structure of special knowledge of an expert and a specialist, according to M. Scherbakovskiy, is distinguished by taking into account the peculiarities of their procedural functions and the goals of involvement in criminal proceedings [5, p. 65]. However, this is not entirely acceptable, since they can have the same knowledge, skills and abilities, but use them according to their competence.

Non-procedural special knowledge should be considered not outside the limits of the criminal process, but such that is not directly provided for by the legislation. Such forms are: departmental investigations, inspections of technical condition; carrying out research of objects directly at the scene of the event; consulting and reference assistance; provision of technical assistance in the preparation of technical means, performance of labor-intensive works; the use of the help of knowledgeable persons in the implementation of operative and search measures [8, p. 14].

As mentioned above, one of the dangerous crimes, the investigation of which requires the use of special knowledge, are the so-called cybercrimes. These crimes are increasingly becoming organized and group, and sometimes transnational in nature, as criminals use such means of crime as computer viruses, software bookmarks, remote access software attacks, etc., to gain unauthorized access to any computer system.

The concept of "cybercrime", although it exists in informal legal terminology, has long been used to characterize criminal offenses provided for in Chapter XVI of the Criminal Code of Ukraine "crimes in the field of use of electronic computing machines (computers), systems and computer networks and networks telecommunication". Although this term is given in the title "Cybercrime Convention", adopted by the Council of Europe [10] and ratified by the relevant law of Ukraine [11]. According to this document, cybercrimes are divided into four groups: crimes against privacy: illegal access, illegal interception, system interference, data interference, misuse of devices; crimes related to the use of a computer as a means of committing a crime: computer fraud and computer forgery; offenses related to content, in particular child pornography; offenses related to the violation of copyright and related rights. But, in our opinion, the classification dividing cybercrimes into aggressive and non-aggressive is more successful. The first group includes: cyber terrorism; a threat of physical violence transmitted by means of electronic communication; cyber stalking; illegal sexual harassment and stalking of another person via the Internet (cyberstalking), child pornography – creating pornographic materials with the image of children, distributing them, gaining access to such materials. The second group covers: cyber theft, cyber fraud, cyber vandalism, cyber espionage, distribution of virus programs and spam [12, pp. 284-285].

Let's consider the use of special knowledge in the investigation of cybercrimes in the form of involving a specialist in conducting investigative (search) actions. Virtually the only urgent investigative action, which is expedient to carry out at the initial stage of the investigation of cybercrimes, is a review [13, p. 10]. The specified investigative (search) action allows the investigator to directly perceive the situation of the scene of the incident and the objects located there in order to identify traces of the offense, clarify the circumstances of the incident that are important for criminal proceedings. This allows you to get an idea of the mechanism of the crime, put forward investigative versions, and determine the directions of the

investigation. The success of the entire investigation in many cases depends on the timeliness, urgency and quality of the inspection [14, pp. 213-214].

An expert in the field of computer technology is involved as a specialist when conducting an inspection of the scene. Already at the preparatory stage, he helps the investigator in the preparation of appropriate technical means: computer equipment that will be used for reading, copying and saving the extracted information; various connecting cables; special software that enables express analysis of information and its copying directly at the scene of the event, etc. During the work phase of the review, a specialist in the field of computer technology will explain what media may contain information of interest to the investigation: flash drives, laser CD, removable hard drives, etc., and what these media look like, as well as the rules for handling them etc. If the computer is connected to a local network, a specialist in the field of computer technology needs to establish the number of computers and servers connected to the server, their number in the network, the type of communication. If possible, organize a parallel review of computers connected to the local network. In the absence of such an opportunity, ensure that they are stopped and, in the future, conduct an inspection according to the diagram of a non-working computer [15, pp. 166-168].

