МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

ТЕПЛИЦЬКИЙ БРОНІСЛАВ БРОНІСЛАВОВИЧ

УДК 343.983:[343.34:004]

ДИСЕРТАЦІЯ

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

12.00.09 «Кримінальний процес та криміналістика;
судова експертиза; оперативно-розшукова діяльність»
(081 – Право)

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **Б. Б. Теплицький**

Науковий керівник: **Арешонков Віталій Володимирович,** доктор юридичних наук, старший науковий співробітник

Київ – 2021

АНОТАЦІЯ

Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» (081 – Право). – Національна академія внутрішніх справ, Київ, 2021.

У дисертації розроблено теоретичні положення та науково обґрунтовані рекомендації щодо техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Встановлено, що у сучасних умовах питання розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, детально розроблені у кримінально-правовій, кримінальній процесуальній та адміністративно-правовій науці. У криміналістиці більшість наукових праць присвячена загальному дослідженню використанню спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій, особливостям встановлення обставин, які підлягають доказуванню у справах про комп'ютерні злочини. Окремого комплексного дослідження техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку не проводилось.

Обґрунтовано, що зміст техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку складають

мета, на досягнення якої спрямовується така діяльність, а також завдання як окремі напрями досягнення мети, які полягають у: виявленні, зборі, фіксації доказової інформації; подальшому аналізі такої інформації; залученні до слідчих (розшукових), негласних слідчих (розшукових) дій та оперативно-розшукових заходів компетентних у відповідній галузі осіб (які володіють спеціальними знаннями); техніко-криміналістичному супроводі, який здійснюється в організаційних і процесуальних формах використання спеціальних знань у процесі оперативно-розшукової та слідчої роботи; оснащенні уповноважених на здійснення техніко-криміналістичного забезпечення суб'єктів сучасними технічними засобами; формуванні у таких суб'єктів умінь і навичок практичного застосування криміналістичної техніки тощо.

Важлива роль у техніко-криміналістичному забезпеченні розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку належить уповноваженим на таку діяльність суб'єктам. Під цими суб'єктами розуміються особи, які реалізують свої повноваження на підставі чинного законодавства, використовуючи техніко-криміналістичні засоби задля здійснення ефективного розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Суб'єктів техніко-криміналістичному забезпеченні розслідування кіберзлочинів класифіковано на індивідуальних (слідчі; слідчі-криміналісти; спеціалісти; працівники кіберполіції, оперативних та оперативно-технічних підрозділів; експерти) та колективних (слідчо-оперативна група; слідча група; судово-експертні установи; група експертів).

На підставі проаналізованого зарубіжного досвіду технічного забезпечення протидії кіберзлочинам сформовані пропозиції щодо розвитку правового регулювання вітчизняного науково-технічного забезпечення кібербезпеки; рекомендації із розроблення організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки; шляхів залучення вітчизняних

фахівців до вирішення завдань техніко-криміналістичного забезпечення кібербезпеки (досвід Німеччини); налагодження взаємодії між підрозділами Національної поліції, Експертної служби МВС з кібервійськами системи Міністерства оборони України в аспекті забезпечення технічними ресурсами (досвід Франції); забезпечення підвищення матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів; пріоритетних напрямів залучення міжнародної технічної допомоги щодо відповідного забезпечення кібербезпеки України тощо.

З'ясовано, що техніко-криміналістичні засоби розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – це система спеціально виготовлених або пристосованих приладів, пристроїв, інструментів, матеріалів, інформаційних пошукових, ідентифікаційних та інших систем, а також криміналістичних технологій їх застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів, а також здійснення інших дій з виявлення, розслідування та попередження злочинів. Видами цих техніко-криміналістичних засобів є: апаратні і програмні засоби мобільної криміналістики; апаратні блокиратори запису; програмні засоби комп'ютерної експертизи; апаратні засоби відновлення даних; відкрите спеціалізоване програмне забезпечення; дистрибутиви на основі Linux.

Досліджено техніко-криміналістичне забезпечення проведення огляду, обшуку, допиту під час розслідування кіберзлочинів, викоремлено його особливості. Встановлено, що огляд під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку має на меті об'єктивне закріплення обстановки та слідів злочину, що забезпечує збирання доказів й унеможливлює знищення комп'ютерної інформації. До особливостей огляду, що впливають на застосування техніко-криміналістичних засобів, належать: місце його проведення

(місце безпосереднього вчинення злочину; місця розміщення локальної мережі ЕОМ; місце настання шкідливих наслідків); обов'язкова участь спеціаліста у сфері комп'ютерної техніки та програмного забезпечення; необхідність технічного супроводження виконаних слідчим дій із збирання слідової інформації в цифровому (електронному) середовищі; спеціалізоване програмне забезпечення для виявлення, фіксації і копіювання комп'ютерних даних.

Доведено, що успішних результатів обшуку в процесі розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку досягають завдяки використанню чинника раптовості, залучення спеціалістів у галузі комп'ютерних технологій та програмування, тактичних прийомів обшуку. «Груповий обшук» одночасно проводять у співучасників злочинного ланцюжка у всіх приміщеннях, де встановлені ЕОМ, які об'єднані в локальну мережу. Правильний вибір моменту таких обшуків запобігає витоку інформації про викриття злочинців, знищенню комп'ютерних даних. За одночасного проведення обшуків у різних місцях заздалегідь готують відповідні техніко-криміналістичні засоби, формують слідчі групи, забезпечують участь необхідних спеціалістів.

Звернуто увагу, що проведення допиту оптимізує типовий перелік питань, що підлягають з'ясуванню у підозрюваного та свідків. Окремо подані питання для допиту операторів ЕОМ, програмістів, відповідальних осіб за інформаційну безпеку, адміністраторів комп'ютерної мережі, співробітників, які здійснюють технічне обслуговування обчислювальної техніки.

Встановлено, що типовими негласними слідчими (розшуковими) діями проведеними із застосуванням техніко-криміналістичних засобів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є: зняття інформації з транспортних телекомунікаційних мереж; спостереження за особою, річчю або місцем; обстеження публічно недоступних місць, житла чи іншого володіння особи; установлення місцезнаходження радіоелектронного засобу;

аудіо-, відеоконтроль особи; зняття інформації з електронних інформаційних систем; контроль за вчиненням злочину.

Досліджено судові експертизи, які проводяться під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, та запропоновано типові види цих експертиз: комп'ютерної техніки і програмних продуктів; телекомунікаційних систем і засобів; традиційні криміналістичні (трасологічна, дактилоскопічна, технічна експертиза документів, тощо), судово-економічні, а також комплексні та комісійні експертизи. Досліджені комплексні експертизи проводилися для вирішення завдань, що відносяться до господарчої, фінансової діяльності (комп'ютерно-технічна та судово-бухгалтерська експертиза); вивчення споживчих властивостей, умов зберігання, вартості комп'ютерних засобів, програмного забезпечення (комп'ютерно-технічна та судово-товарознавча експертиза); для встановлення джерела походження програмних продуктів, відео-, аудіопродукції (комп'ютерно-технічна та експертиза об'єктів інтелектуальної власності).

З'ясовано, що сучасний рівень розвитку техніко-криміналістичного забезпечення судово-експертної діяльності дозволяє вирішувати завдання із встановлення способу та механізму злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; встановлення фактів та способів передачі (отримання) інформації в мережі; встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій тощо.

Експертиза комп'ютерної техніки та програмних продуктів проводиться відносно трьох груп об'єктів: апаратних, програмних та інформаційних. Підвидами цієї експертизи є: дослідження комп'ютерної техніки; дослідження програмних продуктів; інформаційно-комп'ютерні дослідження. Виявлені типові слідчі помилки при призначенні експертизи комп'ютерної техніки та програмних продуктів ускладнюють або унеможливлюють її проведення, що позбавляє

слідчого значимих доказів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Оцінюючи висновок експерта у кримінальному провадженні про злочин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, слідчий, прокурор, слідчий суддя, суд звертають увагу на те, чи є він належний, допустимий і достовірний, а також чи експертиза відповідає засадам законності, незалежності судового експерта, всебічності, об'єктивності та повноти дослідження, використання сучасних досягнень науки і техніки, максимального збереження об'єктів дослідження.

Обґрунтовано, що використання висновку експерта під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є оперування ним уповноваженими особами під час кваліфікації кримінального правопорушення, для встановлення фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню, а також для вирішення інших тактичних завдань. Окреслено можливості використання висновків експертиз у відповідній категорії кримінальних проваджень: для забезпечення потреб розслідування: з'ясування фактів (обставин) кримінального правопорушення; збирання та перевірки доказів; обґрунтування процесуальних дій, рішень; забезпечення дотримання змагальності судочинства; кримінально-правової кваліфікації злочину; для забезпечення криміналістичних потреб: висунення версій та їх перевірки; моделювання обставин події; для забезпечення експертної профілактики кіберзлочинності; уникнення експертних помилок.

Ключові слова: кіберзлочинність, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, техніко-криміналістичне забезпечення, техніко-криміналістичні засоби, експертиза комп'ютерної техніки і програмних продуктів, експертиза телекомунікаційних систем і засобів.

SUMMARY

Teplytsky B.B. Technical and forensic support for the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage. – Qualifying scientific work on the rights of the manuscript.

The dissertation on competition of a scientific degree of The Candidate of Legal Sciences on a specialty 12.00.09 "Criminal process and criminology; forensic examination; operational and investigative activities" (081 – Law). – National Academy of Internal Affairs, Kyiv, 2021.

The dissertation develops theoretical provisions and scientifically substantiated recommendations for technical and forensic support for the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage.

It is known that the issues of investigation of crimes in the field of use of electronic computer systems, computer and telecommunication networks in modern conditions, are carefully developed in criminal law, criminal procedure and administrative law. Considering criminology, most research is devoted to the general study of the use of specialized knowledge in the investigation of crimes committed with the use of computer technology, the peculiarities of establishing the circumstances to be proved in cases of cybercrimes. There is no separate study of forensic support in the sphere of electronic computer systems, computer and telecommunications networks usage

It is substantiated that the main goals of technical and forensic support for the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage, to which such activities are directed, as well as tasks for separate areas are: detection, collection and recording of evidence; further analysis of such information; involvement of persons competent in the relevant field (who have special knowledge) to investigative (search) or covert investigative (search) actions and operational-investigative measures; technical and forensic support, which is carried out in organizational and procedural forms with the use of special knowledge in

the process of operational and investigative work; equipping the authorized persons for the implementation of technical and forensic subjects with modern technical tools; formation of skills and abilities for practical application of forensic techniques in such subjects, etc.

An important role in the technical and forensic support of the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage belongs to the entities authorized for such activities. These entities are persons who exercise their powers on the basis of current legislation, using forensic tools to effectively investigate crimes involving the use of computer systems and telecommunication networks. Subjects of technical-forensic support of cybercrime investigation are classified into individual (investigators; forensic investigators; specialists; cyberpolice officers, operational and operational-technical units; experts) and collective (investigative-operational group; investigative group; forensic institutions; expert group).

On the basis of the analyzed foreign experience of technical support for counteraction to cybercrimes proposals on development of legal regulation of domestic scientific and technical maintenance of cybersecurity are formed; recommendations for the development of organizational and technical model of cybersecurity, which will respond to current threats, challenges in cyberspace and global trends in the cybersecurity industry are made; ways to involve domestic experts in solving problems of technical and forensic cybersecurity (German experience) are presented; cooperation between units of the National Police, the Expert Service of the Ministry of Internal Affairs and cyber troops of the system of the Ministry of Defense of Ukraine in terms of providing technical resources (French experience) are established increase of material and technical support of forensic experts in the areas of research of computer hardware and software products, communication systems and tools are ensured; priority areas for attracting international technical assistance for appropriate cyber security of Ukraine are given.

It was found that forensic tools for the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage – is a

system of specially made or adapted devices, instruments, apparatuses, tools, materials, information retrieval, identification and other systems, as well as forensic technologies of their application for the purpose of detection, fixing, extraction, research, accounting, analysis and evaluation of electronic/virtual traces of crime and other material evidence, as well as other actions to detect, investigate and prevent such crimes. Types of these forensic tools are: hardware and software for mobile forensics; hardware recording blockers; computer examination software; data recovery hardware; open specialized software; Linux-based distributions.

The technical and forensic support for the inspection, search, interrogation during the investigation of cybercrime has been studied, its peculiarities have been eradicated.

It is established that the review during the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage aims to objectively consolidate the situation and traces of the crime, which ensures the collection of evidence and prevents destruction of computer information. The features of the review that affect the use of forensic tools include: place of its conduct (place of direct commission of the crime; location of the local computer network; place of occurrence of harmful consequences); mandatory participation of a specialist in the field of computer hardware and software; the need for technical support of the investigator's actions to collect trace information in a digital (electronic) environment; specialized software for detection, capturing and copying computer data.

It is proved that successful results of the search in the process of investigating crimes in the sphere of electronic computer systems, computer and telecommunications networks usage are achieved through the use of the factor of suddenness, involvement of specialists in the field of computer technology and programming, search tactics. "Group search" is carried out simultaneously with the accomplices of the criminal chain in all rooms where computers are installed, which are connected to the local network. Choosing the right time for such searches prevents the leakage of information about the detection of criminals, the destruction of computer data. At the same time conduction of searches in different places must to be prepared in advance with the relevant technical

and forensic tools, formation of investigative teams, ensuring the participation of the necessary specialists.

It is noted that the interrogation optimizes the typical list of issues to be clarified with the suspect and witnesses. Separate questions must be asked during the interrogation of computer operators, programmers, information security officers, computer network administrators, and computer maintenance personnel.

It is known that typical covert investigative (search) actions carried out with the use of technical and forensic tools during the investigation of crimes in the field of electronic computer systems, computer and telecommunications networks usage are: withdrawal of information from transport telecommunication networks; observation of a person, thing or place; inspection of publicly inaccessible places, housing or other property of a person; locating an electronic device; audio, video control of the person; removal of information from electronic information systems; control over the commission of a crime.

Forensic examinations conducted during the investigation of crimes in the field of electronic computer systems, computer and telecommunications networks usage are studied, and typical types of these examinations are proposed. Main types of expertise are connected with: computer hardware and software products; telecommunication systems and tools; traditional forensic (trasological, dactyloscopic, technical examination of documents, etc.), forensic-economic, as well as complex and commission examinations. The studied complex examinations were conducted: to solve problems related to economic, financial activities (computer and technical and forensic accounting); to study consumer properties, storage conditions, cost of computer tools, software (computer-technical and forensic examination); to establish the source of software products, video, audio products (computer and technical and examination of intellectual property).

It was found that the current level of development of technical and forensic support for forensic science allows: to solve the problem of establishing the method and mechanism of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage; detection of information and software contained

on computer media; to establish facts and methods of transmission (receipt) of information in the network; to formalize facts and methods of access to systems, resources and information in the field of telecommunications, etc.

Examination of computer hardware and software products is carried out in relation to three groups of objects: hardware, software and information. Subtypes of this examination are: research of computer technology; research of software products; information and computer research. Typical investigative errors in the appointment of computer hardware and software examination (make it difficult or impossible to conduct it) have been identified. Such errors deprive the investigator of significant evidence during the investigation of crimes in the field of electronic computer systems, computer and telecommunications networks usage.

Assessing the opinion of an expert in criminal proceedings on a crime in the sphere of electronic computer systems, computer and telecommunications networks usage, the investigator, the prosecutor, the investigating judge, the court shall pay attention to whether it is appropriate, admissible and reliable, and whether the examination meets the principles of legality, independence of the forensic expert, comprehensiveness, objectivity and completeness of the study, the use of modern science and technology, the maximum preservation of research objects.

It is substantiated that the use of expert opinion in the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage is always an operation of authorized persons during the qualification of a criminal offense, made to establish the facts and circumstances, relevant to criminal proceedings and subject to proof, as well as to solve other tactical tasks. Possibilities of using the conclusions of examinations in the corresponding category of criminal proceedings are outlined: to meet the needs of the investigation: clarification of the facts (circumstances) of the criminal offense; collection and verification of evidence; substantiation of procedural actions, decisions; ensuring compliance with the adversarial proceedings; criminal and legal qualification of the crime; to meet forensic needs: versioning and testing; simulation of the circumstances of the event; to ensure expert prevention of cybercrime; avoid expert mistakes.

Key words: cybercrime, crimes in the field of electronic computer systems, computer and telecommunications networks usage, forensic software, forensic tools, examination of computer equipment and software, examination of telecommunication systems and means.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковано основні наукові результати дисертації:

1. Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. *Науковий вісник Національної академії внутрішніх справ.* 2018. № 3 (108). С. 303–315.

2. Теплицкий Б. Використання зарубіжного досвіду техніко-криміналістичного забезпечення розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *KELM*. 2020. № 3-3. С. 112–116. (Республіка Польща).

3. Теплицький Б. Б. Застосування техніко-криміналістичних засобів при проведенні обшуку під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *Юридична наука*. 2020. № 5. С. 143–148.

4. 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*. 2020. № 6. С. 177–183.

5. Теплицький Б. Б. Сучасні можливості судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Юридичний часопис Національної академії внутрішніх справ.* 2021. № 1 (21). С. 30–37.

6. 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.

які засвідчують апробацію матеріалів дисертації:

7. Теплицький Б. Б. Практичні проблемні питання призначення комп'ютерно-технічної судової експертизи в кримінальних провадженнях. *Актуальні проблеми криміналістики та судової експертології*: матеріали міжвідом. наук.-практ. конф. (Київ, 22 листоп. 2018 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2018. С. 406–409.

8. Теплицький Б. Б. Щодо завдань комп'ютерно-технічних експертиз при розслідуванні незаконного зайняття гральним бізнесом в Україні. *Судова експертиза: сучасність та майбутнє*: матеріали круглого столу (м. Львів, 25 січня 2018 р.); за заг. ред. д. т. н. Кузіна М.О. / Львівський науково-дослідний інститут судових експертиз Міністерства юстиції України. Львів, 2019. С. 127–129.

9. Теплицький Б. Б. Особливості оцінки результатів судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Використання досягнень сучасної науки й техніки в розкритті злочинів* : матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лют. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 223–225.

10. Теплицький Б. Б. Особливості суб'єктної складової техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку. *Кримінальне судочинство: сучасний стан та перспективи розвитку*: матеріали Всеукр. наук.-практ. конф. (Київ, 28 трав. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 384–387.

11. Теплицький Б. Б. Щодо визначення терміну «техніко-криміналістичне забезпечення розслідування кримінальних правопорушень». *Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності:* зб. матеріалів засідання № 1 постійно діючої Міжнар. наук.-практ. конф. (м. Кропивницький, 24 верес. 2021 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2021. С. 71–74.

які додатково відображають наукові результати дисертації:

12. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз: наук.-практ. посіб. / Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін. Київ: ПАЛИВОДА А.В., 2019. 168 с.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕОМ – Електронно-обчислювальні машини

ЕОТ – Електронно-обчислювальна техніка

КК – Кримінальний кодекс

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

НПУ – Національна поліція України

НСРД – негласні слідчі (розшукові) дії

СОГ – слідчо-оперативна група

СРД – слідчі (розшукові) дії

ВСТУП

Обґрунтування вибору теми дослідження. Аналіз криміногенної ситуації в Україні та практики органів досудового розслідування підтверджує тенденцію до збільшення кількості випадків кримінальних правопорушень, пов'язаних з обігом комп'ютерної інформації, а також діянь, у яких комп'ютерні інформаційні системи є засобами та знаряддями їх учинення або ж використовуються для приховування факту і слідів злочинної діяльності, а також спрямування зусиль правоохоронців на хибні об'єкти. Процеси глобальної інформатизації безпосередньо впливають на криміногенну ситуацію, обумовлюють нові способи і технології злочинних посягань в інформаційному простості й середовищі комп'ютерних мереж.

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, а також мереж електрозв'язку здебільшого високолатентні. Поряд з відсутністю очевидної слідової картини й традиційного «місця події» доволі ускладненим є збирання доказів, що зумовлено як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним, елементом обстановки – кібернетичним простором.

Злочинній діяльності відповідного спрямування притаманні переважно системний, професійний і груповий характер, наявність у правопорушників спеціальних знань, умінь і навичок у різних галузях науки і техніки (електроніка, електротехніка, програмування, телекомунікації, зв'язок тощо).

Згідно з офіційною статистикою, динаміка цієї категорії кримінальних правопорушень в Україні має тенденцію до щорічного зростання: якщо у 2013 р. їх зареєстровано 595, то тільки за 10 місяців 2021 р. – 2,8 тис. Йдеться про «класичні» кіберзлочини (ст. 361–363-1 КК України): несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (1,4 тис. або 50 %); несанкціоновані дії з інформацією, яка оброблюється в електронно-

обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації (1,2 тис. або 44 %) тощо[1].

Отже, забезпечення швидкого, повного та неупередженого розслідування і судового розгляду відповідних кримінальних проваджень неможливе без комплексного криміналістичного забезпечення. Відтак особливої актуальності набуває переосмислення теоретичних, правових і практичних основ використання слідчим (дізнавачем), спеціалістом та експертом сучасних техніко-криміналістичних засобів з метою отримання орієнтуючої та доказової інформації, зокрема під час проведення слідчих (розшукових) та інших процесуальних дій.