We agree with the opinion of B. Teplytsky regarding the need to review mobile computer equipment with a telephone function. Considering the widespread use of mobile communication devices and the ability of mobile phones to collect, store and process information, the analysis of the information contained in them is important in the process of proof. In addition to making and receiving calls, a modern mobile phone combines many different functions, including: address and phone books; a diary with a list of meetings and affairs; notebook; messaging device; camera and video camera; dictaphone; multimedia player and others. All of the above data may contain indicative or evidentiary information displayed in digital traces, which can be analyzed in the presence of appropriate tools [16, p. 251]. Mobile phones can be inspected either directly at the scene or separately.

Specialists in the field of computer equipment and technologies are also involved in conducting a search and questioning of a suspect. During the search, his actions are similar to those performed when inspecting the scene. During the interrogation of the suspect, special knowledge is needed to explain to the investigator the meaning of certain terms related to the field of digital technologies or the content of the criminal actions described by the suspect.

In addition to specialists in the field of computer technology, forensic specialists are involved in the review. Their actions, depending on the stages of the review, are, in our opinion, traditional and sufficiently regulated by the Instruction on the Procedure for Engaging Employees of Pretrial Investigation Bodies of the Police and the Expert Service of the Ministry of Internal Affairs of Ukraine as specialists to participate in the inspection of the scene [17].

At the final stage of the examination with the participation of a specialist, it is necessary to determine which media can serve as sources of evidence, and which of them should be removed, taking into account the data on computer use. Such media can be: computer system units with hard drives installed on them (it is not recommended to remove them separately from the system unit); laptops; tablets; printers with memory cards; other computer components; portable media: flash cards, magnetic disks, memory cards, card readers, etc. The completeness of the evidence base depends on the number of information carriers that are removed and its quality, since the removed objects will be the objects of expert research in the future. Let's dwell on the types and subject of examination of examinations, which are assigned in the investigation of cybercrimes, as conducting examination is the second important form of using special knowledge.

The main expertise assigned during the investigation of this category of criminal proceedings is the expertise of computer equipment and software products. According to the Instructions on the Appointment and Conduct of Forensic Examinations, the main tasks of this examination include establishing: the working condition of computer and technical equipment; circumstances related to the use of computer and technical means; information and software contained on computer media; compliance of software products with certain versions or requirements for its development [4]. At the same time, the expert is provided with the computer medium itself for research, and if necessary, the computer unit; copies of the software product or software code, as well as all possible media specified by us above.

Taking into account the types of investigated objects of forensic examination of computer equipment and software products and the specifics of the tasks solved by it, B. Teplytskyi separates three subtypes of the specified examinations: computer equipment, which

establishes the circumstances and facts related to the functioning and operation of computer systems; software products, which establishes facts and circumstances related to methodological, hardware and structural features of software development and use; information and computer, establishing facts and circumstances related to information processing of the contents of file systems, their reproduction and storage on computer media [18, p. 31].

Electronic communications examination is an independent type of forensic examination, which is a type of engineering and technical examination, which is assigned during the investigation of cybercrimes. Electronic communications networks and their components, radio equipment, radio electronic devices, radiating devices and the information transmitted, received and processed by them are the objects of electronic communications expertise. The main tasks of electronic communications expertise are the research of electronic communications networks and their components, radio equipment, radio electronic means and radiating devices, namely: determination of their characteristics and parameters; establishment of facts and methods of transmission (reception) of information; establishment of facts and methods of access to them; determination of technical factors of the quality of the provision of electronic communication services at the level of their consumption; establishing their configuration and operating status; establishment of type, brand, model and other classification categories; research of information processing algorithms and its protection [4].

Conclusion. In conclusion, it can be noted that, based on the analysis of the opinions of scientists and law enforcement practice, we considered the concepts and signs of special knowledge, which should be understood as a set of theoretical knowledge and practical abilities and skills in the field of science, technology, art or craft, acquired as a result of special theoretical training or professional work experience used in the investigation of criminal offenses. Two forms of using special knowledge in the investigation of cybercrimes are considered: the involvement of a specialist in the conduct of investigative (search) actions, in particular, the inspection of the scene of the incident and the appointment of expertise, in particular, computer equipment and software products and electronic communications. The use of special knowledge during the investigation of cybercrimes contributes to obtaining objective and complete evidentiary information, expands the possibilities of the investigator in obtaining evidence.