Теоретичним підґрунтям дослідження стали праці вітчизняних й іноземних учених різних часів, зокрема: Ю. П. Аленіна, В. В. Арешонкова, І. В. Басистої, В. П. Бахіна, В. Д. Берназа, Р. С. Бєлкіна, Т. В. Варфоломеєвої, В. І. Василинчука, Г. П. Власової, А. Ф. Волобуєва, В. І. Галагана, В. Г. Гончаренка, В. Я. Горбачевського, І. В. Гори, В. А. Журавля, А. П. Запотоцького, А. В. Іщенка, Н. І. Клименко, І. І. Когутича, В. А. Колесника, О. Н. Колесніченка, В. П. Колмакова, В. О. Коновалової, В. С. Кузьмічова, В. В. Лисенка, В. К. Лисиченка, В. Г. Лукашевича, Є. Д. Лук'янчикова, Д. М. Мірковця, А. В. Мовчана, Д. Й. Никифорчука, В. Т. Нора, О. В. Одерія, Ю. Ю. Орлова, В. Л. Ортинського, І. В. Пирога, М. А. Погорецького, І. В. Рогатюка, М. В. Салтевського, М. Я. Сегая, Д. Б. Сергєєвої, О. С. Старенького, Р. Л. Степанюка, О. В. Таран, О. Ю. Татарова, В. В. Тіщенка, В. В. Топчія, Л. Д. Удалової, В. І. Фаринника, В. Г. Хахановського, П. В. Цимбала, К. О. Чаплинського, С. С. Чернявського, Ю. М. Чорноус, В. М. Шевчука, В. Ю. Шепітька, М. Г. Щербаковського та ін.

[1] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування (2012–2021 рр.): статистична інформація Генеральної прокуратури України. URL: http://www. gp. gov. ua/ua/stat. html.

На монографічному рівні питання протидії комп'ютерній злочинності та забезпечення цієї діяльності в кримінально-правовому, кримінальному процесуальному, кримінологічному та криміналістичному аспектах вивчали Л. А. Безуглий, Л. В. Борисова, В. О. Голубєв, А. І. Журба, Н. В. Карчевський, Т. В. Коршикова, О. І. Мотлях, Л. П. Паламарчук, Д. В. Пашнєв, О. Д. Ричка, Н. А. Розенфельд, С. В. Шапочка, І. Р. Шинкаренко та інші науковці. Водночас засади техніко-криміналістичного забезпечення розслідування комп'ютерних злочинів на рівні дисертаційних робіт окремо не розглядалися. З урахуванням стрімких змін у законодавстві, злочинній діяльності та правоохоронній практиці зазначена проблематика потребує цільового комплексного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до положень Стратегії сталого розвитку «Україна – 2020» (Указ Президента України № 5/2015), Стратегії національної безпеки України (Указ Президента України № 392/2020), Стратегії розвитку системи Міністерства внутрішніх справ України до 2020 року (розпорядження Кабінету Міністрів України № 1023-р/2017), Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 років (наказ МВС України № 275/2015), Тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України № 454/2020), Основних напрямів наукових досліджень Національної академії внутрішніх справ на 2018–2020 роки (рішення Вченої ради НАВС від 26 грудня 2017 р., протокол № 28/1).

Тему дисертації затверджено рішенням Вченої ради Національної академії внутрішніх справ 22 грудня 2015 р. (протокол № 23).

Мета і завдання дослідження. *Метою* дисертації є розроблення теоретичних положень та науково обґрунтованих рекомендацій щодо техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Реалізація поставленої мети зумовила необхідність вирішення таких *задач*:

– з’ясувати стан наукового розроблення проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

– визначити поняття, зміст і суб’єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

– висвітлити найкращий зарубіжний досвід техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

– запропонувати поняття та здійснити розподіл техніко-криміналістичних засобів, що застосовуються під час досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

– розкрити особливості техніко-криміналістичного забезпечення проведення окремих слідчих (розшукових) дій у досліджуваній категорії кримінальних проваджень, надати пропозиції з удосконалення такого забезпечення;

– визначити специфіку та запропонувати рекомендації з удосконалення техніко-криміналістичного забезпечення проведення окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

– розкрити особливості призначення найбільш типових видів судових експертиз при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

– виявити типові помилки при призначенні експертизи комп'ютерної техніки і програмних продуктів як найбільш поширеного різновиду судових експертиз за злочинами даної категорії, запропонувати шляхи їх попередження;

– визначити особливості оцінки результатів судових експертиз та напрями їх використання під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Об'єкт дослідження – правовідносини, що виникають під час досудового розслідування і судового розгляду кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Предмет дослідження – техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Методи дослідження обрано з огляду на специфіку об'єкта, предмета, мети й завдань дослідження, а саме: *загальнонаукові* методи *(спостереження, порівняння, опису, класифікації)* – для визначення та систематизації правових категорій, що характеризують злочинну діяльність і слідчу практику, а також спеціальні методи: *історико-правовий* – для висвітлення етапів розвитку кримінального, кримінального процесуального законодавства, практики забезпечення органів досудового розслідування техніко-криміналістичними засобами і методами (підрозділ 1.1); *системно-структурний* – для розгляду видів і загальних вимог до техніко-криміналістичного забезпечення проведення слідчих (розшукових) дій, у тому числі негласних (підрозділи 1.2, 1.3, 2.2, 2.3); *догматичний* – з метою тлумачення понять і категорій кримінального процесу, криміналістики, оперативно-розшукової діяльності, що сприяло уточненню понятійно-категоріального апарату дослідження (розділи 1–3); *формально-логічний* – під час розгляду сутності техніко-криміналістичного забезпечення огляду, обшуку, допиту, проведення експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та

комп'ютерних мереж і мереж електрозв'язку (підрозділ 2.2, розділ 3); *моделювання* – для розроблення та впровадження в практику алгоритмів дій під час призначення експертиз у досліджуваній категорії кримінальних проваджень (підрозділи 3.1, 3.2); *соціологічні* – для з'ясування думок працівників правоохоронних органів щодо сучасного стану техніко-криміналістичного забезпечення розслідування кримінальних правопорушень цієї категорії (розділи 1−3); *статистичний* – для узагальнення результатів соціологічних досліджень, вивчення матеріалів кримінальних проваджень (розділи 1–3).

Емпіричну базу дослідження становлять результати вивчення та узагальнення 285 кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку упродовж 2016–2021 років; зведені дані опитування 180 слідчих, 350 судових експертів з Вінницької, Дніпропетровської, Житомирської, Закарпатської, Запорізької, Івано-Франківської, Київської, Львівської, Одеської, Рівненської, Чернівецької областей та м. Києва; статистичні й аналітичні матеріали Департаменту інформаційно-аналітичної підтримки Національної поліції України, Державного науково-дослідного експертно-криміналістичного центру МВС України, Офісу Генерального прокурора, Державної судової адміністрації України за 2016–2021 роки, а також результати багаторічного вивчення слідчої та судово-експертної практики з урахуванням значного досвіду роботи автора в експертних підрозділах МВС України.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним з перших в Україні комплексних монографічних досліджень засад техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. У роботі сформульовано й обґрунтовано низку положень і висновків теоретичного та практичного спрямування, а саме:

вперше:

– запропоновано визначення техніко-криміналістичних засобів розслідування злочинів у сфері використання електронно-обчислювальних машин

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку як системи спеціально виготовлених або пристосованих приладів, пристроїв, засобів вимірювальної техніки, допоміжного обладнання, інструментів, матеріалів, інформаційних пошукових, ідентифікаційних та інших систем, а також криміналістичних технологій їх ефективного застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів;

– запропоновано нормативне закріплення діяльності комп'ютерно-технічної лабораторії у складі спеціалізованої пересувної лабораторії Експертної служби МВС та необхідність її залучення під час розслідування злочинів у даній сфері;

– надано пропозиції до кримінально процесуального законодавства щодо посилення захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій та зберігання технічних засобів і первинних носіїв інформації, які використовувались під час проведення негласних слідчих (розшукових) дій;

– узагальнено типові помилки під час призначення експертизи комп'ютерної техніки та програмних продуктів, з поділом їх щодо якості і кількості поданих на дослідження об'єктів, процесуальних питань винесення постанов (ухвал) про призначення експертизи тощо, розроблено комплекс заходів з їх попередження;

– обґрунтовано необхідність, з метою підвищення ефективності розслідування злочинів даної категорії, запровадження відповідної спеціалізації слідчих Національної поліції України, а також регламентації у вимогах до цих посад крім юридичної наявності професійно-технічної або вищої технічної освіти принаймні початкового рівня (короткого циклу) за відповідним напрямом;

удосконалено:

– поняття техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку шляхом включення до нього в якості складових елементів сукупності техніко-криміналістичних засобів та прийомів їх

застосування, діяльності уповноважених суб'єктів щодо створення належних умов для використання зазначених засобів, а також системи наукових положень, спрямованих на реалізацію практичних завдань із застосування криміналістичної техніки;

– поняття та класифікацію суб'єктів техніко-криміналістичного забезпечення розслідування злочинів даної категорії як осіб, які реалізують свої повноваження на підставі чинного законодавства, використовуючи техніко-криміналістичні засоби для здійснення ефективного розслідування злочинів; поділ їх на індивідуальних та колективних суб'єктів;

– положення щодо організації і тактики застосування техніко-криміналістичних засобів під час проведення огляду, обшуку, допиту у кримінальних провадженнях при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– критерії оцінки висновків експертів з урахуванням кількісно-якісних характеристик наданих на дослідження об'єктів і порівняльних зразків, застосованих експертом методик, повноти досліджень, правильності опису та наукової обґрунтованості проміжних і підсумкових висновків;

дістало подальший розвиток:

– визначення напрямів наукових досліджень різних аспектів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– рекомендації на основі аналізу зарубіжного досвіду з удосконалення правового регулювання протидії кіберзлочинам, залучення вітчизняних фахівців у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку до вирішення завдань техніко-криміналістичного забезпечення розслідування кіберзлочинів, а також міжнародної технічної допомоги, пов'язаної з техніко-криміналістичним забезпеченням протидії кіберзлочинам в Україні тощо;

– наукові погляди щодо видів техніко-криміналістичних засобів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку з їх розподілом на апаратні та програмні засоби мобільної криміналістики; апаратні блокиратори запису; програмні засоби копіювання даних; програмні засоби комп'ютерної експертизи; апаратні засоби відновлення даних; відкрите спеціалізоване програмне забезпечення; дистрибутиви на основі Linux;

– рекомендації з техніко-криміналістичного забезпечення проведення окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– бачення можливостей судових експертиз для встановлення обставин учинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та рекомендацій з підготовки до їх призначення.

Практичне значення отриманих результатів полягає в тому, що результати дисертації впроваджено та може бути використано в:

законотворчій діяльності – при підготовці змін та доповнень до нормативно-правових актів, якими регламентуються призначення і проведення судових експертиз та експертних досліджень (акт Інституту законодавства Верховної Ради України від 16 травня 2019 р. № 22/696-1-15);

правозастосовній діяльності – у системі службової підготовки та в оперативно-службовій діяльності органів досудового розслідування й експертних підрозділів МВС України (акт Головного слідчого управління Національної поліції України від 16 серпня 2021 р.; акт Державного науково-дослідного експертно-криміналістичного центру МВС України від 15 квітня 2021 р.);

освітньому процесі – під час викладання блоку навчальних дисциплін з криміналістики, розслідування окремих категорій кримінальних правопорушень, судової експертизи, підготовки навчальних та методичних посібників,

підручників, курсів лекцій і проведення наукових досліджень відповідного спрямування (акт Національної академії внутрішніх справ від 04 жовтня 2021 р.).

Особистий внесок здобувача. Дисертація є самостійною, завершеною науковою працею. Сформульовані в ній узагальнення, висновки, рекомендації та пропозиції обґрунтовано на підставі самостійно здійснених досліджень. В опублікованому у співавторстві науково-практичному посібнику «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз» власні теоретичні розробки дисертанта становлять не менше 25 %. Наукові ідеї та висновки, що належать співавторам, у дисертації не використано.

Апробація результатів дисертації. Основні положення та висновки дисертації оприлюднено на трьох міжнародних і всеукраїнських науково-практичних конференціях та засіданнях круглих столів, серед яких: «Судова експертиза: сучасність та майбутнє» (Львів, 25 січня 2018 року); «Актуальні проблеми криміналістики та судової експертології» (Київ, 22 листопада 2018 року); «Використання досягнень сучасної науки й техніки в розкритті злочинів» (Київ, 25 лютого 2021 р.); «Кримінальне судочинство: сучасний стан та перспективи розвитку» (Київ, 28 травня 2021 р.); «Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності» (Кропивницький, 24 вересня 2021 року).

Структура та обсяг дисертації. Робота складається з анотації, переліку умовних позначень, вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел (202 найменування на 22 сторінках) і шести додатків (на 31 сторінці). Повний обсяг дисертації становить 268 сторінок, з них основного тексту – 197 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ОСНОВИ ТЕХНІКО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

1.1. Стан наукових досліджень проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Пошуки шляхів підвищення ефективності боротьби зі злочинами, що вчиняються у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, ведуться в різних напрямках. Один з них – наукова розробка проблеми. Інтерес учених до цих питань останнім часом значно зріс. Більш детальне вивчення комп'ютерної злочинності виявляє ряд аспектів цієї проблеми, які найважче піддаються дослідженню. Як правило, вони знаходяться у так званих суміжних галузях науки, на стикові різних наукових дисциплін [33].

Більше того, розвиток сучасних інформаційних технологій, удосконалення виробництва й розширення сфери застосування новітньої кібернетичної техніки дали можливість зародження специфічного, складного виду злочинних діянь, де комп'ютерне оснащення та електронна інформація є об'єктом протиправного посягання [173, с. 12]. Водночас із позитивними здобутками інформатизація супроводжується побічним негативним явищем криміногенного характеру, до якого належать злочини у сфері ЕОМ (комп'ютерів), систем і комп'ютерних мереж або ж «комп'ютерна злочинність» (скорочена назва цього виду злочинів). На сучасному етапі технологізації суспільства відбувається перехід від простої поодинокої комп'ютерної злочинності до організованої – складної.

Прослідковується динаміка її злиття з міжнародним криміналітетом, що несе відповідну загрозу суспільству загалом [198].

Правові засади протидії комп'ютерній злочинності визначено у Кримінальному кодексі України (далі – КК), який у розділі XVI Особливої частини «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить низку статей, що передбачають кримінальну відповідальність за комп'ютерні злочини.

Поряд з цим, перелік комп'ютерних злочинів не вичерпується діяннями, зазначеними у розділі XVI КК України. Певні злочини, які існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій.

Варто зазначити, що така транскордонність значно ускладнює для працівників правоохоронних органів різних держав можливість розкриття та розслідування цієї категорії злочинів.

Завдання даного підрозділу полягає у проведенні комплексного аналізу стану наукових досліджень проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Питанням протидії злочинам у сфері високих інформаційних технологій у вітчизняній криміналістичній літературі приділялася певна увага з акцентуванням на деякі проблеми у тактиці та методиці розслідування цих злочинних деліктів [85]. Зокрема, зазначеній проблематиці у різні часи присвятили свої роботи такі вчені: В. О. Голубєв, М. А. Погорецький, О. І. Мотлях, Л. П. Паламарчук, Д. В. Пашнєв, І. Р. Шинкаренко, В. Ю. Шепітько, Н. В. Карчевський та інші. Однак з урахуванням стрімких змін у кримінальному середовищі й появи нових способів злочинних посягань, ситуація вимагає постійного вдосконалення та доопрацювання засобів вирішення зазначених проблем [85].

Водночас, мають місце також і шахрайства, учинені з використанням ЕОМ. Відповідно, проблема розслідування шахрайств, учинених з використанням ЕОМ, постійно перебувала в полі зору сучасних науковців, зокрема, Т. Аверьянова, Д. Азарова, Б. Андрєєва, Ю. Батуріна, О. Баранова, М. Вертузаєва, Т. Варфоломеєва, О. Волєводз, В. Гончаренка, В. Голубєва, М. Гуцалюка, В. Гавловського, В. Губанова, М. Карчевського, В. Колесник, О. Котляревського, В. Крилова, Р. Калюжного, М. Камлика, В. Міщенка, В. Оборського, Б. Романюка, О. Стрільціва, О. Усова, В. Хорста, В. Цимбалюка та інших. Розробка проблем криміналістичної методики на цьому етапі стосувалася передусім окремих питань розслідування злочинів відповідно до побудови норм законодавства про кримінальну відповідальність [68; 83].

Зокрема, на думку Л. Кривоченка, конструкція «шахрайство, учинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки», свідчить про специфічний спосіб учинення цього злочину, до того ж його небезпечність полягає в тому, що ця техніка значно полегшує вчинення шахрайства, дає змогу заволодівати значними коштами, завдаючи непоправної шкоди власникам [79, с. 160], а науковець М. Хавронюк вважає, що електронно-обчислювальна техніка в ч. 3 ст. 190 Кримінального кодексу України [80] є засобом учинення шахрайства [179, с. 196].

Згодом, з огляду на накопичення емпіричного матеріалу та розвиток загальної теорії криміналістики, розпочалося вивчення методологічних засад цієї діяльності, її загальних положень, які нині складають базу кожної окремої методики [11; 106].

Різним аспектам комп’ютерної злочинності, способам і механізму їх учинення, технології та техніці виявлення та закріплення слідів, тактиці проведення слідчих дій приділяють увагу вітчизняні й зарубіжні вчені. Скажімо, дослідженнями окремих аспектів боротьби зі злочинами, що вчиняються з використанням комп’ютерних мереж загалом, і шахрайством зокрема, займалися такі вчені: Д.С. Азаров, Б.В. Андрєєв, О.А. Баранов, Ю. М. Батурін, В. М. Бутузов, Т.В. Варфоломеєв, М.С. Вертузаєв, О.Г. Волєводз, В. Д. Гавловський,

В.О. Голубєв, В.Г. Гончаренко, В.А. Губанов, М.В. Гуцалюк, Д.О. Зиков, М.І. Камлик, М.В. Карчевський, В.А. Колесник, А.А. Комаров, О.І. Котляревський, В.В. Крилов, В. Д. Ларичев, А. К. Лебедєв, О.В. Лисодєд, В.Б. Міщенко, О.І. Мотлях, В.І. Оборський, Б.В. Романюк, О.В. Смаглюк, О.М. Стрільців, О.І. Усов, С.С. Чернявський, В.П. Хорст, В.С. Цимбалюк, В.П. Шеломенцев, О.М. Юрченко та інші.

Убачається, що одне з перших досліджень у цьому напрямі здійснив О.І. Мотлях у дисертації «Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій» [101]. Автором проаналізовано сучасний стан розвитку злочинності з використанням комп'ютерних технологій. Наголошено, що новий Кримінальний кодекс України, в якому є окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», кваліфікує злочини у сфері високих технологій, і це позитивно позначилося на практиці його застосування. Автор доводить, що розкриття розслідуваної категорії злочинів має доволі складний характер і потребує окремого теоретичного і практичного досвіду. З цією метою О. І. Мотлях визначив зміст кримінально-правової та криміналістичної характеристики комп'ютерних злочинів; зробив аналіз типових слідчих ситуацій, які можуть скластися при розслідуванні таких злочинів; виклав порядок висунення та перевірки криміналістичних версій тощо. Звернуто увагу на фахову підготовку відповідних спеціалістів у структурі правоохоронних органів для цього напряму розслідування злочинів. Запропоновано розробку нового науково-технічного спорядження, яке сприятиме виявленню, фіксації і вилученню електронних джерел доказового значення. Вказав на особливості проведення деяких слідчих дій та призначення необхідних видів експертиз, сформулював рекомендації для відшкодування потерпілому заподіяних злочином збитків і моральної шкоди [100, с. 4–5].

Л. П. Паламарчук у дисертації «Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (2005) [110]. Зокрема,

Л.П. Паламарчук розкрив системне уявлення про способи вчинення цих кримінальних правопорушень, слідову картину незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що розширили і поглибили знання про методику його розслідування. У своїй роботі науковець зазначав, що незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж може вчинятися шляхом отримання інформації в результаті злочинних шахрайських дій. Разом з тим учений оминув у дослідженні вчинення доступу з використанням шахрайських дій [109, с. 3–4].

Досить цікавою, на нашу думку, є дисертація А.І. Журби «Особливості предмету доказування у справах про комп'ютерні злочини». Зокрема, до найбільш суттєвих нових положень і висновків, обґрунтованих у дисертаційному дослідженні, автор відніс такі: вперше – вказано на необхідність спеціалізації не лише органів дізнання, досудового слідства, але й прокуратури, суду під час розслідування та судового розгляду кримінальних справ про комп'ютерні злочини, що обумовлюється формуванням внутрішнього переконання суб'єкта доказування на якісній оцінки доказів з урахуванням технічної сторони злочину; запропоновано створення криміналістичної бази даних про осіб, засуджених за вчинення комп'ютерних злочинів, яка містить їх групове розмежування за особливостями технічних пізнань; запропоновано зміни до норм чинного кримінального законодавства з метою приведення їх у відповідність до існуючої сучасної технічної термінології у сфері автоматизованих систем; удосконалено – поняття комп'ютерного злочину, в основу якого покладено вчинення суспільно небезпечного діяння з використанням ЕОМ та спрямування його на комп'ютерну інформацію; зміст предмета кримінально-процесуального доказування та визначено його співвідношення зі складом злочину: встановлення елементів складу злочину є пріоритетним під час кримінально-процесуального доказування; дістало подальшого розвитку визначення місця події комп'ютерного злочину відносно місця настання суспільно небезпечних наслідків, з урахуванням чого запропоновано нову редакцію п. 1 ст. 64 КПК України; положення про

обов’язкове доказування інтелектуальної спроможності обвинуваченого вчинити комп’ютерний злочин. Для встановлення рівня спеціальних знань обвинуваченого запропоновано доводити за кожною кримінальною справою про комп’ютерний злочин особливі пізнання обвинуваченого у галузях комп’ютерних технологій, враховуючи різноманітність механізмів вчинення комп’ютерних злочинів, використання індивідуальних та загальних методик і інструментів вчинення злочину тощо [47, с. 4].

Не менш важливим є наукове дослідження Д.В. Пашнєва «Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп’ютерних технологій». Так, у роботі автор дає визначення «комп’ютерним злочинам» «комп’ютерним технологіям» і розкриває їх зміст. Досліджуються типові способи застосування комп’ютерних технологій в злочинних цілях. Способи диференціюються згідно підготовчому, основному, заключному етапам вчинення комп’ютерних злочинів. Зазначено, що комп’ютерні сліди виникають під впливом комп’ютерних технологій і являють собою якісні та кількісні зміни комп’ютерної інформації. У дисертації розглядається структура та форми використання спеціальних знань при розслідуванні комп’ютерних злочинів [113, с. 5]. Вказується, що знання фахівців складають основні спеціальні технічні знання та додаткові юридичні знання. Дисертантом запропоновані принципи створення комп’ютерних технологій збирання комп’ютерних слідів, наведені існуючи програмно-технічні засоби їх дослідження. Особливу увагу приділено застосуванню спеціальних знань на стадії порушення кримінальної справи. Підтримана пропозиція щодо проведення на цій стадії судової експертизи. Розглянуті особливості роботи спеціаліста при проведенні слідчих дій в залежності від ситуацій. Дано визначення предмету комп’ютерно-технічної експертизи, її задач та об’єктів дослідження тощо [113, с. 5].

Заслуговує на увагу і дисертаційна робота Т. А. Пазинич «Криміналістична характеристика шахрайств та основні положення їх розслідування». Так, наприклад, авторка здійснила класифікацію шахрайств, визначила особливості їх криміналістичної характеристики та сформулювала положення і рекомендації

щодо розслідування окремих класифікаційних груп шахрайств. Окремо науковець виділила категорію шахрайств, що вчиняються у сферах використання електронних технологій, та проаналізувала основні елементи їх механізму. Ученою наголошено, що шахрайства названої категорії специфічні з точки зору використовуваних засобів і середовища (обстановки), які обумовлюють особливість носіїв інформації про кримінальне правопорушення і, відповідно, виявлення, фіксацію, дослідження і використання доказів [108, с. 6].

Крім того, Т.А. Пазинич акцентує на тому, що особливістю вказаних кримінальних правопорушень є те, що вони можуть бути вчинені в різноманітних сферах суспільного життя, зокрема у побуті, функціонуванні окремих суспільних інститутів, підприємницькій діяльності тощо. Місце безпосереднього вчинення протиправного діяння (місцезнаходження злочинця, засобів вчинення кримінального правопорушення) не співпадає з місцем знаходження потерпілого і настання наслідків кримінального правопорушення, що пов’язано з використанням ЕОМ. Шахрай заволодіває предметом посягання (грошовими коштами) з використанням різноманітних електронних технічних засобів і відповідного середовища (стільникового зв’язку, пластикових платіжних карток, комп’ютерної Інтернет-мережі) [108, с. 6].

Л.А. Безуглий у дисертаційному дослідженні «Запобігання незаконному відтворенню та розповсюдженню комп’ютерних програм і баз даних» розглянув проблеми запобігання незаконному відтворенню та розповсюдженню комп’ютерних програм і баз даних, зокрема, процеси виникнення та встановлення кримінальної відповідальності за порушення авторського права на комп’ютерні програми та бази даних. Крім того, автором з’ясовано генезис законодавства України та деяких країн Європи та Азії з питань запобігання злочинам, пов’язаним із порушенням авторського права у цій сфері. Визначено стан і тенденції злочинності, пов’язаної з порушенням авторського права на комп’ютерні програми та бази даних в Україні. Проаналізовано зв’язок таких злочинів з іншими злочинами у сфері економіки та корупцією. Обґрунтовано детермінанти таких злочинів. Наведено кримінологічну класифікацію осіб, які

вчиняють незаконні відтворення та розповсюдження комп'ютерних програм та баз даних. Розроблено систему заходів загально-соціального та спеціально-кримінологічного запобігання незаконному відтворенню та розповсюдженню комп'ютерних програм та баз даних тощо [7, с. 3].

У дисертації С.В. Шапочки «Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж» (2018 р.), автором запропоновано власну класифікацію шахрайства, що вчиняється з використанням комп'ютерних мереж, визначаються детермінанти та ступінь його латентності.

Однією з нових наукових робіт є дисертація Т.В. Романенко-Коршикової «Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» (2021). Так, авторкою вперше розроблено алгоритм першочергових заходів, які здійснюють уповноважені підрозділи Національної поліції України в разі надходження інформації про шахрайство, вчинене з використанням ЕОТ, які об'єднано в блоки: з'ясування обставин шахрайства; внесення відомостей до ЄРДР; визначення напрямів встановлення IP-адрес, які використовувались ЕОТ з метою вчинення шахрайства; виявлення ЕОТ, які використовувались з метою вчинення шахрайства; фіксація причетності осіб до використання ЕОТ з метою вчинення шахрайства та отримання/неотримання коштів чи майна під час вчинення шахрайства; проведення СРД та НСРД; визначено обставини, які підлягають встановленню під час розслідування шахрайств, учинених з використанням ЕОТ; розроблено наукові основи розслідування шахрайства, вчиненого з використанням ЕОТ, а також структуру криміналістичної характеристики, до якої включено такі елементи: предмет злочинного посягання та спосіб вчинення кримінального правопорушення, у поєднанні зі способами готування і приховування вчинення шахрайства з використанням ЕОТ; слідова картина вчиненого кримінального правопорушення, типові цифрові сліди такого виду шахрайства та механізм їх утворення; особа злочинця та особа потерпілого; обстановку вчинення – місце, час, умови та інші обставини, що є типовими для вчинення кримінального правопорушення цієї категорії; визначено порядок і тактику огляду ЕОТ, а також інформації, що

міститься в ній, з метою виявлення матеріальних та цифрових слідів, які можуть бути доказами у кримінальних провадженнях про вчинення шахрайства з використанням ЕОТ [146, с. 134].

Що стосується наукових робіт, присвячених дослідженням проблем кримінально-правової характеристики злочинів, які вчиняються з використанням ЕОТ, то тут необхідно відмітити праці окремих науковців.

У 2003 році Н.А. Розенфельд здійснила дисертаційне дослідження на тему: «Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». Дисертація присвячена теоретичним та практичним питанням застосування кримінально-правової норми, що передбачає відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж в Україні. Досліджений юридичний склад злочину, передбаченого ст. 361 КК України, види, співвідношення аналізованих злочинів з іншими злочинами та критерії їх відмежування від суміжних складів злочинів, питання кваліфікації за сукупністю з іншими злочинами, а також нормативно-правові та міжнародно-правові заходи захисту від таких злочинів [142, с. 126–127].

Авторка наголошує на практичній доцільності виокремлення і розгляду як самостійних юридичних складів злочинів «Несанкціонований доступ до комп'ютерної інформації» та «Умисне розповсюдження шкідливих комп'ютерних програм», альтернативних діянь, передбачених чинною редакцією ч.1 ст. 361 КК України. У роботі запропоновано закріпити вказані юридичні склади в окремих статтях Особливої частини КК України та наводиться рекомендована редакція таких статей, яка підготовлена дисертанткою з урахуванням сучасних світових вимог до кримінально-правової регламентації норм, що передбачають відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Надано коментар до рекомендованої редакції статей, що передбачають кримінальну відповідальність

за злочини «Несанкціонований доступ до комп'ютерної інформації» та «Умисне розповсюдження шкідливих комп'ютерних програм» [142, с. 126–127].

М.В. Карчевським у дисертації «Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)» розкрито кримінально-правовий зміст інформаційних відносин у сфері використання комп'ютерної техніки як родового об'єкта злочинів, передбачених розділом XVI КК України, обґрунтовано пропозицію про доцільність визначення їх загальним терміном «комп'ютерні злочини». На підставі визначення родового об'єкта розкрито зміст безпосереднього об'єкта незаконного втручання як суспільних відносин власності на комп'ютерну інформацію [57, с. 67]. Відповідно по-новому визначено комп'ютерну інформацію як предмет цього злочину і надано пропозиції щодо недоцільності передбачення в диспозиції ст. 361 КК України вказівки на носії інформації як самостійний предмет незаконного втручання. Визнано необґрунтованим передбачення комп'ютерного вірусу в ч. 1 ст. 361 КК України як самостійного предмета злочину. Замість цього запропоновано визначити предметами незаконного втручання програмні та технічні засоби, призначені для незаконного втручання, до яких відносяться комп'ютерні віруси. По-новому визначено знищення та перекручення комп'ютерної інформації як різні форми порушення права власності на комп'ютерну інформацію. Автором вперше у вітчизняній науці здійснено спробу класифікації способів незаконного втручання, що має важливе значення для встановлення об'єктивної сторони та ступеня суспільної небезпечності злочину, що досліджується. Доведено необхідність доповнення ч. 2 ст. 361 КК України кваліфікуючими ознаками, як «вчинення незаконного втручання шляхом несанкціонованого доступу до комп'ютерної інформації» та «вчинення незаконного втручання особою, яка має доступ до роботи на ЕОМ», у системі чи комп'ютерній мережі зважаючи виконувану роботу або посадою, яку займає особа. Обґрунтовано необхідність доповнення ст. 361 КК України частиною 3, яка б передбачала відповідальність за незаконне втручання, що спричинило тяжкі наслідки, та розкрито зміст таких наслідків. Запропоновано

нову редакцію ст. 361 КК України «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» [57, с. 67].

О.Д. Ричкою у дисертації «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» розкрито особливості кримінально-правової кваліфікації у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено засади здійснення кримінально-правової кваліфікації. Окреслено ознаки, притаманні даній категорії злочинної діяльності. Визначено ознаки кібернетичних злочинів. Висвітлено ґенезу та поняття злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Досліджено різновиди як міжнародних, так і національних кібернетичних злочинів. Проведено комплексний аналіз елементів складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено об'єкт і предмет 17 кібернетичних злочинів, здійснено аналіз та розкрито зміст об'єктивної сторони; встановлено суб'єктів та досліджено особливості суб'єктивної сторони злочинів даної категорії. Розглянуто кваліфікуючі ознаки та здійснено їх відмежування від суміжних складів, на підставі чого сформовано нововведення та доповнення до чинного законодавства України з питань здійснення кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [141, с. 78–79].

Поряд з цим, на рівні монографічних робіт окремі аспекти зазначеної проблематики вивчалися Д.С. Азаровим, М.О. Кравцовою. В.М. Бутузовим тощо.

Убачається, що Д.С. Азаров у монографії «Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)», провів перше в Україні комплексне монографічне кримінально-правове дослідження проблем

відповідальності за посягання, що нині все частіше називають кіберзлочинами. Ця праця видається досі актуальною, адже відповідні норми кримінального права останнім часом не зазнавали змістовного редагування. У монографії також досліджуються проблеми кримінальної відповідальності за злочини у сфері комп'ютерної інформації, пов'язані зі ступенем і характером суспільної небезпеки цих посягань та їх міжнародним характером, ознаками складів цих злочинів, а також санкціями, передбаченими за їх вчинення. Узагальнюється зарубіжний та міжнародний досвід кримінально-правової протидії «комп'ютерним» злочинам. Розроблена доктринальна модель системи норм про кримінальну відповідальність за аналізовані злочини, для втілення якої пропонується проект Закону України «Про внесення змін і доповнень до Кримінального кодексу України щодо відповідальності за злочини у сфері комп'ютерної інформації» тощо [2, с. 234].

В. М. Бутузовим у монографії «Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз), розкрито основні проблеми протидії комп'ютерній злочинності в Україні. Висвітлено наукові підходи до визначення поняття та сутності комп'ютерній злочинності, розглянуто її характеристики. Наведено результати системно-структурного аналізу даного явища. Охарактеризовано системи суб'єктів, заходів і правового забезпечення протидії комп'ютерній злочинності в Україні [21, с. 336–337].

Монографія А.М. Панова «Запобігання кіберзлочинності в Україні» присвячена вивченню кримінологічних засад запобігання кіберзлочинності в Україні. Охарактеризовано сучасний стан кіберзлочинності в Україні: встановлено її рівень, динаміку, величину та фактори латентності, структуру, географію. Проаналізовано соціально-демографічні, кримінально-правові та морально-психологічні риси осіб, засуджених за вчинення кіберзлочинів. Автором встановлено основні політико-правові, соціально-економічні, організаційно-управлінські та культурно-психологічні фактори кіберзлочинності. Досліджено стан та запропоновано шляхи удосконалення правового регулювання діяльності органів внутрішніх справ і Національної поліції щодо запобігання кіберзлочинності [112, с. 112].

Поряд з цим, низку методичних рекомендацій було присвячено способам встановлення місцезнаходження ЕОТ, з використанням якої вчинялися кримінальні правопорушення. Серед яких можна відмітити наступні: «Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту (2014) [106, с. 35], «Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів» (2016) [144, с. 26], «Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет медійного контенту провайдерами програмних послуг та Інтернет-провайдерами» (2017) [143, с. 22], «Використання спеціальних знань під час розслідування несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» (2018) [26, с. 25] «Розслідування кримінальних правопорушень, вчинених у сфері захисту інтелектуальної власності з використанням мережі Інтернет» (2021) [145, с. 39] тощо.

У підсумку, варто зазначити, що сучасний стан боротьби зі злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, визначив для криміналістики низку невирішених завдань. Найбільш суттєві з них – у галузі криміналістичної методики, оскільки саме тут відзначається основне відставання рівня науково-методичних рекомендацій від потреб практики. Йдеться не лише про відсутність методик розслідування «нових» кримінальних правопорушень, а й про застарілість підходів до розслідування тих діянь, що, зберігаючи стару кримінально-правову форму, значно змінилися змістовно. Нині у криміналістиці розробка окремих методик ведеться за шаблоном, у якому практичний аспект, нерідко, взагалі відсутній, тоді як їх основою повинні бути саме методи, адаптовані до рівня сприйняття конкретним користувачем.

Зазначене підтверджується результатами проведеного в межах дисертаційного дослідження анкетування. Так, на питання чи відповідає існуюча методика розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж

електрозв'язку існуючому рівню злочинності в даній сфері 87% опитаних респондентів (слідчі Національної поліції, експерти Експертної служби МВС України) відповіли негативно на дане питання, 10% - підтвердили відповідність методики, та 3% не змогли відповісти на дане питання. Серед положень методики розслідування злочинів даної категорії, які потребують свого доопрацювання та подальшого розроблення, 64% опитаних респондентів відповіли про необхідність розроблення положень саме техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Відтак, вивчення проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, на рівні дисертаційних робіт не проводилось, що і обумовлює його актуальність.

1.2. Поняття, зміст і суб'єкти техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

У сучасних умовах розвитку України як правової демократичної держави особливого значення набуває якісне застосування технічних засобів у діяльності з протидії злочинності. Різноманітні засоби криміналістичної техніки створюються, вдосконалюються і використовуються для ефективного пошуку та дослідження слідів злочинів, фіксації ходу і результатів слідчих (розшукових) дій у кримінальному провадженні, а також у судово-експертній діяльності. Отже, правові, організаційні й тактичні засади відповідної діяльності органів правопорядку залишаються в центрі уваги криміналістичної науки, оскільки тільки правильне, засноване на неухильному дотриманні принципів законності та

наукової обґрунтованості, застосування криміналістичної техніки є запорукою забезпечення прав і свобод людини в судочинстві [116, с. 221–222].

Власне тому, одним із першочергових наукових завдань видається з'ясування поняття, змісту і суб'єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Тому вказані органи в своїй діяльності використовують весь потенціал розроблених криміналістичною наукою технічних засобів і рекомендацій задля оптимізації діяльності з досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Зокрема, мова йде про такий різновид криміналістичного забезпечення досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Видається за доцільне зупинитися на встановленні сутності поняття та змісту технічко-криміналістичного забезпечення досудового розслідування злочинів взагалі, злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, зокрема.

Так, питання, пов'язані з криміналістичним, в тому числі техніко-криміналістичним забезпеченням розслідування кримінальних правопорушень, його поняттям, змістом, значенням і місцем у структурі криміналістики були предметом досліджень у працях таких вітчизняних і зарубіжних учених як: В.Д. Берназ, Р.С. Бєлкін, В.А. Волинський, А.Ф. Волобуєв, Г.І. Грамович, Р.Б. Єзерський, В.А. Журавель, Н.І. Клименко, В.Я. Колдін, В. Г. Коломацький, В.О. Коновалова, В.В. Лисенко, Є.Д. Лук'янчиков, В.О. Образцов, О.В. Одерій, М.В. Салтевський, Р.Л. Степанюк, П.Т. Скорченко, А.С. Падей, І.В. Пиріг, Ж.В. Удовенко, Ю.М. Чорноус, В.Ю. Шепітько, Н.П. Яблоков та інших.

Утім, у наукових працях спостерігається відсутність диференціації у сприйнятті сутності, змісту та місця техніко-криміналістичного забезпечення досудового розслідування, суб'єктів проведення такої діяльності, окремих засобів, які використовуються в її межах уповноваженими особами тощо.

Поряд з цим, варто наголосити й на значному оновленні чинного національного законодавства, що визначає правові й організаційні засади діяльності органів досудового розслідування, що має свій безпосередній вплив і на її техніко-криміналістичне забезпечення.

Убачається, що найбільш широкого вжитку в науковому обігу на цей час набуло поняття техніко-криміналістичного забезпечення слідчої діяльності. Це пов'язано передусім із загальною спрямованістю криміналістичних рекомендацій на досудове розслідування, що історично викликано успадкуванням Україною моделі криміналістики передусім як науки про розслідування злочинів. Приблизно наприкінці 80-х – на початку 90-х років минулого століття криміналістичну техніку і техніко-криміналістичні засоби науковці почали ототожнювати з техніко-криміналістичним забезпеченням розкриття і розслідування злочинів. Ці проблеми досліджувалися протягом наступних років, але дотепер не вироблено єдиного розуміння наведеного поняття [116, с. 223–224].

Одним із перших почав ґрунтовно вивчати сутність техніко-криміналістичного забезпечення розкриття та розслідування злочинів В.О. Волинський [29, с. 25–26]. Автор надав визначення даного поняття як здійснюваної правоохоронними органами діяльності, спрямованої на створення умов їх постійної готовності до застосування методів і засобів криміналістичної техніки та реалізацію цих умов у кожному конкретному випадку розкриття й розслідування злочинів [76, с. 67]. Тобто було запропоновано говорити насамперед про відповідний аспект практичної діяльності уповноважених органів.

Видається, що такий підхід надалі був розвинений як самим автором, так і іншими ученими-криміналістами. При цьому удосконалення даного поняття здійснюється в основному шляхом розширення його трактування не просто як

діяльності, а як складної системи, що включає не тільки діяльність як частину цієї системи, а й її організацію, нормативно-правове регулювання, науковий супровід тощо [116, с. 222].

Проте, К.В. Бугаєв не поділяє позицію науковців, котрі визначають техніко-криміналістичне забезпечення розкриття і розслідування злочинів тільки як діяльність, і підкреслює, що ця діяльність є функцією системи. Проте, надаючи поняття функції, необхідно розуміти сутність самої системи. Тому техніко-криміналістичне забезпечення є комплексною організаційно-функціональною системою, що у своїй діяльності спрямована на збирання і дослідження криміналістично значущої інформації та реалізує свої можливості шляхом застосування техніко-криміналістичних методів і засобів [18].

Підтримуємо думку С. Перліна, що у цілому є підстави стверджувати, що в криміналістичній науці трактування техніко-криміналістичного забезпечення розкриття і розслідування злочинів як складної системи знайшло широку підтримку [116, с. 222].

Зокрема, Р.Б. Єзерський визначає його як організаційно-функціональну систему, що спрямована на створення умов постійної готовності служб і підрозділів органів досудового розслідування до швидкого та ефективного вирішення завдань щодо отримання, накопичення й опрацювання криміналістично-значущої (доказової, пошукової та тактично-орієнтуючої) інформації і ефективного її використання у процесі розкриття й розслідування злочинів [44, с. 12]. Поряд з цим, В.О. Михайлов, П.Т. Скорченко, Ю.М. Чорноус та інші автори також пропонують розуміти під техніко-криміналістичним забезпеченням слідчої діяльності систему наукових, правових, організаційних положень і прикладних заходів із розроблення, впровадження та практичного використання техніко-криміналістичних засобів з метою успішного виявлення, розкриття, розслідування злочинів та запобігання їм [156, с. 21]. Незважаючи на деякі редакційні відмінності у визначеннях, погляди вказаних авторів загалом збігаються, адже техніко-криміналістичне забезпечення трактується як певна

система теоретичних положень і практичних засобів, спрямованих на реалізацію досягнень криміналістичної техніки в розслідуванні злочинів [116, с. 222].

Н. І. Пінчук у своєму дослідженні, присвяченому теоретичним і правовим питанням та практиці криміналістичного забезпечення діяльності нотаріату звертає увагу на те, що частіш за все про криміналістичне забезпечення кажуть як про створення умов для успішного застосування криміналістичних можливостей з метою успішного розв'язання завдань конкретної сфери правоохоронної діяльності, як про систему запровадження в практичну діяльність посадових осіб, підрозділів, служб органів внутрішніх справ з охорони громадського порядку та боротьби зі злочинністю криміналістичних знань, втілених в уміння працівників використовувати наукові, методичні, техніко-криміналістичні засоби і технології їх застосування з метою попередження, розкриття і розслідування злочинів [120, с. 62–64].