Conflict of Interest and other Ethics Statements

The author declares no conflict of interest.

References

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України. 2013. № 9–10, № 11–12, № 13. Ст. 88. URL : <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.
2. Офіс Генерального прокурора України. URL : <https://www.gp.gov.ua/>.
3. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII. URL : <http://zakon4.rada.gov.ua/laws/show/4038-12>.
4. Про затвердження Інструкції про призначення та проведення судових експертиз : Наказ Міністерства юстиції України № 53/5 від 08.10.1998 р. URL : <http://zakon4.rada.gov.ua/laws/show/z0705-98>.
5. Щербаковський М. Г. Проведення та використання судових експертиз у кримінальному провадженні : монографія. Харків : В деле, 2015. 560 с.
6. Пиріг І. В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування: монограф. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2015. 454 с.
7. Кузьмічов В. С., Пиріг І. В. Використання спеціальних знань при розслідуванні розкрадань вантажів на залізничному транспорті : монограф. Д. : Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2008. 165 с.
8. Бідняк Г.С., Пиріг І. В. Використання спеціальних знань на досудовому розслідуванні: навч. посібник. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 134 с.
9. Салтевський М. В. Криміналістика (у сучасному викладі): Підручник. К.: Кондор, 2005. 588 с.
10. Конвенція про кіберзлочинність. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.
11. Про ратифікацію конвенції про кіберзлочинність. Закон України від 07.09.2005 р. № 2824-IV. URL : <https://zakon.rada.gov.ua/laws/show/2824-15#Text>.
12. Методика розслідування окремих видів злочинів: навч. посібник / О. І. Гарасимів, О. М.

Дуфенюк, О. В. Захарова та ін.; за заг. ред. Є. В. Пряхіна. 2-ге вид., перероб. та допов. Львів: ЛьвДУВС, 2019. 312 с.

13. Довженко О. Ю. Основи методики розслідування кіберзлочинів: автор. дис. на здобуття наук. ступеня канд. юрид. наук за спец. 12.00.09. Харківський національний університет внутрішніх справ. Харків. 2020. 20 с.

14. Криміналістика: підруч. для студ. вищ. навч. закл. / К. О. Чаплинський, О. В. Лускатов, І. В. Пиріг, В. М. Плетенець, Ю. А. Чаплинська. 2-е вид. перероб. і доп. Дніпро: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2017. 480 с.

15. Протидія злочинам у сфері використання інформаційних технологій: інтегрований навчально-практичний посібник. кол. авт.; за ред. д.ю.н., проф. М. В. Карчевського. Севеодонецьк: ПВВ ЛДУВС ім. Е. О. Дідоренка, 2019. 187 с.

16. Теплицький Б. Б. Особливості застосування техніко-криміналістичних засобів при проведенні окремих слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Юридична наука. Науковий юридичний журнал*. К.: Національна академія управління. 2020. № 6 (108). С. 248-255.

17. Інструкція про порядок залучення працівників органів досудового розслідування поліції та Експертної служби МВС України як спеціалістів для участі в проведенні огляду місця: Наказ МВС України від 03.11.2015 р. № 1339. URL: <https://zakon.rada.gov.ua/laws/show/z1392-15>.

18. Теплицький Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 3 (120). С. 28-34.

Submitted 16.10.2023

1. Kryminalnyy protsesualnyy kodeks Ukrayiny [Criminal Procedure Code of Ukraine]: Zakon Ukrayiny vid 13.04.2012 № 4651-VI. Vidomosti Verkhovnoyi Rady Ukrayiny. 2013. No. 9-10, No. 11-12, No. 13. Art. 88. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>. [in Ukr.].