Як слідує з аналізу наведеного визначення поняття «криміналістичне забезпечення», в його складі присутній такий елемент як «техніко-криміналістичні засоби та технології», що може свідчити про віднесення до його складу діяльності із техніко-криміналістичного забезпечення. На думку Д.О. Карпенко, при вирішенні питання щодо різновидів криміналістичного забезпечення, зокрема щодо віднесення до них техніко-криміналістичного забезпечення, слід керуватися положеннями щодо структури криміналістики взагалі [55, с. 135].

У цьому контексті вірною здається позиція К.Є. Поджаренко, яку вона відстоює в дослідженні, присвяченому особливостям криміналістичного забезпечення розкриття та розслідування злочинних порушень прав інтелектуальної власності. На думку вченої, система криміналістичного забезпечення розкриття й розслідування злочинних порушень прав інтелектуальної власності відповідає його змісту як дворівневому виду діяльності, яка має загальні й спеціальні завдання. Вчена наголошує на тому, що з формально-структурних позицій, систему криміналістичного забезпечення розкриття і розслідування злочинних порушень прав інтелектуальної власності

можна представити відповідно до системи криміналістики: 1) теоретичні основи криміналістичного забезпечення; 2) техніко-криміналістичне забезпечення; 3) тактико-криміналістичне забезпечення; 4) методико-криміналістичне забезпечення [121, с. 151–152].

Власне тому, техніко-криміналістичне забезпечення досудового розслідування необхідно розглядати як складову частину або ж різновид криміналістичного забезпечення взагалі.

На переконання Г.І. Грамовича, техніко-криміналістичне забезпечення має два аспекти. У широкому значенні це регламентована певними нормативними актами діяльність науково-дослідних, судово-експертних та інших установ і відповідних посадових осіб, на яких покладений обов'язок розроблення та реалізації комплексу взаємопов'язаних заходів з метою створення оптимальних умов ефективного застосування спеціальних знань і науково-технічних засобів у боротьбі зі злочинністю. У вузькому значенні це комплекти науково-технічних засобів, якими повинні забезпечуватися конкретні учасники правоохоронної діяльності відповідно до їхньої компетенції, і комплекс знань, умінь та навичок, якими ці учасники повинні володіти, щоб застосовувати ці засоби [36, с. 191]. Цей підхід ілюструє інше поширене в науці розуміння техніко-криміналістичного забезпечення як сфери практичної діяльності та сукупності технічних засобів, що застосовуються в цій діяльності.

Крім того, І. В. Гора також наголошує на тому, що техніко-криміналістичне забезпечення розкриття й розслідування злочинів доцільно розглядати як у широкому логічному, так і у вузькому розумінні. При цьому, в широкому розумінні техніко-криміналістичне забезпечення – це система взаємоузгоджених науково-дослідних, організаційних, інформаційних, матеріально-технічних й інших заходів у межах функцій суб'єктів такої діяльності, визначених чинним законодавством, спрямованих на попередження, виявлення, припинення та розкриття злочинів [35, с. 121]. Навряд чи наведений підхід можна вважати широким розумінням техніко-криміналістичного забезпечення відповідної діяльності, оскільки відповідно до нього таке забезпечення обмежується лише

вчиненням уповноваженими суб'єктами ряду заходів. Більш того, намагаючись назвати окремі з таких заходів, за допомогою яких здійснюється техніко-криміналістичне забезпечення, учений використовує конструкцію «інші заходи», що вказує на невичерпність переліку, а тому ставить під сумнів доцільність наведення під час розкриття змісту досліджуваного явища окремих із них. У даному випадку задля полегшення сприйняття дефініції «техніко-криміналістичне забезпечення» можна було б обмежитися вказівкою на те, що таке забезпечення здійснюється за допомогою ряду заходів, вказавши при цьому, що підстави та порядок їх здійснення встановлені на нормативно-правовому рівні. Проте, в будь-якому разі, наведену дефініцію, з огляду на її обмеженість не можна сприймати як широке розуміння техніко-криміналістичного забезпечення [35, с. 120].

Разом з тим, широке розуміння досліджуваного поняття наводить і Т. Нішніанідзе під час визначення сутності техніко-криміналістичного забезпечення розкриття й розслідування сексуальних вбивств [175, с. 89]. На переконання науковця, техніко-криміналістичне забезпечення в широкому розумінні становить регламентовану певними нормативними актами діяльність науково-дослідних, судово-експертних та інших установ, а також відповідних посадових осіб, на яких покладений обов'язок щодо розроблення та реалізації комплексу взаємозалежних заходів для створення оптимальних умов ефективного застосування спеціальних знань і науково-технічних засобів у боротьбі зі злочинністю [105, с. 28]. Наведене визначення сутності техніко-криміналістичного забезпечення є більш вдалим, оскільки в ньому підкреслюється, що така діяльність є нормативно врегульованою. Проте, сутність техніко-криміналістичне забезпечення розкривається також через вчинення уповноваженими суб'єктами ряду заходів, а наприклад, про оснащення їх відповідними технічними засобами мова не йде. Зокрема, навіть якщо суб'єкти, які уповноважені здійснювати техніко-криміналістичне забезпечення досудового розслідування, будуть володіти всіма необхідними навичками використання техніко-криміналістичних засобів, будуть наділені високим рівнем знань у цій сфері, без надання їм відповідних технічних засобів їхні знання не будуть мати

сенсу на практиці. А тому під час визначення сутності техніко-криміналістичного забезпечення досудового розслідування необхідно враховувати цей аспект.

У свою чергу, наведені вище вчені у вузькому розумінні техніко-криміналістичне забезпечення відповідної діяльності розглядають як: створення умов для підвищення ефективності контррозвідувальної, оперативно-розшукової та слідчої діяльності шляхом розробки та впровадження техніко-криміналістичних методів й засобів збирання та дослідження матеріальних носіїв доказової інформації; комплекс науково-технічних засобів, якими повинні забезпечуватися конкретні учасники правоохоронної діяльності відповідно до їх компетенції, комплексу знань, умінь і навичок [105, с. 28; 175, с. 103]. І хоча такі підходи розглядаються зазначеними вченими як вузькі по відношенню до вищенаведених, аналіз їх змісту свідчить, що вони є більш розширеними оскільки включають в себе більше складових: мету такої діяльності (підвищення ефективності); що така діяльність, пов’язана із впровадженням відповідних техніко-криміналістичних методів і засобів, забезпечення ними уповноважених суб’єктів; формування в суб’єктів необхідних знань, умінь і навичок тощо. На думку Д. О. Карпенко такий підхід видається більш вдалим [55, с. 48].

Отже, ґрунтуючись на зазначеному вище, під техніко-криміналістичним забезпеченням розслідування кримінальних правопорушень пропонуємо розуміти багаторівневу складну систему створення умов для функціонування суб’єктів правоохоронної діяльності у сфері розкриття кримінальних правопорушень шляхом застосування комплексу науково-теоретичних, кримінально-процесуальних положень і техніко-криміналістичних засобів а також методик та технологій їх застосування [170].

Також, як нам видається, необхідно вказати на те, що широкий підхід щодо розуміння сутності техніко-криміналістичного забезпечення відрізняється від вузького тим, що в першому випадку розкривається або ж перелік суб’єктів, на яких законом покладено обов’язок здійснювати таку діяльність, або ж конкретні заходи, що вчиняються задля досягнення мети такої діяльності, або ж взагалі види діяльності, ефективне здійснення якої вимагає такого забезпечення. У такому

випадку, на нашу думку, визначення досліджуваного явища стає занадто громіздким, що ускладнює його розуміння [55, с. 49]. При цьому все одно не називаються якісь вичерпні переліки тих суб'єктів, заходів або видів діяльності, що свідчить про недоцільність використання такого підходу. Більш того, наявність широкого та вузького підходів до розуміння юридичної природи одного і того ж самого явища, в тому числі техніко-криміналістичного забезпечення, ускладнює й без того складну специфіку його використання в практичній діяльності, породжує непорозуміння в суб'єктів відповідних правовідносин щодо сутності його юридичної природи й у цілому не сприяє встановленню єдності понятійного апарату.

Як зазначалося вище, сутність криміналістичного забезпечення найчастіше розкривають через діяльність зі створення належних умов. Такі підходи зустрічаються й під час розкриття сутності техніко-криміналістичного забезпечення. Зокрема, на думку В.А. Сас, яку він висловлює в дослідженні, що присвячено висвітленню особливостей організації та тактики слідчих дій при розслідуванні злочинів, вчинених засудженими до позбавлення волі, техніко-криміналістичне забезпечення досудового розслідування полягає в створенні належних умов для застосування в розслідуванні злочинів традиційних і новітніх криміналістичних засобів і методів, зокрема судової фотографії, звуко- та відеозапису, трасології, балістики, дослідження документів, дослідження людини за зовнішніми ознаками, криміналістичних обліків тощо [153, с. 99].

На переконання Д.О. Карпенко, визначення сутності техніко-криміналістичного забезпечення через конструкцію «створення належних умов», здебільшого пов'язане із семантичним сенсом слова «забезпечення» [55, с. 50]. До прикладу, авторський колектив великого тлумачного словника сучасної української мови, зазначив, що «забезпечення» слід використовувати як: матеріальні засоби до існування; сукупність математичних, програмних, мікропрограмних, апаратурних засобів, спрямованих на автоматичну обробку даних за допомогою цифрових обчислювальних машин і пристроїв; а також дію за значенням «забезпечувати», тобто: постачаючи щось у достатній кількості,

задовольняти кого-, що-небудь у якихось потребах; надавати кому-небудь достатні матеріальні засоби до існування; створювати надійні умови для здійснення чого-небудь; гарантувати щось; захищати, охороняти кого-; що-небудь від небезпеки [25, с. 375]. Із наведеного слідує, що техніко-криміналістичне забезпечення є тією умовою, за допомогою належного виконання якої може бути досягнуто кінцеву мету досудового розслідування.

На нашу думку, мета техніко-криміналістичного забезпечення в якійсь мірі буде співпадати із метою досудового розслідування, адже вони співвідносяться як загальне та його складова частина. Це обумовлено тим, що в рамках проведення досудового розслідування виконуються багато різноманітних видів діяльності, у тому числі його техніко-криміналістичне забезпечення.

Утім, й техніко-криміналістичне забезпечення як цілеспрямована діяльність має власну мету. Зокрема, мета техніко-криміналістичного забезпечення є складовою змісту такої діяльності. Так, у змісті техніко-криміналістичного забезпечення виокремлюють такі структурні елементи: цілі використання криміналістичних засобів і методів, конкретні напрями криміналістичного забезпечення та способи отримання необхідної інформації для досягнення мети у межах конкретного напряму. При цьому до числа цілей техніко-криміналістичного забезпечення відносять: виявлення, отримання, фіксацію, вилучення, збереження носіїв криміналістичної (оперативно значущої) інформації; діагностику (розпізнавання – встановлення певних характеристик осіб та матеріальних об’єктів); ідентифікацію – встановлення тотожності особи або матеріального об’єкта за проявами загальної родової (групової) належності порівнюваних матеріальних об’єктів; визначення ситуації (явища, події або дії осіб) за залишеними матеріальними відображеннями; відтворення матеріальних об’єктів у їх первісному стані шляхом реконструкції (уявного образу) або реставрації (фізичного відтворення); профілактику; криміналістичну класифікацію (систематизація даних про осіб та матеріальні об’єкти у відповідних криміналістичних інформаційних системах з метою отримання оперативно-значущої й доказової інформації) [35, с. 122–123].

Беручи до уваги розглянуті положення, необхідно наголосити, що в них увага акцентується лише на окремих напрямках техніко-криміналістичного забезпечення, реалізація яких і направлена на досягнення кінцевої мети такої діяльності. Знову ж таки серед названих вище напрямків відсутні ті, що стосуються оснащення суб'єктів техніко-криміналістичного забезпечення відповідними технічними засобами (приладами, пристроями тощо), які необхідні їм задля вирішення поставлених перед ними завдань, досягнення мети своєї діяльності. Скоріш за все мова йде про завдання техніко-криміналістичного забезпечення, які тісно взаємопов'язані з метою такої діяльності. Зокрема, встановлюючи особливості неізоляційних запобіжних заходів в кримінальному процесі А. В. Захарко звертає увагу на той факт, що мета представляє собою те, до чого прямують, що потрібно здійснити, інакше кажучи, результати, які очікуються, на досягнення яких направлені дії. А під завданням розуміють мету, досягнення якої бажано до визначеного моменту часу. Виходячи з прийнятого в філософії розподілу мети на найближчу та перспективну, можна сказати, що завдання – це найближча мета, а мета – це кінцеве завдання [48, с. 38].

Поряд з цим, як цілком слушно відмічає В.С. Бондар під час розв'язання проблем теорії та практики використання спеціальних криміналістичних знань в розслідуванні крадіжок з проникненням у житло, оптимальне техніко-криміналістичне забезпечення проведення експертних досліджень, підготовка об'єктів для перевірки за криміналістичними обліками, також вимагає кваліфікованого знання їх методик, суворого дотримання правил підготовки початкових матеріалів. Це свідчить про необхідність залучення слідчими до проведення слідчих дій, з метою збирання речових доказів, спеціалістів, компетентних в області застосування криміналістичної техніки [16, с. 39].

Власне тому, завдання техніко-криміналістичного забезпечення полягають не тільки у вчиненні дій (фіксація, збирання, виявлення) уповноваженими суб'єктами, а й залучення ними до такої діяльності в разі необхідності інших осіб, які мають більш поглибленні знання в певній галузі, вміння та навички їх практичного використання, а також компетенцію щодо процесуального

оформлення результатів таких дій. При цьому, дивлячись на значну кількість суб'єктів техніко-криміналістичного забезпечення, першорядність їх ролі в такій діяльності, питання, пов'язані зі встановленням їх сутності та характеристикою окремих з них, будуть розглянуті нами в рамках окремого підрозділу представленого наукового дослідження [55, с. 52].

Видається за доцільне зазначити, що окремою складовою частиною техніко-криміналістичного забезпечення досудового розслідування є технічний супровід розслідування окремих видів злочинів. У зв'язку з цим в криміналістичній літературі все частіше можна побачити намагання визначити поняття техніко-криміналістичного забезпечення розслідування окремих видів злочинів [116, с. 223–224].

На переконання Д.Ю. Стригуна, під техніко-криміналістичним забезпеченням розкриття та розслідування контрабанди наркотичних засобів слід розуміти організаційно-функціональну систему, спрямовану на створення умов постійної готовності правоохоронних органів до швидкого та ефективного вирішення техніко-криміналістичних функцій і на практичну реалізацію цих умов з метою отримання, накопичення, обробки та забезпечення доказового значення криміналістично значущої інформації та її використання у процесі розкриття і розслідування контрабанди наркотичних засобів [159, с. 3–4].

Натомість, Б.О. Павлишин розглядає техніко-криміналістичне забезпечення протидії злочинам проти життя і здоров'я особи як систему правових, наукових, організаційних та дидактичних заходів з розробки, впровадження і практичного застосування техніко-криміналістичних засобів та наукових методів оперативними службами, органами досудового слідства, експертно-криміналістичними підрозділами для найбільш ефективного вирішення цілей і завдань, що стоять перед ними [107, с. 121].

Видається, що вказані погляди формально мають право на існування, але фактично підтримують або дублюють одне з раніше сформульованих визначень понять техніко-криміналістичного забезпечення розслідування злочинів, тільки з уточненнями стосовно певного виду злочину та/або суб'єкта

застосування [116, с. 221]. Відтак, у криміналістичній літературі поряд із техніко-криміналістичним забезпеченням можна побачити термін «техніко-криміналістичний супровід». Це поняття охоплює практичну реалізацію повсякденної готовності правоохоронних органів до застосування науково-технічних засобів і методів у кожному конкретному випадку розкриття та розслідування злочинів. Їх техніко-криміналістичний супровід здійснюється в організаційних і процесуальних формах використання спеціальних знань у процесі оперативно-розшукової та слідчої роботи [99, с. 32; 41, с. 253].

Крім того, для усунення суперечностей, дублювання та плутанини у понятійному апараті необхідно розглянути співвідношення понять «техніко-криміналістичне забезпечення» і «техніко-криміналістичний супровід», виходячи із семантичного аналізу вказаних термінів. Загалом вказані слова мають широкий смисловий спектр. «Забезпечення» розуміється як процес дії, як матеріальні засоби, що забезпечують можливість жити, існувати, і як те, що служить гарантією, забезпечує збереження або виконання чого-небудь. Забезпечити означає поставляти щось у достатній кількості, задовольняти кого-, що-небудь у якихось потребах, надавати кому-небудь достатні матеріальні засоби, створювати надійні умови для здійснення чого-небудь, гарантувати щось [24, с. 375]. Тлумачення підкреслює неоднозначність терміна: з одного боку, це процес, дія, а з іншого – це самі матеріальні засоби, але в обох випадках термін «забезпечити» має завершене в часі і просторі смислове навантаження [116, с. 223–224].

Значення терміна «супровід» дещо відрізняється. Під супроводом розуміється процес і те, що супроводжує яке-небудь явище, дію [24, с. 1415]. Супроводжувати означає слідувати разом із ким-небудь в якості супутника, йдучи за ким-небудь, виражати як-небудь своє відношення, відбуватися, здійснюватися, мати місце одночасно з чим-небудь, услід за чим-небудь і додавати до чого-небудь, доповнювати чим-небудь [157, с. 850]. Вказане дозволяє говорити про те, що супровід не є, як забезпечення, обмеженим просторово-часовими рамками процесом, дозволяючи одночасно з ним, після здійснення його виконувати потрібні дії, а також доповнювати його. З огляду на семантичний аналіз, супровід

не може початися без самого процесу дії, тобто забезпечення, а забезпечення може здійснитися і без супроводу. З цього можна зробити висновок про те, що супровід є динамічним доповненням забезпечення, тобто його елементом [116, с. 224].

На переконання С. Перліна, стосовно розслідування окремих видів і груп злочинів доцільніше користуватись поняттям техніко-криміналістичного супроводу як більш вузьким порівняно із забезпеченням, тобто складовою частиною, різновидом останнього [116, с. 224–225]. У свою чергу, щодо проведення окремих слідчих (розшукових) дій пропонуємо вести мову про техніко-криміналістичне сприяння. На нашу думку, термін «сприяння» більш точно визначає діяльність спеціаліста під час проведення окремих слідчих (розшукових) дій. Така думка базується, по-перше, на значенні цього терміна як створення відповідних умов для здійснення, виконання і т. ін. чого-небудь [24, с. 1377]; по-друге, на положеннях Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події, згідно з якою спеціалісти залучаються для надання безпосередньої технічної допомоги; по-третє, на тому, що термін «сприяти» означає подавати допомогу [24, с. 1377].

Продовжуючи дослідження в даному напряму, необхідно наголосити, що Д. О. Карпенко доречно підкреслює, що в наведених випадках, визначаючи як сутність, так і окремі змістовні складові техніко-криміналістичного забезпечення відповідної діяльності, вчені майже не звертають увагу на те, що вона не може бути здійснена поза належним оснащенням її суб’єктів відповідними техніко-криміналістичними засобами. А тому поділяємо позицію Р.Б. Єзерського, яку він відстоює під час дослідження криміналістичної техніки та її ролі в розкритті й розслідуванні злочинів [45, с. 128]. Власне, автор акцентує увагу, що мета техніко-криміналістичного забезпечення розкриття та розслідування злочинів здійснюється у напрямах забезпечення постійної готовності служб і підрозділів органів досудового розслідування, їх оснащення криміналістичними засобами і

методами, рівня техніко-криміналістичної підготовки співробітників, організації їх діяльності, який відповідає вимогам швидкого і ефективного застосування можливостей криміналістичної науки і техніки в процесі розкриття і розслідування злочинів, та практичної реалізації умов постійної готовності, що по суті, є повсякденною діяльністю слідчих, спеціалістів-криміналістів, працівників органів дізнання, яка пов'язана із застосуванням техніко-криміналістичних засобів та методів в загальному процесі розкриття і розслідування злочинів [45, с. 11]. Видається, що в наведеному вище випадку дуже вдало підкреслено, що техніко-криміналістичне забезпечення має на меті не лише формування практичних навичок використання криміналістичної техніки уповноваженими суб'єктами, а й їх оснащення відповідними криміналістичними засобами.

Поряд з цим, аналіз наукових джерел свідчить, що про таку складову техніко-криміналістичного забезпечення науковці часто не згадують під час визначення сутності даного правового явища, що, на нашу думку, не в повній мірі розкриває сутність такої діяльності.

Так, наприклад, Р.Б. Єзерський визначає сутність техніко-криміналістичного забезпечення розкриття та розслідування злочинів як організаційно-функціональну систему, спрямовану на створення умов постійної готовності служб і підрозділів органів досудового розслідування до швидкого та ефективного вирішення завдань щодо отримання, накопичення й опрацювання криміналістично-значущої (доказової, пошукової та тактично-орієнтуючої) інформації та ефективного її використання в процесі розкриття й розслідування злочинів [45, с. 11]. Для суб'єктів техніко-криміналістичного забезпечення також характерна організаційна та виконавча діяльність, оскільки вона направлена на досягнення двоєдиної мети (створення умов постійної готовності і їх практична реалізація у кожному конкретному випадку розкриття злочинів) [45, с. 12].

Убачається, що під «створенням умов постійної готовності» можна розуміти й ті, що пов'язані із наданням відповідним суб'єктам усіх необхідних їм для досягнення мети техніко-криміналістичного забезпечення засобів. Однак, як нам

видається, під час розкриття сутності досліджуваного явища все ж таки необхідно було більш детально акцентувати увагу на цьому аспекті.

Зокрема, як цілком слушно відмічає О.Ю. Пілюков у дослідженні особливостей використання інформаційних систем в експертних підрозділах Міністерства внутрішніх справ України, особливість криміналістичних знань полягає в тому, що їх значна частина реалізується на практиці лише із застосуванням певних технічних засобів [119, с. 173]. Відповідно як змістовну складову техніко-криміналістичного забезпечення досудового розслідування слід розглядати й оснащення суб'єктів такої діяльності техніко-криміналістичними засобами.

Також необхідно зазначити, що важливою структурною складовою правовідносин, які виникають у зв'язку із здійсненням техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, є їх суб'єктний склад.

Саме завдяки діяльності суб'єктів таких правовідносин, від ефективності практичної реалізації ними знань, умінь та навичок використання техніко-криміналістичних засобів здебільш залежить ефективність досудового розслідування даної категорії злочинів, поставлення законного й обґрунтованого рішення в проведеному кримінальному проваджені. А тому окрему увагу слід приділити встановленню сутності суб'єктів техніко-криміналістичного забезпечення досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та визначенню особливостей правового статусу окремих з них.

Так, вирішення поставленого вище наукового завдання видається неможливим без з'ясування сутності такої категорії як «суб'єкт». Сьогодні ж в юриспруденції категорію «суб'єкт» здебільшого використовують у двох випадках – для позначення «суб'єкта права» або ж «суб'єкта правовідносин». При цьому, деякі вчені вважають що зміст вищенаведених категорій збігається, тобто вони є

синонімічними поняттями, використовуються для позначення одного й того ж самого явища. Зокрема, авторський колектив сучасної правової енциклопедії вважає, що суб'єкт права – це фізична або юридична особа, поведінка якої регулюється нормами права за наявності в них ознак правоздатності та дієздатності. Учені стверджують, що суб'єкт права виступає необхідним елементом правовідносин [162, с. 336].

У наведеному випадку сутність суб'єкта права розкривається з позиції віднесення його до структури правовідносин, тобто фактично мова йде про категорію «суб'єкт правовідносин». На переконання Д.О. Карпенка, така позиція, потребує деяких уточнень. Зокрема, видається вдалою позиція тих учених-правознавців, які вважають, що суб'єкт права та суб'єкт правовідносин не є однаковими, рівнозначними категоріями. Таке розуміння даних понять має важливе методологічне значення як для встановлення сутності суб'єктів техніко-криміналістичного забезпечення досудового розслідування дорожньо-транспортних пригод, так і для здійснення характеристики правового статусу окремих з них [55, с. 136].

Суб'єктом права є лише перспективний суб'єкт правовідносин. У цьому контексті вдалою є позиція Л.І. Миськів, на думку якої, суб'єкти права та суб'єкти правовідносин є різними категоріями. Під суб'єктом права слід розглядати носія передбачених правовими нормами суб'єктивних прав та обов'язків, що має потенційну можливість участі в правовідносинах, тоді як суб'єкт правовідносин – це реальний учасник правовідносин [97, с. 114]. Суб'єкти права виступають як особи, що мають правосуб'єктність і в конкретному випадку може й не бути учасником правовідносин. Він має лише потенційну можливість вступати в правовідносини, для чого він наділяється об'єктивним правом відповідною правосуб'єктністю [97, с. 111]. О.І. Харитонова зауважує, що на відміну від суб'єкта (об'єктивного) права суб'єкт правовідносин – це фактичний (або такий, що моделюється) учасник правових зв'язків. У конкретному випадку суб'єкт права може і не бути учасником правовідносин, але учасник правовідносин обов'язково є суб'єктом права [181, с. 101].

Відтак, під такими суб'єктами пропонується розуміти осіб, які реалізують свої повноваження на підставі чинного національного законодавства, використовуючи техніко-криміналістичні засоби задля здійснення техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Таким чином, визначивши понятійний апарат, що буде використовуватися в представленому дослідженні, здається можливим перейти до характеристики правового статусу окремих суб'єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Так, одним із провідних суб'єктів досліджуваних правовідносин виступають органи та підрозділи Національної поліції. Правові засади організації та діяльності Національної поліції України, статус поліцейських, а також порядок проходження служби в Національній поліції визначено на рівні Закону України «Про Національну поліцію» від 2 липня 2015 року. Відповідно, Національна поліція України – це центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку. У контексті досліджуваного питання увагу слід звернути на окремі з повноважень поліції, перелік яких міститься в ст. 23 Закону: здійснює своєчасне реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події; здійснює досудове розслідування кримінальних правопорушень у межах визначеної підслідності; розшукує осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від виконання кримінального покарання, пропали безвісти, та інших осіб у випадках, визначених законом тощо [134].

У складі Національної поліції України функціонують такі суб'єкти техніко-криміналістичного забезпечення досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та

комп'ютерних мереж і мереж електрозв'язку як органи досудового розслідування. Правовий статус вищенаведених суб'єктів визначено в наказі МВС України «Про організацію діяльності органів досудового розслідування Національної поліції України» від 6 липня 2017 року № 570, що затверджує Положення «Про органи досудового розслідування» [135]. Відповідно до п. 1 вищенаведеного нормативно-правового акта органи досудового розслідування є структурними підрозділами апарату центрального органу управління поліції, її територіальних органів – головних управлінь Національної поліції в Автономній Республіці Крим та місті Севастополі, областях та місті Києві, територіальних (відокремлених) підрозділів головних управлінь Національної поліції в Автономній Республіці Крим та місті Севастополі, областях та місті Києві, які згідно з кримінальним процесуальним законодавством є органами досудового розслідування, які забезпечують досудове розслідування кримінальних правопорушень, віднесених до підслідності слідчих органів Національної поліції [135].

Звичайно, в контексті досліджуваного питання інтерес для нас представляє не сам орган досудового розслідування, а окремі його співробітники, які виступають суб'єктами техніко-криміналістичного забезпечення досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Власне серед таких осіб, в першу чергу, слід назвати слідчого. Відповідно до наказу № 570 слідчим є службова особа органу Національної поліції, уповноважена в межах КПК України, здійснювати досудове розслідування кримінальних правопорушень [135]. При цьому відповідно до ст. 40 КПК України слідчий як сторона обвинувачення наділений наступними повноваженнями: починати досудове розслідування за наявності підстав, передбачених КПК України; проводити слідчі (розшукові) дії та негласні слідчі (розшукові) дії у випадках, встановлених КПК України; доручати проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій відповідним оперативним підрозділам; звертатися за погодженням із прокурором до слідчого судді з клопотаннями про застосування заходів забезпечення кримінального провадження, проведення

слідчих (розшукових) дій і негласних слідчих (розшукових) дій; повідомляти за погодженням із прокурором особі про підозру; за результатами розслідування складати обвинувальний акт, клопотання про застосування примусових заходів медичного або виховного характеру та подавати їх прокурору на затвердження; приймати процесуальні рішення у випадках, передбачених КПК України, у тому числі щодо закриття кримінального провадження; здійснювати інші повноваження, передбачені КПК України [81].

Не менш важливим суб'єктом техніко-криміналістичного забезпечення досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, є дізнавач. Так, наприклад, у Положенні про організацію діяльності підрозділів дізнання органів Національної поліції України, затвердженого наказом МВС України від 20 травня 2020 № 405, зазначено, що на підрозділи дізнання покладаються такі завдання: захист особи, суспільства та держави від кримінальних проступків; охорона прав, свобод та законних інтересів учасників кримінального провадження; забезпечення швидкого, повного та неупередженого розслідування кримінальних проступків, віднесених до підслідності органів Національної поліції України; забезпечення відшкодування фізичним і юридичним особам шкоди, заподіяної кримінальними проступками; виявлення причин і умов, які сприяють учиненню кримінальних проступків, і вжиття заходів щодо їх усунення [132].

Поряд з цим, відповідно до положення Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, що затверджено наказом МВС України від 7 липня 2017 року № 575, слідчий очолює слідчо-оперативну групу (далі – СОГ) [126]. Так, на місці події слідчий (дізнавач): керує діями інших членів СОГ та відповідає за якість проведення огляду місця події; разом з іншими членами СОГ, залученими спеціалістами, запрошеними потерпілими, свідками та іншими учасниками кримінального провадження в установленому КПК України порядку

фіксує відомості щодо обставин учинення кримінального правопорушення; вилучає речі і документи, які мають значення для кримінального провадження, та речі, вилучені з обігу, у тому числі матеріальні об'єкти, придатні для з'ясування обставин, що підлягають доказуванню, забезпечує в установленому порядку їх належне зберігання для подальшого направлення для проведення судової експертизи; має право заборонити будь-якій особі перебувати на місці огляду або залишати його до закінчення огляду та вчиняти будь-які дії, що заважають проведенню огляду; за наявності підстав інформує уповноваженого працівника чергової частини про залучення додаткових сил і засобів для фіксування всіх обставин учиненого кримінального правопорушення; за необхідності після початку кримінального провадження допитує про обставини вчиненого кримінального правопорушення заявника, потерпілого, свідків та інших учасників кримінального провадження; надає письмові доручення працівникам оперативних підрозділів про проведення слідчих (розшукових) дій у кримінальному провадженні [126]. Із наведеного слідує, що слідчий (дізнавач) здійснюють техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку із початку такого розслідування до його логічного завершення та є постійними, незмінними суб'єктами такої діяльності.

Окремої уваги заслуговує такий суб'єкт техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є як інспектор-криміналіст (технік-криміналіст). На місці події: надає консультації слідчому (дізнавачу) з питань, що потребують відповідних спеціальних знань і навичок; з використанням спеціальних знань та навичок, науково-технічних засобів і спеціального обладнання проводить вимірювання, фотографування, звуко- чи відеозапис, складає плани і схеми, виготовляє графічні зображення оглянутого місця чи окремих речей; виявляє, фіксує, здійснює вилучення та пакування матеріальних об'єктів, які несуть на собі слідову

інформацію вчиненого правопорушення; проводить експрес-аналіз за зовнішніми характеристиками вилучених об’єктів (без надання письмового висновку), звертає увагу слідчого на фактичні дані, що мають значення для розслідування обставин кримінального правопорушення; відповідає за якісну фіксацію всієї слідової інформації, повноту відображених про це даних у протоколі огляду та схемі (плані) до нього [126]. Процесуальний статус такого суб’єкта визначено в ст. 71 КПК України, відповідно до якої спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками застосування технічних або інших засобів і може надавати консультації під час досудового розслідування та судового розгляду з питань, що потребують відповідних спеціальних знань і навичок. При цьому спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень, відбір зразків для проведення експертизи тощо) сторонами кримінального провадження під час досудового розслідування і судом під час судового розгляду [81]. Отже, можна стверджувати, що ще одним суб’єктом техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку виступає спеціаліст.

Крім того, важливу роль у техніко-криміналістичному забезпеченні розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку займають Дільничний офіцер поліції (поліцейський патрульної поліції) та кінолог. Так, на місці події завданнями Дільничного офіцера поліції є: до прибуття СОГ забезпечує охорону місця події, збереження слідів учиненого кримінального правопорушення та в разі необхідності організовує надання невідкладної медичної допомоги потерпілим особам; з’ясовує обставини вчиненого кримінального правопорушення, установлює свідків, очевидців події, прикмети правопорушників, збирає інші відомості, що можуть бути використані як докази; інформує уповноваженого працівника чергової частини органу, підрозділу поліції про обставини вчинення кримінального правопорушення та осіб, які його

вчинили, для вжиття невідкладних заходів щодо їх затримання; з прибуттям СОГ негайно інформує слідчого (дізнавача) про одержані дані щодо обставин учинення кримінального правопорушення та осіб, які його вчинили, для їх подальшої фіксації шляхом проведення слідчих (розшукових) та негласних слідчих (розшукових) дій [126].

Кінолог на місці події: за узгодженням зі слідчим (дізнавачем) визначає межі огляду місця події і порядок його проведення з метою виявлення слідів і предметів, які мають значення для застосування службового собаки, на основі наявної інформації визначає доцільність його застосування; уживає заходів для розшуку та затримання особи, яка вчинила кримінальне правопорушення, шляхом застосування службового собаки по запахових слідах, речах і предметах, залишених на місці події, а також з метою пошуку слідів і предметів, які мають значення для розкриття і розслідування кримінального правопорушення; бере участь у блокуванні місця вчинення кримінального правопорушення, його огляді, виявленні, фіксації, вилученні і зберіганні предметів і слідів, які можуть бути використані для розшуку особи, яка вчинила кримінальне правопорушення, із застосуванням службового собаки; позначає місця виявлення на шляху слідування службового собаки предметів і речей, які можуть бути використані для пошуку особи, яка вчинила кримінальне правопорушення, із застосуванням службового собаки; доводить до відома керівника СОГ інформацію про можливе походження запаху носіїв (слідів, предметів), виявлених на місці події, та їх використання для розкриття та розслідування кримінального правопорушення; використовуючи отриману інформацію, застосовує службового собаку для розшуку особи, яка вчинила кримінальне правопорушення, за її запаховими слідами; обстежує за допомогою службового собаки прилеглу до місця події територію та можливі місця укриття особи, яка вчинила кримінальне правопорушення (горища і підвали прилеглих будівель, які не є житлом чи іншим володінням особи, незамкнені сховища, лісопаркові зони, кар’єри тощо); разом з іншими працівниками поліції бере участь у переслідуванні та затриманні осіб, які підозрюються у вчиненні кримінального правопорушення, застосовує при цьому службового собаку; за

відсутності можливостей застосування службового собаки або в разі втрати ним сліду діє за вказівкою керівника СОГ [126].

Убачається, що в якості суб'єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку також необїхідно розглядати оперативні підрозділи Національної поліції, які відповідно до ст. 41 КПК України здійснюють слідчі (розшукові) дії та негласні слідчі (розшукові) дії в кримінальному провадженні за письмовим дорученням слідчого [81]. Більш того, відповідно до наказу № 575 в разі залишення місця дорожньо-транспортної пригоди особою, яка його вчинила, на місце пригоди також направляються працівники уповноважених оперативних підрозділів територіального органу, підрозділу поліції та працівники відповідних оперативно-технічних підрозділів [126].

Наступним і одним із провідних суб'єктів техніко-криміналістичного забезпечення досудового розслідування виступає експерт. Відповідно до ст. 66 КПК України експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право на проведення експертизи й якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань [81]. Правовий статус експерта, а також питання, пов'язані з призначенням судових експертиз, врегульовано на рівні Закону України «Про судову експертизу» від 25 лютого 1994 року [137]. З аналізу положень даного нормативно-правового акта слідує, що судовими експертами можуть бути особи, які мають необхідні знання для надання висновку з досліджуваних питань. При цьому йдеться про два види судових експертів – судові експерти державних спеціалізованих установ та судові експерти, які не є працівниками таких установ. Судовими експертами державних спеціалізованих установ можуть бути фахівці, які мають відповідну вищу освіту, освітньо-кваліфікаційний рівень не нижче спеціаліста, пройшли відповідну підготовку й

отримали кваліфікацію судового експерта з певної спеціальності. У свою чергу, судові експерти, до проведення судових експертиз (обстежень і досліджень), крім тих, що проводяться виключно державними спеціалізованими установами, можуть залучатися також судові експерти, які не є працівниками цих установ, за умови, що вони мають відповідну вищу освіту, освітньо-кваліфікаційний рівень не нижче спеціаліста, пройшли відповідну підготовку в державних спеціалізованих установах Міністерства юстиції України, атестовані та отримали кваліфікацію судового експерта з певної спеціальності у порядку, передбаченому цим Законом [137]. Зазначимо, що експерт є важливим суб'єктом техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, оскільки тільки він вправі проводити відповідні експертизи й надавати висновки по ним, формуючи при цьому доказову базу.

Усі перераховані вище суб'єкти техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна визначити як індивідуальних, тобто таких, що характеризують статус конкретної особи (посадової, службової, працівника, співробітника тощо). Проте, можна говорити й про колективних суб'єктів техніко-криміналістичного забезпечення такого досудового розслідування. У даному випадку мова йде про колективи людей, які спільними зусиллями, вступаючи у відносини із взаємодії здійснюють діяльність із техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. А тому необхідно визначити й правовий статус даних суб'єктів.

Зокрема, Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, визначає особливості організації взаємодії при досудовому розслідуванні

кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів) [126].

Так, наприклад, досудове розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку здійснюється слідчими, які спеціалізуються на розслідуванні кримінальних правопорушень зазначеного виду [178, с. 113–114].

Матеріали оперативного підрозділу, у тому числі Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, що направляються до слідчого підрозділу для початку та здійснення досудового розслідування, мають містити: письмове пояснення заявника, в якому зафіксовані відомі заявнику дані про вчинення кримінального правопорушення з відповідними додатками, що містять відомості, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм), а також у разі наявності документи, що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби; установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку (логін і пароль для доступу до мережі Інтернет, IP-адреса, WEB-адреса, номер абонента мережі електрозв'язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо) [126].

Утворення СОГ за участю оперативних працівників Департаменту кіберполіції Національної поліції України, його структурних підрозділів, які діють за міжрегіональним принципом, для розслідування кримінальних правопорушень у сфері використання комп`ютерів, систем та комп`ютерних мереж і мереж електрозв`язку здійснюється за спільним наказом керівників органу досудового розслідування та Департаменту кіберполіції Національної

поліції України. Утворення СОГ у кримінальному провадженні, досудове розслідування у якому здійснюється Головним слідчим управлінням Національної поліції України, здійснюється за наказом Голови Національної поліції України або за наказом заступника Голови Національної поліції України – начальника Головного слідчого управління, погодженим керівництвом Департаменту кіберполіції Національної поліції України. Старшим СОГ є слідчий, якого керівником органу досудового розслідування визначено здійснювати досудове розслідування кримінального правопорушення [126].

Керівник Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, оперативний працівник якого включений до складу СОГ або за матеріалами якого розпочато кримінальне провадження, забезпечує взаємодію з органом досудового розслідування Національної поліції України, який здійснює розслідування кримінальних правопорушень зазначеної категорії [126].

Також, враховуючи те, що проведення експертизи може бути доручено як конкретному експерту, так і відповідній установі, останні також слід віднести до складу колективних суб'єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Так, у ст. 7 Закону України «Про судову експертизу встановлено», що судово-експертну діяльність здійснюють державні спеціалізовані установи, їх територіальні філії, експертні установи комунальної форми власності, а також судові експерти, які не є працівниками зазначених установ, та інші фахівці (експерти) з відповідних галузей знань у порядку та на умовах, визначених цим Законом. До державних спеціалізованих установ належать: науково-дослідні установи судових експертиз Міністерства юстиції України; науково-дослідні установи судових експертиз, судово-медичні та судово-психіатричні установи Міністерства охорони здоров'я України; експертні служби Міністерства внутрішніх справ України, Міністерства оборони України, Служби безпеки України та Державної прикордонної служби України. Виключно державними спеціалізованими установами здійснюється

судово-експертна діяльність, пов’язана з проведенням криміналістичних, судово-медичних і судово-психіатричних експертиз [126].

Окрім цього, в якості колективних суб’єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку необхідно розглядати й експертів у разі проведення ними комісійної або комплексної експертизи. У такому разі експерти діють не як індивідуальні, а як колективні суб’єкти правовідносин, так як вирішують поставлені перед ними завдання спільними зусиллями. Так, як слідує з аналізу Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, що затверджена наказом Мінюсту України від 8 жовтня 1998 року № 53/5 (далі – наказ 53/5) комісійною є експертиза, яка проводиться двома чи більшою кількістю експертів, що мають кваліфікацію судового експерта за однією експертною спеціалізацією (фахівцями в одній галузі знань) [129]. Комісія експертів може утворюватися органом (особою), який (яка) призначив(ла) експертизу (залучив(ла) експерта), або керівником експертної установи. У свою чергу, комплексною є експертиза, що проводиться із застосуванням спеціальних знань різних галузей науки, техніки або інших спеціальних знань (різних напрямів у межах однієї галузі знань) для вирішення одного спільного (інтеграційного) завдання (питання). До проведення таких експертиз у разі потреби залучаються як експерти експертних установ, так і фахівці установ та служб (підрозділів) інших центральних органів виконавчої влади або інші фахівці, що не працюють у державних спеціалізованих експертних установах [39].

Говорячи про суб’єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, доцільно звернутися до Положення про Департамент кіберполіції Національної поліції України, затвердженого наказом МВС України 10.11.2015 № 85 [130].

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який відповідно до законодавства України забезпечує реалізацію державної політики у галузі протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції. Департамент кіберполіції бере участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Департамент відповідно до покладених на нього завдань: визначає, розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням у галузі протидії кіберзлочинності; у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у галузі протидії кіберзлочинності; уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, у тому числі об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень; організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності; проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті; забезпечує в порядку, передбаченому законодавством України, формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності; організовує виконання, у межах компетенції, доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та

негласних слідчих (розшукових) дій у кримінальних провадженнях; у межах компетенції розробляє рекомендації для підвищення професійного рівня і поінформованості органів Національної поліції України, а також, громадськості про результати діяльності кіберполіції; вивчає позитивний вітчизняний і зарубіжний досвід боротьби з кримінальними правопорушеннями у сфері протидії кіберзлочинності та вносить пропозиції керівництву Національної поліції України щодо його впровадження; вносить в установленому порядку пропозиції щодо вдосконалення законодавства у сфері протидії кіберзлочинності, а також бере участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері; відповідно до чинного законодавства створює та забезпечує функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі; аналізує та систематизує дані про кримінальні правопорушення, вчинені у галузі протидії кіберзлочинності та з використанням високих технологій, що надходять від громадян каналами кол-центрів, електронними листами та терміналами зворотного зв'язку; відповідно до чинного законодавства збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінює результати за окремими показниками службової діяльності, надає, відповідно до законодавства України, звіти про результати роботи та відповідну інформацію керівництву Національної поліції України, МВС, органів державної влади з питань попередження та протидії кіберзлочинам [130].