2. Ofis Heneral'noho prokurora Ukrayiny. URL: <https://www.gp.gov.ua/>. [in Ukr.].

3. Pro sudovu ekspertyzu [On forensic examination]: Zakon Ukrayiny vid 25.02.1994 r. № 4038-XI. URL: <http://zakon4.rada.gov.ua/laws/show/4038-12>. [in Ukr.].

4. Pro zatverdzhennya Instruksiyi pro przyznachennya ta provedennya sudovykh ekspertyz [On the approval of the Instructions on the appointment and conduct of forensic examinations]: Nakaz Ministerstva yustytysiyi Ukrayiny No. 53/5 vid 08.10.1998 r. [in Ukr.].

5. Shcherbakovs'kyi, M. (2015). Provedennya ta vykorystannya sudovykh ekspertyz u kryminal'nomu provadzhenni [Conducting and using forensic examinations in criminal proceedings]: monohrafiya. Kharkiv: V dele. 560 p. [in Ukr.].

6. Pyrih, I. (2015). Teoretyko-prykladni problemy ekspertnoho zabezpechennya dosudovoho rozsliduvannya [Theoretical and applied problems of expert support for pre-trial investigation]: monohraf. Dnipropetrovs'k: Dniprop. derzh. un-t vnutr. sprav; Lira LTD. 454 p. [in Ukr.].

7. Kuz'michov, V. & Pyrih, I. (2008). Vykorystannya spetsial'nykh znan' pry rozsliduvanni rozkradan' vantazhiv na zaliznychnomu transporti [Use of special knowledge in the investigation of theft of goods on railway transport]: monohraf. D. : Dniprop. derzh. un-t vnutr. sprav; Lira LTD. 165 p. [in Ukr.].

8. Bidnyak, H. & Pyrih, I. (2018). Vykorystannya spetsial'nykh znan' na dosudovomu rozsliduvanni [Use of special knowledge in pre-trial investigation]: navch. posibnyk. Dnipro: Dniprop. derzh. un-t vnutr. sprav. 134 p. [in Ukr.].

9. Saltevs'kyi, M. (2005). Kryminalistyka (u suchasnomu vykladni) [Criminalistics (in modern terms)]: Pidruchnyk. K.: Kondor, 588 p. [in Ukr.].

10. Konventsiya pro kiberzlochynnist' [Convention on cybercrime]. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. [in Ukr.].

11. Pro ratyfikatsiyu konventsiyi pro kiberzlochynnist' [On the ratification of the convention on cybercrime]. Zakon Ukrayiny vid 07.09.2005 r. No. 2824-IV. URL: <https://zakon.rada.gov.ua/laws/show/2824-15#Text>. [in Ukr.].

12. Metodyka rozsliduvannya okremykh vydiv zlochyniv. (2019). [Methods of investigation of certain types of crimes]: navch. posibnyk / O. I. Harasymiv, O. M. Dufenyuk, O. V. Zakharova ta in.; za zah. red. YE. V. Pryakhina. 2-he vyd., pererob. ta dopov. L'viv: L'vDUVS. 312 p. [in Ukr.].

13. Dovzhenko, O. (2020). Osnovy metodyky rozsliduvannya kiberzlochyniv [Fundamentals of cybercrime investigation methodology]: avtor. dys. na zdobuttya nauk. stupenya kand. yuryd. nauk za spets. 12.00.09. Kharkivs'kyi natsional'nyy universytet vnutrishnikh sprav. Kharkiv. 20 p. [in Ukr.].

14. Kryminalistyka [Criminalistics]: pidruch. dlya stud. vyshch. navch. zakl. / K. O. Chaplyns'kyi, O. V. Luskatov, I. V. Pyrih, V. M. Pletenets', Yu. A. Chaplyns'ka. 2-e vyd. pererob. i dop. Dnipro: Dniprop. derzh. un-t vnutr. sprav; Lira LTD, 2017. 480 p. [in Ukr.].