1.3. Закордонний досвід техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Серед сучасних тенденцій розвитку суспільства варто зазначити глобальну інформатизацію практично всіх сфер життєдіяльності людини. Крім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Для підвищення ефективності боротьби з кіберзлочинністю Україна досить давно почала відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Верховною Радою України було зроблено спробу врегулювати відносини, що виникають у кіберпросторі, а саме ухвалено Закон України «Про основні засади забезпечення кібербезпеки в Україні». Незважаючи на ці кроки, Україна постійно стає жертвою кібератак, у зв'язку з чим питання протидії кіберзлочинності набуває особливої актуальності. Саме тому питання вивчення та запозичення міжнародного досвіду провідних країн світу у сфері державної діяльності щодо правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності, забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є недослідженим та потребує вивчення [92, с. 101–102].

Питання забезпечення кібербезпеки та протидії кіберзлочинності неодноразово ставали предметом наукових дискусій та досліджень. Так, зазначена проблематика знайшла своє відображення у працях таких вітчизняних вчених та науковців як: В.Б. Авер'янов, О.Ф. Андрійко, О.М. Бандурка, В.Ю. Баскаков, В.В. Береза, К.І. Бєляков, О.В. Бойченко, В.М. Бутузов, В.В. Василевич, В.П. Горбулін, С.М. Гусаров, І.В. Діордіца, Є.В. Додін, О. Ю. Дрозд, М.Г. Каращук, Н.В. Коваленко, Т.О. Коломоєць, В.К. Колпаков, А.Т. Комзюк, О.Є. Користін, В.І. Куріло, А.М. Лобода, В.А. Ліпкан, Ю.Є. Максименко, В.В. Марков, Л.В. Могілевський, О.М. Музичук, А.М. Новицький, О.П. Орлюк,

О.Ю. Салманова, Р.Ю. Сень, О.Ю. Синявська, Т.Л. Сироїд, В.С. Сідак, В.В. Сокуренко, В.О. Тімашов, В.В. Чернєй, В.В. Чумак, Д.В. Швець, О.В. Шепета та інші. Наразі недостатньо уваги приділено діяльності спеціалізованих державних в тому числі міжнародних органів та організацій у сфері протидії кіберзлочинності як сучасного виду злочинності в Україні та за кордоном. У зв'язку з чим активізуються питання щодо дослідження зарубіжного та міжнародного досвіду техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також на вжиття заходів з протидії кіберзлочинності та забезпечення кібербезпеки держави [164, с. 113].

Так, наприклад, Сполучені Штати Америки стали першою країною, що прийняли відповідний закон та створили Національну стратегію безпеки в кіберпросторі. Причиною написання цього документа стала терористична атака 11 вересня 2001 р. Стратегія була частиною більш загальної Стратегії забезпечення національної безпеки (National Strategy for Homeland Security). Крім того, за оцінками фахівців, саме в США щорічно втрати корпорацій від злочинності перевищують 200 млрд, а від комп'ютерних злочинів – 6 млрд дол., тому питання боротьби з кіберзлочинністю для цієї країни є надзвичайно актуальним [202, с. 57]. Поряд із США активна боротьба з кіберзлочинністю проводиться в країнах Європейського Союзу. В ЄС створений необхідний нормативно-правовий фундамент із питань захисту кіберпростору. Стратегія кібербезпеки ЄС була прийнята в 2013 р. Її особливістю є те, що стратегією були охоплені різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика [164, с. 114–115].

Більш того, водночас із Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС. Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є: свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі; застосування

законодавства ЄС у кіберпросторі в тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому суспільстві: від звичайних громадян до цілих держав; розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [98].

При цьому, особлива увага приділяється функціонуванню такого органу в США є Федеральне бюро розслідувань, що головним суб'єктом забезпечення кібербезпеки держави та протидії кіберзлочинності на всій території США. ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Оскільки кібер-вторгнення стають все більш поширеним явищем, сьогодні діяльність ФБР постійно удосконалюється, щоб краще протистояти терористичній загрозі після терактів 11 вересня 2001 року [61]. Поряд із цим, одним із пріоритетних напрямків протидії кіберзлочинності є протидія торгівлі людьми, що здійснюється із застосуванням інформаційних технологій у віртуальному просторі та завдає шкоди охоронюваним законом правам та основоположним свободам людини й громадянина [184, с. 310].

Крім того, при ФБР створено інтернет-центр скарг на кіберзлочини, місією якого є розгляд скарг на злочин в Інтернеті, надання громадськості надійний і зручний механізм звітності про підозрюваних, схеми шахрайства з використанням Інтернету і створення ефективних альянсів з правоохоронними органами та галузевими партнерами. Інформація аналізується і поширюється в слідчих і розвідувальних цілях серед співробітників правоохоронних органів і для інформування громадськості [61].

Також, слід зазначити, що окрім Команди критичного реагування Бюро по боротьбі з тероризмом, з метою протидії кіберзлочинності та тероризму в Бюро по боротьбі з тероризмом функціонують також такі групи: Об'єднана оперативна група з питань тероризму та кіберзлочинності; група забезпечення кібербезпеки Нижнього Манхеттена; та група з аналізу ризиків та загроз тероризму та кіберзлочинності. Кожна із зазначених груп виконує ряд своїх завдань та функцій,

що в кінцевому підсумку спрямовані на вжиття заходів з протидії кіберзлочинності та тероризму [13, с. 112–113].

Зокрема, Об’єднана оперативна група з питань тероризму та кіберзлочинності розслідує факти кіберзлочинності та тероризму, що вчиненні на території штату Нью-Йорк, а також здійснюють систематизацію вчинених злочинів та їх аналіз.

Група забезпечення кібербезпеки Нижнього Манхеттена призначена виявляти та попереджувати загрози кібератак та тероризму на території Нижнього Манхеттена.

Група з аналізу ризиків та загроз тероризму та кіберзлочинності здійснює заходи стратегічної розвідки щодо виявлення кібератак та загроз тероризму та веде їх аналіз.

Таким чином, при Департаменті поліції Нью-Йорка функціонує ряд поліцейських підрозділів, що здійснюють завдання протидії кіберзлочинності та тероризму.

В той же час, належний рівень функціонування поліцейських органів, що здійснюють заходи боротьби з кіберзлочинністю залежить від належного рівня їх нормативно-правового регулювання, що в США складає досить потужну базу для ефективної реалізації національної політики забезпечення кібебезпеки держави [13, с. 113].

Поряд з цим, з метою попередження вчинення кіберзлочинності, на офіційному сайті ФБР розміщені матеріали щодо захисту своїх персональних даних у віртуальному просторі. Зокрема, також є наявна інструкція захисту свого персонального комп’ютера від різних програм та шпигунського програмного забезпечення.

Убачається за доцільне також зазначити, що новелою у американському законодавстві у сфері кібербезпеки є затвердження програми ФБР щодо безпечного онлайн-серфінгу (FBI-SOS) – це загальнонаціональна ініціатива, покликана інформувати дітей 3-8 класів про кібернебезпеки, з якими вони стикаються в Інтернеті, і сприяти запобіганню злочинів проти дітей. Він просуває

кібер громатні ідей та положення серед студентів, залучаючи їх у веселу, відповідну віку, конкурентоспроможну онлайн-програму, де вони вчаться безпечного і відповідального використання Інтернету. Програма підкреслює важливість питань кібербезпеки, таких як захист паролем, розумні звички серфінгу та захист особистої інформації. Аналогічні програми існують у Латвії [186, с. 146]. Зазначена програма має вигляд яскравих картинок для конкретного віку дітей з інтерактивними іграми. Кожна гра передбачає проходження по черзі рівнів гри, що мають відповідну назву [13, с. 113].

Однак, кіберзагрози в США продовжують з'являтися майже кожного дня, для ФБР в області кримінальної та національної безпеки, вкрай важливо залучення державних і приватних партнерів щодо обміну інформацією поряд з правоохоронними та розвідувальними колами. Щоб залучити надійних галузевих партнерів в розвідувальну групу, ФБР спростило свою систему відстеження та управління погрозами Guardian з метою захищеного інформаційного порталу, що дозволяє окремим партнерам в галузі повідомляти про інциденти, пов'язані з кіберзлочинністю, в режимі реального часу. iGuardian надає приватним компаніям стандартизований спосіб повідомляти інформацію в ФБР, якщо вони стають жертвами комп'ютерних вторгнень. Портал iGuardian – це еволюція платформи, через яку правоохоронні партнери ФБР надають потенційні загрози тероризму і повідомлення про підозрілі дії. У той час як eGuardian залучає співробітників правоохоронних органів, iGuardian був розроблений спеціально для партнерів в критичних секторах телекомунікацій, оборони, банківської справи та фінансів, а також в області енергетичної інфраструктури і доступний через чутливу, але несекретну мережу InfraGard. InfraGard – це коаліція ФБР щодо захисту державної і приватної інфраструктури, в яку входять тисячі перевірених і націлених на галузь членів. Організація підтримує свою власну захищену мережу для поширення попереджень та бюлетенів ФБР і дозволяє обмінюватися інформацією про ключові загрози серед своїх членів. Використовуючи систему iGuardian, учасникам пропонується направляти інформацію про вторгнення безпосередньо в ФБР, в тому числі детальну інформацію про зараження шкідливим ПЗ, псування

веб-сайтів і атаках типу «відмова в обслуговуванні». Програма iGuardian також надає партнерів InfraGard доступ до інформації та відомостями, отриманими в результаті пов'язаних інцидентів [17, с. 136].

Резюмуючи викладене вище, зазначимо, в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі [13, с. 113–114].

Необхідно зазначити, що одним із важливих напрямків діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними злочинами, розслідуванням яких займається підрозділ Королівської канадської кінної поліції (федеральної поліції, КККП) з боротьби з комп'ютерною злочинністю, опираючись на дані канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами. Діяльність підрозділу направлена на розслідування та розкриття злочинів, пов'язаних із комп'ютерами і телекомунікаціями. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектора, дає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань злочинів, пов'язаних із комп'ютерними системами. Враховуючи, що інформаційна система дозволяє передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2500 точок доступу, до яких входять близько 1285 федеральних і провінційних поліцейських відділень. 1180 підрозділів спеціалізованих відділів КККП підключені до ліній системи [23, с. 134]. Безперечно, цей напрямок діяльності поліції є важливим, оскільки економічні втрати вже досягли широких масштабів, деякі злочинці діють на міжнародному рівні організованою групою. Водночас слід визнати, що канадське законодавство щодо визначення комп'ютерної злочинності потребує вдосконалення. Враховуючи, що завдання, які стоять перед підрозділами поліції з

боротьби з комп'ютерною злочинністю, носять міжнародний характер і не є специфічними для Канади, вони активно співпрацюють з іншими країнами та Інтерполом з метою вдосконалення законодавства у цьому напрямку [92, с. 102].

Розкриття комп'ютерних злочинів являє собою складне завдання, у першу чергу через фактор часу. Оскільки передача даних може бути виконана майже миттєво, часто буває даремно шукати будь-які докази, що підтверджують порушення міжнародного законодавства. За даними КККП, на сьогодні безліч комп'ютерних злочинів здійснюється дітьми, які не досягли дванадцятирічного віку. Згідно з кримінальним кодексом Канади для встановлення кримінальної відповідальності необхідно довести несанкціоноване використання комп'ютерної системи та намір особи заподіяти своїми діями шкоду. Такий підхід потребує чіткого встановлення параметрів доступу до комп'ютерної техніки з метою попередження порушень. Необхідно враховувати дані про осіб, параметри доступу з урахуванням обмежень, можливість службовців «експериментувати» з програмами. Кваліфіковану консультацію щодо можливої неправомірної поведінки в цьому напрямку може надати міністерство юстиції чи відповідний підрозділ КККП [92, с. 102–103].

Поряд з цим, слід зазначити, що методика розслідування випадків несанкціонованого дистанційного доступу до комп'ютерних мереж технічно складна, ними займаються спеціалізовані поліцейські підрозділи. З огляду на небезпеку комп'ютерної злочинності, тенденцію її розвитку та впливу на світове співтовариство у межах ООН регулярно проводяться симпозіуми з профілактики і припинення комп'ютерної злочинності. Як один із напрямків фахівці відзначають програмні методи захисту інформації в комп'ютерних системах колективного користування шляхом удосконалення системи автоматичного контролю. На попередження та зменшення злочинів щодо незаконного використання телекомунікаційних систем на міжпровінційному, державному і міжнародному рівних спрямовані дії та управління боротьби з економічними злочинами. Допомагає поліцейським підрозділам Інформаційний центр [92, с. 103].

Поліцейська діяльність щодо попередження та розкриття діянь, пов'язаних із кіберзлочинністю, спрямована і на різнобічний розвиток відносин з якомога більшим суспільним колом через засоби масової інформації, консультативні зустрічі з представниками громадськості, взаємовідносини з різноманітними органами влади і управління, громадськими організаціями, окремими громадянами. Таким чином, поліція є важливим партнером у співтоваристві відомств, що займаються боротьбою зі злочинністю, в тому числі кіберзлочинністю, забезпеченням дотримання прав людини, забезпеченням захисту федеральних державних комп'ютерних центрів, приватного сектора [23, с. 135]. Ефективна боротьба із комп'ютерною злочинністю вимагає більш дієвого та ефективно функціонуючого співробітництва правоохоронних органів різних країн, у тому числі в межах Інтерполу.

Поряд з США і Канадою активну боротьбу з кіберзлочинністю проводять в країнах Європейського Союзу. Так, в ЄС створений необхідний нормативно-правовий фундамент з питань захисту кіберпростору [117, с. 56]. Стратегія кібербезпеки ЄС була прийнята в 2013 році. Її особливістю є те, що стратегією були охоплені різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика. Разом із Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС [185, с. 152].

Так, наприклад, фахівці правоохоронних органів Франції виділяють дві форми даного виду злочинності. Одна з них – суспільно небезпечні діяння, пов'язані з незаконним тиражуванням комп'ютерного програмного забезпечення, незаконним втручанням до автоматизованих систем обробки даних, вторгненням на сайти, створенням та розповсюдженням шкідливих програм та інші. Друга форма кіберзлочинів – вважається більш розвинутою і динамічною, використовує глобальні інформаційні мережі. До неї відносять розповсюдження сайтів, пов'язаних з наступним контентом: дитячою порнографією; збутом наркотиків; расистською, ксенофобною або антисемітської спрямованістю; терористичного

толку; про замахи на приватне життя; з інструкціями з експлуатації вибухових речовин; повідомлень, реклами в шахрайських цілях [20, с. 240–241].

З огляду на сказане, міністром внутрішніх справ Франції Мішель Алліот-Марі 14 лютого 2008 року була оприлюднена французька Стратегія з питань боротьби з кіберзлочинністю. Мета Стратегії – співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) та правоохоронними органами з обміну інформацією та питаннях щодо об'єднання зусиль у боротьбі з кіберзлочинністю.

У 2015 році Франція прийняла Національну стратегію інформаційної безпеки. Вона спрямована на супровід переходу французького суспільства до цифрових технологій і на рішення нових завдань, пов'язаних зі зміною використання цифрових технологій і викликаними цим погрозами. У ній виділено п'ять напрямків роботи: забезпечення державного суверенітету – ефективне реагування на зловмисні дії в комп'ютерних системах і мережах; інформування широкої громадськості; перетворення інформаційної безпеки в конкурентну перевагу французьких підприємств; підвищення впливу Франції на міжнародній арені [14, с. 96–97].

Разом з тим, вказану стратегію доповнили: 1) Міжнародна стратегія Франції в області інформаційних технологій, була представлена міністром Європи і закордонних справ в грудні 2017 року. У ній узагальнені всі стратегічні цілі, які Франція підтримує в області інформаційних технологій в трьох основних сферах: управління, економіка і безпека; 2) Стратегічний огляд з питань кіберзахисту, що складений генеральним секретарем з питань оборони і національної безпеки за дорученням прем'єр-міністра, був представлений в лютому 2018 року. У ньому визначається доктрина управління кіберкрізісамі. Огляд також роз'яснює цілі національної стратегії в області кіберзахисту, підтверджує ефективність французької моделі і покладає основну відповідальність в цій галузі на державу [22, с. 316].

Слід також зазначити, що на технічному і оперативному рівні ефективності французької системи сприяє ряд учасників, зокрема:

- Французьке агентство безпеки інформаційних систем (ANSSI), створене в 2009 році, є національним органом, що відповідає за кібербезпека. Виступаючи у французькому кіберпросторі як «рятівника», ANSSI забезпечує запобігання (в тому числі з нормативно-правової точки зору) і реагування на інциденти в сфері IT, що зачіпають стратегічно важливі установи. Агентство також забезпечує відпрацювання управління в кризових ситуаціях на національному рівні;

- Міністерство збройних сил виконує подвійну місію по захисту мереж, що забезпечують його діяльність, і по інтеграції цифрового протидії в військові операції. З метою підтримки діяльності міністерства в цій сфері на початку 2017 року було створено штаб кіберзахисту (COMCYBER), переданий під командування начальника штабу збройних сил;

- Міністерство внутрішніх справ веде боротьбу з усіма формами кіберзлочинності, спрямованої як проти національних установ та інтересів, господарюючих суб'єктів і державних органів, так і проти фізичних осіб. З цією метою міністерство спирається на спеціалізовані центральні служби та територіальні мережі національної поліції, національної жандармерії і сил внутрішньої безпеки. Їм доручено ведення слідчої діяльності з метою виявлення та притягнення до судової відповідальності осіб, винних у зловмисних діях в комп'ютерних системах і мережах. Ці служби також беруть участь в профілактичній та інформаційній роботі з відповідним категоріям громадян.

Більше того, протягом останніх декількох років Франція повністю переформатувала свої пріоритети в області оборони і національної безпеки, з огляду на збільшення обсягу, рівня, інтенсивності та складності національних кіберзагроз, в тому числі кібер-злочинності, політичного і економічного шпигунства, нападів на найважливіші об'єкти інфраструктури, а також інших кібер-порушень. «Біла книга з питань національної оборони і безпеки» 2008 року була першим основоположним документом, адресованим виключно проблематики національних кібер-загроз як основного ризику для національної безпеки і суверенітету. У ній визначалися нові пріоритети, такі як запобігання і

реагування на кібератаки, а також передбачалися інституційні зміни, необхідні для забезпечення національної безпеки [30, с. 40].

Власне штаб із кіберзахисту як один із суб'єктів забезпечення кібербезпеки держави визначив основні (ключові) поняття для сфери кібербезпеки. Кіберзахист- це всі дії, здійснювані з метою військового втручання або втручання в кіберпростір, щоб гарантувати ефективність дій збройних сил, виконання доручених місій і належне функціонування міністерства. Кіберзахист слід відрізняти від кіберзлочинності, яка відповідає всім традиційним і новим злочинам і злочинам, що вчиняються за допомогою цифрових мереж [38, с. 40].

Штаб із кіберзахисту Франції (COMCYBER) є оперативним підрозділом, командувачем, органічно або функціонально, усіма силами кіберзахисту французьких армій. Що знаходиться під безпосереднім керівництвом начальника штабу оборони, COMCYBER відповідає за загальний кібер-маневр. Створений в 2017 році [46, с. 143]. Штаб із кіберзахисту Франції виконує наступні завдання: захист інформаційних систем, що знаходяться під відповідальністю начальника штабу оборони в якості компетентного органу з безпеки інформаційних систем; захист інформаційних систем Міністерства збройних сил, за винятком систем Генерального директорату зовнішньої безпеки (DGSE) і Управління військової розвідки і безпеки (DRSD); розробка, планування і проведення військових операцій з кіберзахисту під керівництвом заступника начальника штабу з «операціями»; внесок в розробку кадрової політики в області кіберзахисту; внесок армій і спільних організацій в національну та міжнародну політику в області кіберзахисту, зокрема в розробку і реалізацію планів співробітництва; визначення конкретних технічних потреб для кіберзахисту – узгодженість моделі кіберзахисту департаменту і загальної координації; розробка та управління резервом кіберзахисту. Штаб із кіберзахисту Франції здійснює оперативний нагляд за майже 3400 кібер-комбатантами в міністерстві. Для виконання своїх місій, Штаб із кіберзахисту Франції має штат і має повноваження над трьома спільними організаціями: CALID, CASSI і CPROC [46, с. 140–141].

Відтак, з метою забезпечення кібербезпеки держави у Франції створено належну нормативно-правову базу функціонування уповноважених на забезпечення кібербезпеки держави органів. При цьому, захист кібернетичного простору та протидія кіберзлочинності вважаються пріоритетом для забезпечення національної безпеки Франції та здійснюється не лише органами поліції (жандармерії), але й також на рівні Міністерства оборони та спеціально створених органів [13, с. 120].

Щодо окремих фахівців, які приймають участь у розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку досить цікавим є досвід Великобританії. Там, існує інститут консультантів, як спеціалізованих фахівців, які вивчають обставини конкретного кримінального провадження, аналізують наявну доказову базу і надають рекомендації слідчим щодо доцільності дослідження конкретних речових доказів, визначення виду експертиз та послідовності їх призначення.