15. Protydiya zlochynam u sferi vykorystannya informatsiynykh tekhnolohiy [Combating crimes

in the field of information technology use]; intehrovanyy navchal'no-praktychnyy posibnyk. kol. avt. ; za red. d.yu.n., prof. M. V. Karchevs'koho. Syevyerodnets'k : RVV LDUVS im. E. O. Didorenka, 2019. 187 p. [in Ukr.].

16. Teplyts'kyy, B. (2020). Osoblyvosti zastosuvannya tekhniko-kryminalistychnykh zasobiv pry provedenni okremykh slidchykh (rozshukovykh) diy pid chas rozsliduvannya zlochyniv u sferi vykorystannya elektronno-obchyslyval'nykh mashyn (komp'yuteriv), system ta komp'yuternykh merezh i merezh elektrozv'yazku [Peculiarities of the use of technical and forensic means when conducting separate investigative (search) actions during the investigation of crimes in the field of the use of electronic computing machines (computers), systems and computer networks and telecommunication networks]. *Yurydychna nauka. Naukovyy yurydychnyy zhurnal*. K.: Natsional'na akademiya upravlinnya. 6 (108). Pp. 248-255 [in Ukr.].

17. Instruktsiya pro porjadok zaluchennya pratsivnykiv orhaniv dosudovoho rozsliduvannya politsiyi ta Ekspertnoyi sluzhby MVS Ukrayiny yak spetsialistiv dlya uchasti v provedenni ohlyadu mistysya [Instructions on the procedure for involving employees of pretrial investigation bodies of the police and the Expert Service of the Ministry of Internal Affairs of Ukraine as specialists to participate in the inspection of the site]; Nakaz MVS Ukrayiny vid 03.11.2015 r. No. 1339. URL : <https://zakon.rada.gov.ua/laws/show/z1392-15>. [in Ukr.].

18. Teplyts'kyy, B. (2021). Aktual'ni pytannya pryznachennya ekspertyzy komp'yuternoyi tekhniky i prohramnykh produktiv pid chas rozsliduvannya zlochyniv u sferi vykorystannya elektronno-obchyslyval'nykh mashyn (komp'yuteriv), system, komp'yuternykh merezh i merezh elektrozv'yazku [Current issues of appointment of examination of computer equipment and software products during the investigation of crimes in the field of use of electronic computing machines (computers), systems, computer networks and telecommunication networks]. *Naukovyy visnyk Natsional'noyi akademiyi vnutrishnikh sprav*. 3 (120). Pp. 28-34 [in Ukr.].

ABSTRACT

The article, based on the analysis of the opinions of scientists and law enforcement practice, considers the concepts and signs of special knowledge, which should be understood as a set of theoretical knowledge and practical abilities and skills in the field of science, technology, art or craft, acquired as a result of special theoretical training or professional work experience. used in the investigation of criminal offenses. It is emphasized that the general purpose of using special knowledge is to solve the tasks of criminal proceedings, defined in Art. 2 of the Criminal Procedure Code of Ukraine, namely the provision of a quick, complete and impartial investigation. The use of special knowledge contributes to the formation of an evidence base by revealing new information that cannot be obtained using only legal knowledge.

Attention is paid to the forms of using special knowledge. It is noted that they are nothing more than a way of implementing the theoretical provisions of science in the practice of investigating crimes. Separate issues of the use of special knowledge in procedural and non-procedural forms in the investigation of cybercrimes are considered. Attention is focused on the procedural forms of using special knowledge, namely, the involvement of a specialist in the conduct of investigative (search) actions and the appointment and conduct of an examination. Specialists participating in the investigation of a certain category of criminal proceedings are identified, the main actions performed by them are indicated, and attention is focused on the objects seized during the inspection of the scene. The objects and subject of examinations: computer equipment and software products and examination of electronic communications, which are most often assigned during the investigation of criminal offenses committed in wartime conditions, were considered, and the objects and subject of their research were determined.

Keywords: *criminal proceedings, investigation, cybercrimes, computer technologies, investigative (search) actions, inspection of the scene of the incident, expertise, specialist, expert.*