На наше переконання, особливу увагу доцільно приділити дослідженню позитивного досвіду протидії кіберзлочинності як Німеччина, що є однією з провідних держав-членів ЄС.

Зокрема, Німеччина продемонструвала прихильність пріоритету забезпечення безпеки і боротьби з кібер-злочинністю підписавши (в 2001 році) і ратифікувавши (у 2009 році) Міжнародну конвенцію по кібер-злочинів Ради Європи, також відому, як Будапештська конвенція, а також зробивши ряд кроків для її реалізації в країні. Німеччина також підписала і ратифікувала Додаткові протоколи до Конвенції по кібер-злочинів, які криміналізують расистську і ксенофобську діяльність, здійснену за допомогою комп'ютерних систем. У своїй Національної стратегії кібер-безпеки Німеччина підтвердила свою прихильність подальших зусиль в області гармонізації міжнародного кримінального права на основі Будапештської конвенції [60].

Так, у липні 2015 року в Німеччині був прийнятий Акт про інформаційну безпеку (IT Security Act), метою якого є запобігання шкоди найважливішим IT-

систем, таким, наприклад, як системи Міністерства внутрішніх справ (BSI), провайдерів телекомунікаційних послуг, операторів критично важливих елементів інфраструктури та ін. в даний час, BSI займається реалізацією положень цього Акта, який включає в себе мінімальні стандарти кібербезпеки для понад 2000 критично важливих інфраструктурних компаній.

Відповідно до законодавства, такі мінімальні стандарти безпеки забезпечуються за рахунок розвитку доступності, автентичності, конфіденційності та цілісності систем кібер-безпеки в усій країні; підвищення рівня інтернет-безпеки для громадян; а також підвищеного рівня захисту критично важливих в національному масштабі елементів інфраструктури [60].

Поряд з цим, в Німеччині діють і інші закони, що забороняють такі злочинні дії, як комп'ютерне шахрайство, фальсифікація даних, комп'ютерний саботаж, кібер-шпигунство, фішинг, а також інші подібні кібер-злочину, які, відповідно до національного законодавства, переслідуються нарівні з звичайними злочинами [60].

Водночас, що стосується правоохоронної діяльності, в Німеччині створені достатні умови для протидії різним видам кібер-злочинності. NCAZ, BSI і BKA спільно працюють в області боротьби з кібер-злочинністю в національному масштабі. Зокрема, NCAZ об'єднує ресурси різних урядових агентств, в т.ч. Федеральної поліції і Федеральної розвідувальної служби, а також приватного сектора.

Крім того, національна стратегія кібер-безпеки, яка була прийнята у 2011 році передбачає розвиток потенціалу правоохоронних органів, BSI, а також приватного сектора, в області боротьби з кіберзлочинністю, а також в галузі захисту країни від шпигунства і саботажу. У Німеччині створено «органи спільного реагування за участю приватного сектора і компетентних правоохоронних органів». Як вказується в Акті про інформаційну безпеку 2015 року, для успішної реалізації зазначених завдань будуть потрібні додаткові зусилля і подальший прогрес. В кінці 2017 року стане відомо, наскільки успішно співпрацювали до цього моменту уряд і приватний сектор, щоб значно знизити

рівень кіберзлочинності. З огляду на все сказане, варто все ж зазначити, що залишається поки неясним, чи існують в країні успішні ініціативи в галузі навчання суддів, прокурорів, юристів, співробітників правоохоронних органів, криміналістів, і також інших фахівців [60].

Також, в лютому 2019 року інформаційне агентство Agence France-Presse повідомило, що Німеччина вступила до лав країн НАТО та надала альянсу власні кібер можливості в боротьбі з кібервзломами та електронною війною [31]. НАТО визначає кіберпростір як область конфлікту поряд із сушею, морем і повітрям, в зв'язку з почастішанням електронними атаками з боку держав, кіберзлочинців і так званих «хактівістів», а також з огляду на можливі наслідки загроз.

Поряд з цим, у липні 2017 року керівництво підрозділу безпеки військової авіації Німеччини започаткувало нову ініціативу щодо протистояння кіберзагроз після того, було оприлюднено дослідження, що показало, що хакери можуть зламувати військові літаки з допомогою недорого обладнання. Отже, в Німеччині з метою забезпечення кібербезпеки держави створено ряд спеціальних органів, зокрема – кібернетичну авіацію, що є важливою складовою протидії кіберзлочинності.

З метою посилення кібербезпеки країн Європейського союзу, Єврокомісія запропонувала в вересні 2017 року пакет заходів, що включає створення Агентства кібербезпеки ЄС і введення сертифікатів для продукції, що випускається в ЄС цифрової продукції і послуг.

На сьогоднішній день вказане агентство успішно функціонує на території країн-членів ЄС. Агентство ЄС з кібербезпеки у відповідності зі Стратегією ЄС керується у своїй діяльності також прийнятою Директивою ЄС з інформаційної безпеки [40].

Крім того, на початку березня 2020 року шість європейських країн підписали угоду, щоб створити загальні кібернетичні війська, очолювані Литвою. Так, Естонія, Литва, Хорватія, Польща, Нідерланди та Румунія підписали меморандум про взаєморозуміння в Загребі, де відбулася неформальна зустріч міністрів оборони ЄС. Відповідно до угоди, в усіх цих країнах будуть створені

міжнародні команди, готові відповісти на кібератаку в будь-який час. Меморандум на законних підставах дозволяє використовувати ці сили в юрисдикціях різних країн, визначає механізм роботи команд, їх правовий статус, роль і процедури [195].

При цьому зазначимо, Литва підняла ідею створення сил швидкого реагування на кіберзагрози в ЄС ще в 2017 році. Багатонаціональна організація для реагування на кіберінциденти, що складається з литовців, голландців, поляків і румунів, знаходиться в режимі очікування з початку 2020 року. Нещодавно створені кібергрупи, названі Групою загальноєвропейського реагування в кіберпросторі (European Union Cyber Rapid Response Teams, CRRT), стали частиною організації Постійного структурованого співробітництва Європейського Союзу (PESCO), заснованої в 2018 році. Вона дозволяє державам-членам ЄС розширювати співпрацю в області оборони [196].

Також, на нашу думку, перспективним і доцільним є запровадження в діяльність судово-експертних установ України «Глобальних керівних принципів лабораторій цифрової криміналістики», підготовлених й опублікованих Інтерполом (INTERPOL Global guidelines for digital forensics laboratories), які схвалені та рекомендовані до впровадження Європейською мережею криміналістичних установ (European Network of Forensic Science Institutes).

У підсумку, зазначимо, що сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому ми маємо використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки, оскільки вона є невід’ємним напрямком побудови інформаційного суспільства, розвиток якого повинен йти не лише через нарощування технологічних можливостей здійснення інформаційного обміну, а й через глибоке усвідомлення всіма суб’єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту інформаційних

ресурсів та забезпечення безпеки держави, у тому числі враховуючи зарубіжний досвід протидії кіберзлочинності в сфері забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [122]. Переконані, що удосконалення техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей країни на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю з метою оптимального входження у європейське та світове правове поле.

Висновки до розділу 1

Результати виконаного в роботі теоретико-методологічного аналізу сукупності наукових праць провідних українських та іноземних учених, у тому числі й дисертаційних досліджень, монографій, наукових статей, пізнавально-аналітичних оглядів з проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку дають можливість зробити такі висновки:

1. У підрозділі висвітлено стан наукових досліджень проблем розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Установлено, що розвиток сучасних інформаційних технологій, удосконалення виробництва й розширення сфери застосування новітньої кібернетичної техніки дали можливість зародження специфічного, складного виду злочинних діянь, де комп'ютерне оснащення та електронна інформація є об'єктом протиправного посягання. Визначено, що поряд із позитивними здобутками, інформатизація

супроводжується побічним негативним явищем криміногенного характеру, до якого належать злочини у сфері електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж або ж «комп'ютерна злочинність».

Загальний огляд стану наукової розробленості та законодавчої регламентації проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, свідчить про незначний спектр проведених досліджень з цієї тематики за різними галузевими спеціальностями.

2. Як і будь-яка діяльність, техніко-криміналістичне забезпечення досудового розслідування здійснюється уповноваженими суб'єктами відповідно до поставлених перед ними завдань, реалізація яких направлена на досягнення кінцевої мети – підвищення ефективності проведення досудового розслідування. У своїй сукупності мета й окремі завдання розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку утворюються зміст такого забезпечення.

Завдання техніко-криміналістичного забезпечення досудового розслідування знаходять свій прояв у конкретних напрямках такої діяльності, серед яких можна назвати: виявлення, збір, фіксацію доказової інформації; подальший аналіз такої інформації; залучення до слідчих (розшукових), негласних слідчих (розшукових) дій та оперативно-розшукових заходів компетентних у відповідній галузі осіб (які володіють спеціальними знаннями); оснащення уповноважених на здійснення техніко-криміналістичного забезпечення суб'єктів сучасними технічними засобами; формування в таких суб'єктів вмінь і навичок практичного застосування криміналістичної техніки; тощо.

Сутність техніко-криміналістичного забезпечення досудового розслідування може бути розкрита як створення належних умов щодо оснащення суб'єктів такої діяльності необхідними техніко-криміналістичними засобами, формування в них

знань, вмінь і навичок практичного їх застосування, а також залучення в разі необхідності компетентних осіб задля швидкого, повного та неупередженого розслідування злочинів даної категорії.

Під час провадження діяльності із здійснення техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виникають і знаходять свій розвиток відповідні суспільні відносини, провідним структурним елементом яких є їх суб'єкти. Під такими суб'єктами можуть бути визначені особи, які реалізують свої повноваження на підставі чинного національного законодавства, використовуючи техніко-криміналістичні засоби задля здійснення техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

3. Встановлено, що ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Визначено, що в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі. Акцентовано на пріоритетах міжнародної політики ЄС у кіберпросторі, а саме: свобода та відкритість – тобто принципи користування основоположними правами людини та громадянина у кіберпросторі; застосування законодавства ЄС у кіберпросторі в тій самій мірі, як і у фізичному світі; розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством.

Розкрито, що з метою забезпечення кібербезпеки держави у Франції створено належну нормативно-правову базу функціонування уповноважених на забезпечення кібербезпеки держави органів. При цьому, захист кібернетичного

простору та протидія кіберзлочинності вважаються пріоритетом для забезпечення національної безпеки Франції та здійснюється не лише органами поліції (жандармерії), але й також на рівні Міністерства оборони та спеціально створених органів [14]. У Німеччині з метою забезпечення кібербезпеки держави створено ряд спеціальних органів, зокрема – кібернетичну авіацію, що є важливою складовою протидії кіберзлочинності.

РОЗДІЛ 2.
ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОВЕДЕННЯ 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

2.1. Поняття та види техніко-криміналістичних засобів, що застосовуються під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Протидія кримінальним правопорушенням є одним із важливих напрямів діяльності держави. Тому на сучасному етапі органи державної влади і уряд України вимагають постійного вдосконалення роботи правоохоронних органів.

Необхідність застосування техніко-криміналістичних засобів, що застосовуються під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, продовжує залишатися актуальною в усьому світі в зв'язку з прогресивною тенденцією скоєння цих злочинів.

Протягом останніх років учені-криміналісти та співробітники органів правопорядку вказують на низький рівень оснащення органів правопорядку новими науково-технічними засобами та інноваційними продуктами [52, с. 125].

Враховуючи події останніх років, кількість кримінальних проваджень, пов'язаних з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, в Україні помітно збільшилась. Про це свідчать повідомлення засобів масової інформації та статистичні дані правоохоронних органів. Зокрема, за даними Національної поліції України, тільки в 2019 році співробітники Департаменту кіберполіції

Національної поліції викрили 4263 злочинів, наразі в Україні у повному обсязіприсутні всі ключові «класичні» кіберзлочини, які вчиняються за допомогою комп'ютерних і телекомунікаційних технологій – платіжні системи 1641, протиправний контент 332, електронна комерція 744, кібербезпека 1494 [50, с. 9].

Незважаючи на те, що в засобах масової інформації періодично з'являються повідомлення про отримання поліцією нової техніки [123], за результатами проведеного нами анкетування співробітників органів досудового розслідування встановлено, що, на думку 86 % респондентів, рівень їх оснащеності науково-технічними засобами та інноваційними продуктами є недостатнім.

Як зауважують В. Ю. Шепітько , В. А. Журавель , Г. К. Авдєєва під час узагальнення матеріалів анкетування 295 слідчих встановлено, що, на думку 9,6 % респондентів, наявні техніко-криміналістичні засоби не є досконалими та компактними. Респонденти висловили такі побажання щодо поліпшення характеристик техніко-криміналістичних засобів вітчизняного виробництва: оновлення до рівня зарубіжних (2,7 %), зменшення габаритних розмірів і маси (3,7 %), підвищення ефективності і точності вимірів (1,7 %), можливості комп'ютерної обробки доказової інформації (3,2 %), збільшення швидкості дії (0,7 %), створення спеціалізованих комплектів науково-технічних засобів для різних відомств (76, 2 %) та ін. [189, с. 39].

Результативність попередження, розкриття та розслідування кримінальних правопорушень, як зазначив професор А. В. Іщенко, безпосередньо залежить від надійності засобів та методів, досконаліть яких зумовлена тим, наскільки вони враховують новітні здобутки науково-технічного прогресу. Чим більше вони містять у собі досягнень передової науки і техніки, тим більше їх використання забезпечує оптимізацію вирішення завдань протидії злочинності [54, с. 8–9].

Як слушно зазначають В.В. Лисенко та О.С. Задорожний, процеси виявлення й розкриття злочинів повинні мати відповідне криміналістичне забезпечення техніко-криміналістичними засобами, тактичними прийомами та методичними рекомендаціями [87, с. 212–213].

Проте практика впровадження здобутків науково-технічного прогресу інколи яскраво демонструє непридатність тих чи інших технологій для використання в реальному житті, тим паче під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Таким чином, на наш погляд, необхідно більш детально зупинитися на науково-технічних засобах.

Так, І.Ф. Хараберюш вдало зазначив, що протягом усієї людської історії в правоохоронній діяльності використовуються різні технічні засоби та досягнення науки, починаючи зі знарядь катувань і закінчуючи новітніми напрацюваннями в галузі поліграфології та біометрії. Об'єктивна необхідність застосування в правоохоронній діяльності науково-технічних засобів визначається не тільки прагненням правоохоронців спростити й прискорити процес розкриття й розслідування злочинів, але також і властивостями останніх значно розширювати діапазон можливостей людського сприйняття. Здатність об'єктивно відображати події, що відбуваються, запам'ятовувати їх із найменшими подробицями, довгостроково зберігати й багаторазово відтворювати робить науково-технічні засоби найважливішим інструментом забезпечення об'єктивного розкриття та розслідування кримінальних проваджень і фактором, що сприяє дотриманню прав і свобод громадян [180, с. 1–7].

Сучасні науково-технічні досягнення криміналістики зумовили розвиток її теоретичних основ, розширили можливості кримінального судочинства щодо ефективного та всебічного судового розслідування кримінальних проваджень. На думку М.В. Салтевського, під науково-технічними засобами слід розуміти засоби, що використовуються в боротьбі зі злочинністю протягом процесуальних слідчих дій для збирання криміналістичної інформації [151, с. 11–14; 64, с. 31], проте такий підхід, на нашу думку, звужує та применшує значимість використання та впровадження здобутків науково-технічного прогресу.

Значно ширших поглядів на предмет науково-технічних засобів притримується В.А. Панюшкін, який вважає, що науково-технічний засіб може бути визначений «як штучно створений матеріальний засіб доцільної діяльності

людей, що втілив у собі наукові знання». На його думку, будь-який технічний засіб може бути визнаний науково-технічним за умови втілення в ньому хоча б невеликої дещиці наукового знання. Якщо такого втілення немає, то немає й науково-технічного засобу. Такий підхід до розуміння науково-технічного засобу видається не зовсім точним через його однобічність. Безумовно, не можна не погодитися з тезою, що технічний засіб повинен утілювати наукове знання. Ні в кого не викликає сумніву, що наукові знання втілюють у собі технічні засоби, спеціально створені або пристосовані для цілей боротьби з правопорушеннями шляхом перероблення (удосконалення) загальнотехнічних засобів. Що ж стосується загальнотехнічних засобів, тобто засобів, запозичених з інших галузей знань і використовуваних без будь-якої переробки, то наукове знання, безумовно, закладене в приладах, апаратурі тощо (наприклад, мікроскоп, плівкова чи цифрова фотокамера). Такі ж загальнотехнічні засоби, як викрутка, молоток, голка й ін., як вважає В.А. Панюшкін, під час їхнього створення навряд чи втілили в собі елементи наукового знання. На користь своєї позиції він, посилаючись на В.М. Радіонова й А.І. Черепнєва, зазначили, що протягом тривалого часу люди створювали технічні засоби відповідно до законів природи, що здебільшого ще не були відкриті. Тому в основі створення техніки лежали факти і явища, виявлені емпіричним шляхом, а саме розроблення технічних засобів ґрунтувалося на практичному досвіді, інтуїції та численних пробах. Наукові знання в процесі створення техніки майже не застосовувалися, тому що наука в цей період відставала в розвитку й займалася в основному осмисленням явищ, що вже використовувалися в технічних засобах [66, с. 37]. На наш погляд, ця теза дещо ідеалізує й узагальнює поняття науково-технічних засобів, але не дає конкретних відповідей стосовно предмета нашого дослідження.

Поділяючи науково-технічні засоби на техніко-криміналістичні і загально-технічні, В.Г. Гончаренко зазначив: поняттям «науково-технічні засоби» слід охоплювати усі без винятку засоби і методи їх застосування, використовувані у слідчій роботі, а терміном «техніко-криміналістичні засоби» – технічні засоби, спеціально створені для криміналістичних цілей чи пристосовані для цього

шляхом зміни загально-технічних засобів [34, с. 9–10]. На наш погляд, наукові дискусії щодо застосування різної термінології при позначенні технічних засобів, що використовуються при розслідуванні, не мають підґрунтя. Є цілком зрозуміле поняття «технічні засоби», що не потребує тлумачення. Будь-які технічні засоби та методи їх застосування, що можуть використовуватись при розслідуванні кримінальних правопорушень розглядаються у розділі криміналістики – криміналістичній техніці, тобто є техніко-криміналістичними.

У зміст поняття техніко-криміналістичних засобів окремі науковці вкладають також методи їх застосування. Так, В.Г. Гончаренко дає таке визначення: науково-технічні засоби, застосовувані в слідчій роботі, являють собою систему загально-технічних пристроїв і спеціально розроблених приладів, апаратів, устаткування, інструментів, пристроїв, матеріалів, а також методів і прийомів їх застосування з метою найефективнішого проведення попереднього розслідування, дізнання і попередження злочинів» [34, с. 10]. Базуючись на визначенні науково-технічних засобів, запропонованих В.Г. Гончаренком, В.В. Коваленко зазначили, що науково-технічні засоби – це система методів, загальнотехнічних засобів і спеціально розроблених приладів, апаратів, устаткування, інструментів, пристосувань, матеріалів, технологій, а також прийомів їхнього застосування з метою найбільш ефективного проведення дізнання, досудового слідства, судового розгляду і профілактики злочинів [65, с. 241].

Аналізуючи наведені визначення можна помітити їх схожість з визначенням криміналістичної техніки, як розділу криміналістики, що є системою наукових положень та розроблюваних на їх основі технічних засобів, прийомів і методів, призначених для збирання, дослідження і використання доказів [78, с. 8] або включає систему теоретичних положень, принципів і технічних засобів і методів, що ґрунтуються на них і застосовуються для збирання, опрацювання, дослідження і подання криміналістичної інформації при розслідуванні та запобіганні злочинів [150, с. 55–56]. На нашу думку, поняття технічних засобів, що застосовуються при розслідуванні не можна ототожнювати з розділом науки

криміналістики. Ми погоджуємось з думкою І.В. Пирога, який на основі етимології понять («засіб – те, що служить знаряддям у якій-небудь дії, справі», а «метод – спосіб пізнання явищ природи та суспільного життя», зазначив, що «застосування будь-якого технічного засобу відбувається певними методами. Розробка методів застосування технічного засобу проходить одночасно з його винаходом. Але за сутністю ці поняття різні та їх неможна ототожнювати» [118, с. 251]. Ми погоджуємось з думками науковців, які під науково-технічними засобами розуміють «прилади, пристосування або матеріали, які використовується для збирання та дослідження доказів або створення умов, що ускладнюють учинення злочинів» [8, с. 73], не вказуючи при цьому на методи їх застосування. У визначенні, наведеному А. А. Саковським, наголошується на науковій та практичній обумовленості технічних засобів криміналістики та можливості їх використання у кримінальному процесі: «спеціальні технічні засоби криміналістики – це науково обумовлені, перевірені експериментально і на практиці ефективні технічні засоби, які використовуються суб'єктами кримінально-процесуальної, експертної, оперативно-розшукової і адміністративної діяльності» [77, с. 69].

Враховуючи аналіз думок науковців та зважаючи на надані вище визначення понять «технічних засобів», «забезпечення», «техніко-криміналістичні дослідження» маємо надати власне визначення *техніко-криміналістичних засобів* що використовуються під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Отже, на наш погляд техніко-криміналістичні засоби, що використовуються під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – це система спеціально виготовлених або пристосованих приладів, пристроїв, пристосувань, інструментів, матеріалів, інформаційних пошукових, ідентифікаційних та інших систем, а також криміналістичних технологій їх застосування з метою виявлення, фіксації, вилучення, дослідження, обліку,

аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів, а також здійснення інших дій по виявленню, розслідуванню та попередженню злочинів.

Розглянемо класифікацію технічних засобів, що застосовуються при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Видами техніко-криміналістичних засобів, що застосовуються під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є (див. Додаток Б):

1) Апаратні засоби мобільної криміналістики.

Комп'ютерна експертиза досліджує велику кількість різноманітних цифрових пристроїв і джерел даних. У дослідженнях можуть використовуватися як програмні, так і апаратні засоби.

Розглянемо найбільш поширені *апаратні засоби мобільної криміналістики.*

Cellebrite UFED Touch 2 – це продукт, який спочатку розроблявся для роботи в польових умовах. Концептуально розділений на дві частини:

– фірмовий планшет *CellebriteUFEDTouch 2* (або *UFED 4PC*– програмний аналог *CellebriteUFEDTouch 2*, що встановлюється на комп'ютер або ноутбук фахівця): використовуються тільки для отримання даних;

– *UFED Physical Analyzer* – програмна частина, призначена для аналізу даних, витягнутих із мобільних пристроїв.

Концепція використання обладнання передбачає, що за допомогою Cellebrite UFED Touch 2 фахівець отримує дані в польових умовах, а потім у лабораторії здійснює їх аналіз за допомогою UFED Physical Analyzer. Відповідно, лабораторний варіант становить два самостійні програмні продукти UFED 4PC і UFED Physical Analyzer, які встановлені на комп'ютері дослідника. Цей комплекс забезпечує отримання даних із максимально можливої кількості мобільних пристроїв [15].

Під час аналізу частина даних може бути втрачена програмою UFED Physical Analyzer. Тому рекомендується проводити контроль повноти аналізу даних, здійснений цією програмою [200].

MSABXRY / MSABXRYField – аналог продуктів Cellebrite, що розробляється шведською компанією MicroSystemation. На відміну від парадигми Cellebrite, компанія MicroSystemation передбачає, що в більшості випадків їхні продукти використовуватимуться на стаціонарних комп'ютерах або ноутбуках. До продукту додається фірмовий USB-хаб, який називають на сленгу «шайба», та комплект перехідників і дата-кабелів для підключення різних мобільних пристроїв [197].

Компанія також пропонує версії *MSABXRYField*і *MSABXRYKiosk*– апаратні продукти, призначені для отримання даних із мобільних пристроїв, реалізовані у вигляді планшета і кіоску. *MSAB XRY* добре зарекомендував себе за отримання даних із застарілих мобільних пристроїв [15].

Віднедавна набули популярності апаратні засоби для проведення chip-off (метод отримання даних безпосередньо з чипів пам'яті мобільних пристроїв), розроблені польською компанією Rusolut. За допомогою цього обладнання можна отримувати дані з пошкоджених мобільних пристроїв і пристроїв, заблокованих PIN-кодом або графічним паролем. Rusolut пропонує кілька наборів адаптерів для отримання даних із певних моделей мобільних пристроїв. Скажімо, комплект адаптерів для отримання даних із чипів пам'яті, які переважно використовуються в «китайських телефонах». Однак широке використання виробниками мобільних пристроїв шифрування даних користувача в топових моделях призвело до того, що це обладнання поступово втрачає актуальність. Витягти дані з чипа пам'яті з його допомогою можна, але вони будуть у зашифрованому вигляді [63].

2) Програмні засоби мобільної криміналістики.

Спостерігаючи за розвитком мобільної криміналістики, можна побачити, що в міру розвитку функціональних можливостей мобільних пристроїв відбувається і розвиток програм для їх аналізу. Якщо раніше слідчі або оперативні працівники задовольнялися даними з телефонної книги, SMS, MMS, викликами, графічними і

відеофайлами, то зараз фахівців просять «витягти» більшу кількість даних, зокрема: дані з програм обміну повідомленнями; дані з електронної пошти; історію відвідування ресурсів мережі Інтернет; дані про геолокацію; видалені файли й іншу видалену інформацію тощо. Усі ці відомості можна витягти спеціальним програмним забезпеченням [15].

«Мобільний криміналіст» – сьогодні одна з найкращих програм для аналізу даних, отриманих із мобільних пристроїв. Інтегровані переглядачі баз даних *SQLite* і *plist-файлів* дозволяють більш досконально досліджувати певні SQLite-бази да-них і plist-файли вручну. Спочатку програма розроблялася для використання на комп'ютерах, тому використовувати її на нетбуці або планшеті (пристроях із розміром екрану 13 дюймів і менш) буде некомфортно. Особливістю програми є жорстка прив'язка шляхів, за якими розташовані файли – бази даних додатків. Тобто, якщо структура бази даних будь-якої програми залишилася незмінною, але змінився шлях, яким база даних знаходиться в мобільному пристрої, «Мобільний криміналіст» просто пропустить таку базу даних під час аналізу. Тому дослідження подібних баз даних доведеться проводити в ручному режимі, використовуючи файловий браузер «Мобільного криміналіста» і допоміжні утиліти [15].

Тенденцією останніх років є «змішання» функціоналу програм. Зокрема, виробники, які традиційно розробляли програми для мобільної криміналістики, впроваджують у свої продукти функціонал, що дає змогу досліджувати жорсткі диски. Виробники криміналістичних програм, орієнтованих на дослідження жорстких дисків, додають у них функціонал, необхідний для дослідження мобільних пристроїв. І ті, і інші додають функціонал із вилучення даних із хмарних сховищ тощо. У підсумку виходять універсальні «програми-комбайни», за допомогою яких можна здійснювати і аналіз мобільних пристроїв, і аналіз жорстких дисків, і вилучення даних із хмарних сховищ, і аналітику даних, отриманих із цих джерел. У переліку програм для мобільної криміналістики саме такі програми посідають два місця: *Magnet AXIOM* – програма канадської

компанії Magnet Forensics і *Belkasoft Evidence Center* – розробка компанії Belkasoft [15].

Ці програми за функціональними можливостями щодо отримання даних із мобільних пристроїв дещо поступаються програмним і апаратним засобам, описаним вище. Але вони добре здійснюють їх аналіз і можуть використовуватися для контролю повноти вилучення різних типів даних. Обидві програми активно розвиваються і стрімко нарощують свій функціонал у дослідженні мобільних пристроїв [15].

3) Апаратні засоби копіювання даних.

Mediaimager GM5 – потужний криміналістичний пристрій-копіювальник цифрових носіїв інформації. Він дає змогу швидко й безпечно робити двійкові копії носія інформації, відповідно здатний зробити одночасно дві копії в базовій версії та до шести копій розширених версіях.

4) Апаратні блокіратори запису.

Tableau T35U – апаратний блокіратор компанії Tableau, який дозволяє безпечно підключати досліджувані жорсткі диски до комп'ютера дослідника по шині USB3 [199].

Цей блокіратор має роз'єми, які дозволяють підключати до нього жорсткі диски за інтерфейсами IDE і SATA (а за наявності перехідників – і жорсткі диски з іншими типами інтерфейсів). Особливістю цього блокіратора є можливість емуляції операцій «читання-запис». Це буває корисним у дослідженні накопичувачів, заражених шкідливим програмним забезпеченням [199].

Tableau Forensic Universal Bridge T356789iu – Tableau Forensic Universal Bridge – це інтегрований блокіратор запису, який монтується у відсік для накопичувачів на робочій станції судового експерта, або по шині USB3 і підтримує інтерфейси SATA, USB 3.0, PCIe, SAS, FireWire 800 і IDE.

WiebitechForensicUltraDockv5 – апаратний блокіратор компанії CRU. Має функціонал, аналогічний блокіратору TableauT35U [201].

Додатково цей блок можна з'єднати з комп'ютером дослідника по більшій кількості інтерфейсів. Якщо до цього блокіратора буде підключено жорсткий

диск, доступ до даних на якому обмежений ATA-паролем, на дисплеї блокіратора з'явиться відповідне повідомлення. Крім того, у підключенні жорсткого диска, що має технологічну зону DCO (Device Configuration Overlay), ця зона автоматично буде розблокована для того, аби фахівець міг скопіювати данхzі, що знаходяться в ній.

Усі блокіратори запису як основне підключення використовують підключення до комп'ютера дослідника по шині USB3, що забезпечує комфортні умови роботи дослідника за клонування й аналізу носіїв інформації [201].

5) Програмні засоби комп'ютерної експертизи.

Ще 15 років тому безперечними лідерами комп'ютерної експертизи були програми *EncaseForensics* і *AccessDataFTK*. Їх функціонал природним чином доповнював один одного і давав змогу отримувати максимальну кількість різних типів даних із досліджуваних пристроїв. У наші дні функціональність Encase Forensics значно відстає від пропонованих сьогодні вимог до програмного забезпечення для дослідження комп'ютерів і серверів під управлінням Windows. Використання Encase Forensics актуально в «нестандартних» випадках: коли необхідно досліджувати комп'ютери під управлінням ОС MacOS або сервера під керуванням ОС Linux, витягувати дані з файлів рідкісних форматів. Умонтована в Encase Forensics макромова Ensripts містить величезну бібліотеку готових скриптів, реалізованих виробником і ентузіастами, за допомогою яких можна здійснити аналіз великої кількості різних операційних і файлових систем [15].

AccessDataFTK намагається підтримувати функціональність продукту на необхідному рівні, але час обробки накопичувачів значно перевищує розумну кількість часу, яку може дозволити собі витратити середньостатистичний фахівець на подібне дослідження.

До особливостей *Access Data FTK* слід віднести:

– пошук за ключовими словами реалізований на дуже високому рівні;

– аналітика різних кейсів, що дозволяє виявляти взаємозв'язки в пристроях, вилучених у різних провадженнях;

– можливість налаштування інтерфейсу програми під себе;

– підтримка файлів рідкісних форматів (приміром, баз даних Lotus Notes).

Encase Forensics і AccessData FTK можуть обробляти величезні масиви вихідних даних, що вимірюються сотнями терабайт [201].

Magnet Axiom є безперечним лідером програмних засобів для комп'ютерної криміналістики. Ця програма покриває функціоналом цілі сегменти: дослідження мобільних пристроїв, витяг із хмарних сховищ, вивчення механізмів під управлінням операційної системи MacOS тощо. Програма має зручний і функціональний інтерфейс, у якому все під рукою, і може застосовуватися для розслідування інцидентів інформаційної безпеки, пов'язаних із зараженням комп'ютерів або мобільних пристроїв шкідливим програмним забезпеченням або з витоками даних [15].

Аналогом Magnet AXIOM є Belkasoft Evidence Center. Belkasoft Evidence Center дозволяє витягувати і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків. При аналізі жорстких дисків здійснюється вилучення даних із веббраузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, витяг файлів за заданим розширенням, даних про геолокацію, електронної пошти, даних із платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо. Має гнучкий функціонал щодо вилучення віддалених даних.

Переваги програми Belkasoft Evidence Center такі:

– широкий спектр даних із різних носіїв інформації;

– вмонтований переглядач баз даних SQLite;

– збір даних із віддалених комп'ютерів і серверів;

– інтегрований функціонал щодо перевірки виявлених файлів на Virustotal.

Недоліками програми є незручний інтерфейс і неочевидність виконання окремих дій в програмі. Для ефективного використання програми необхідно пройти відповідне навчання [201].

Поступово ринок завойовує *X-Ways Forensics*. Особливістю цієї швейцарської програми є велика швидкість обробки даних (порівняно з іншими програмами цієї категорії) та оптимальний функціонал, що задовольняє основні

потреби фахівця з комп'ютерної криміналістики. Програма має вмонтований механізм, що дозволяє мінімізувати хибно позитивні результати. Тобто дослідник, здійснюючи відновлення файлів із жорсткого диска обсягом 100 Гб, бачить не 1 Тб відновлених файлів (велика частина з яких є хибно позитивними результатами, як це зазвичай відбувається у використанні програм відновлення), а саме ті файли, які реально були відновлені [15].

За допомогою програми X-Ways Forensics можливо: знаходити й аналізувати дані електронної пошти; аналізувати історію веб-браузерів, журнали ОС Windows та інші системні артефакти; відфільтрувати результати, залишити тільки цінні й актуальні відомості; побудувати тимчасову шкалу і переглянути активності в період, що цікавить; реконструювати RAID; монтувати віртуальні диски; здійснювати перевірку на наявність шкідливого програмного забезпечення. Ця програма дуже добре зарекомендувала себе у ручному аналізі жорстких дисків, витягнутих із відеореєстраторів. За допомогою функціоналу X-Tension є можливість підключення в програмі модулів сторонніх розробників [15].

До недоліків X-Ways Forensics слід віднести: аскетичний інтерфейс; відсутність повноцінного вбудованого переглядача баз даних SQLite; необхідність глибокого вивчення програми: виконання деяких дій, необхідних для отримання потрібного фахівцю результату, не завжди очевидно [15].

6) Апаратні засоби відновлення даних.

Нині на ринку домінує компанія *ACELab*, яка виробляє апаратні засоби для аналізу, діагностики та відновлення жорстких дисків (комплекси PC-3000 Express, PC-3000 Portable, PC-3000 UDMA, PC-3000 SAS), SSD накопичувачів (ком-плекс PC-3000 SSD), флеш-накопичувачів (комплекс PC-3000 Flash), RAID (комплекси PC-3000 ExpressRAID, PC-3000 UDMARAID, PC-3000 SASRAID) [172].

Домінування ACELab на ринку апаратних рішень із відновлення даних обумовлено високою якістю перелічених продук тів і ціновою політикою ACELab, яка не дозволяє конкурентам увійти на цей ринок.

Незважаючи на велику кількість різних програм відновлення, як платних, так і безкоштовних, дуже важко знайти програму, яка б коректно і повно здійснювала відновлення різних типів файлів у різноманітних файлових системах.

Тепер існують тільки дві програми, що мають приблизно однаковий функціонал, які дають змогу це робити: *R-Studio* і *UFSExplorer*. Тисячі програм відновлення інших виробників або не дотягують за своїми функціональними можливостями до зазначених програм, або істотно поступаються їм [15].

7) Відкрите програмне забезпечення.

Autopsy – зручний інструмент для аналізу комп'ютерів під управлінням операційної системи Windows і мобільних пристроїв під управлінням операційної системи Android, що має графічний інтерфейс. Може бути використаний у розслідуванні комп'ютерних інцидентів. *Photorec* – одна з ліпших безкоштовних програм для відновлення даних. *Eric Zimmerman Tools* – комплект безкоштовних утиліт, кожна з яких дає змогу досліджувати якийсь окремий артефакт Windows. Як засвідчила практика, використання Eric Zimmerman Tools підвищує ефективність роботи фахівця за реагування на інцидент у «польових умовах». Нині ці утиліти доступні у вигляді пакету програм *Kroll Artifact Parser and Extractor (KAPE)* [15].

8) Дистрибутиви на основі Linux.

SIFT – Linux-дистрибутив розроблений і підтримуваний комерційною організацією SANSInstitute, яка спеціалізується на підготовці фахівців у галузі кібербезпеки і розслідуванні інцидентів. SIFT містить велику кількість актуальних версій безкоштовних програм, які можуть бути використані як для отримання даних із різних джерел, так і для їх аналізу. SIFT використовується під час проведення компанією SANS Institute навчань і його вміст постійно актуалізується.

Зручність роботи з цим дистрибутивом визначається конкретним інструментом, із яким доводиться працювати досліднику.

KaliLinux – унікальний Linux-дистрибутив, який використовується фахівцями для проведення аудиту безпеки і розслідування інцидентів. У 2017 році

видавництво «PacktPublishing» опублікувало книгу Шива В. Н. Парасрама (ShivaV.N. Parasram) «DigitalForensicswithKaliLinux», у якій наводяться практичні поради про те, як проводити копіювання, дослідження і аналіз комп'ютерів, окремих накопичувачів, копій даних із оперативної пам'яті і мережевого трафіку за допомогою утиліт, що входять у цей комплект [15].

На сьогодні зазначені прилади та програмні засоби дозволяють з більшою точністю та надійністю віднайти (відновити), зберегти та дослідити інформаційні сліди злочину та носії цифрової інформації.

2.2. 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

Основними засобами збирання доказів у сфері кримінального судочинства є слідчі (розшукові) дії. У КПК це прямо зазначено у ст. 93, де зазначається про те, що сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, а сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження вправі ініціювати їх проведення шляхом подання слідчому, прокурору відповідних клопотань, що розглядаються в порядку, передбаченому ст. 220 КПК.

Однією з найбільш поширених слідчих дій, в ході якої зазвичай збирається найбільша кількість слідової інформації є огляд, саме тому дану слідчу дію потрібно розглянути більш детально.

Огляд. Відповідно до ст. 237 КПК України огляд – це слідча (розшукова) дія, яка проводиться з метою виявлення слідів злочину та інших речових доказів, з'ясування обстановки злочину, а також інших обставин, що мають значення для кримінального провадження [88, с. 176].

Значення огляду для розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку дуже суттєве, бо у ході огляду знаходиться та вилучається значна кількість найважливіших слідів злочину. Огляд є первинною та невідкладною слідчою (розшуковою) дією, від якості якої, значною мірою залежить успіх всього подальшого розслідування [69, с. 7–9; 124, с. 3, 148, с. 95].

Розробкою теоретичних засад проведення огляду при розслідуванні комп'ютерних злочинів займалися Р.С. Бєлкін, В.М. Бутузов, В.Б. Вєхов, В.Д. Гавловський, В.О. Галанов, М.В. Гуцалюк, Д.А. Ілюшин, Ю.М. Казіміров, Д.О. Коваленко, В.В. Лісовий, О.І. Мотлях, Л.П. Паламарчук, В.В. Попова, Б.В. Романюк, М.В. Салтевський, О.В. Таран, Р.Б. Хамєтов та інші. Однак існує цілий ряд особливостей, які варто враховувати під час організації та проведення слідчого огляду під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [168, с. 178].

Завданням огляду місця події при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є своєчасне виявлення, вивчення, фіксація, вилучення та попереднє дослідження в установленому законом порядку необхідної інформації і різних видів слідів (матеріальних, ідеальних, віртуальних) з метою отримання необхідних відомостей і доказів, які мають значення для розкриття і розслідування злочинів, використовуваних в подальшому при висуненні версій у кримінальному провадженні [15].

Мета огляду місця події при розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – виявлення, фіксація та вилучення доказів вчиненого злочину. При розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку огляд може

проводитися на *місці*: а) збереження й обробки комп'ютерної інформації, яка зазнала злочинного впливу (наприклад, у випадку незаконного втручання в роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж); б) знаходження комп'ютерного обладнання, яке використовувалося при вчиненні злочину (наприклад, у випадку розповсюдження комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу); в) збереження інформації, отриманої злочинним шляхом (наприклад, у випадку заволодіння комп'ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем); г) порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі; д) настання шкідливих наслідків (знищення, перекручення комп'ютерної інформації, порушення роботи комп'ютера, системи або комп'ютерної мережі) [158, с. 79].

При огляді місця події докази злочинної діяльності (сліди і відповідну інформацію) можна знайти в комп'ютері (зокрема у його системному блоці на жорсткому диску), машинних носіях інформації (дискетах, магнітно-оптичних дисках, магнітних стрічках).

Зокрема, на *стадії підготовки до огляду місця події ще до виїзду на місце* насамперед необхідно вирішити організаційні питання. Вжити заходів для забезпечення охорони місця проведення огляду. Нерідко огляд необхідно проводити відразу в декількох приміщеннях, де знаходиться комп'ютерне обладнання. При проведенні огляду в комерційних структурах, які мають свої служби безпеки, не виключені спроби перешкодити проходу слідчо-оперативної групи до місця огляду. Такі факти повинні розцінюватися, як перешкода проведенню досудового слідства. До початку проведення слідчої дії необхідно отримати оперативно-розвідувальну інформацію такого змісту: марка та модель комп'ютера; тип операційної системи; периферійні пристрої; засоби зв'язку; інші відомості про систему, яка є об'єктом дослідження [70, с. 184]. Цю попередню інформацію слід терміново надати фахівцеві для своєчасного здійснення ним відповідних заходів, зокрема таких: отримати консультації інших фахівців (якщо в цьому виникла потреба); скласти план збору комп'ютерної інформації

необхідної для доказів; визначити і підготувати до використання відповідне обладнання, інструменти, програмне забезпечення та магнітні носії інформації тощо.

До підготовки будь-яких заходів (слідчих чи оперативно-розшукових), у тому числі й огляду, у розслідуванні незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж доцільно залучити спеціалістів з комп'ютерних систем (за освітою програміст-математик, інженер-програміст тощо). Ними можуть бути системні програмісти (фахівці з експлуатації програмних засобів), програмісти (фахівці зі створення програм для комп'ютерів), інженери з технічної експлуатації і ремонту комп'ютерів. Їх слід залучати з числа співробітників сторонніх організацій – науково-дослідних і навчальних закладів, компаній, які займаються розробкою й експлуатацією програмного та технічного забезпечення. У деяких випадках значну допомогу в розслідуванні можуть надати співробітники служби безпеки. Більшість програмістів вважають, що на сучасному рівні розвитку обчислювальної техніки без участі професіонала знайти «заховану» у комп'ютері інформацію без ризику знищення складно [58, с. 13–14].

Усякий раз при виборі спеціаліста слідчому необхідно переконатися у його компетентності в роботі з певними операційними системами, окремими програмними продуктами і периферійними пристроями [4, с. 36]. Серйозні проблеми, які призводять до значних витрат, можуть виникнути, у випадку коли з комп'ютерною технікою працюватиме некваліфікована особа. Тому існує нагальна потреба у створенні спеціалізованих «комп'ютерних» підрозділів або у залученні до слідства кваліфікованих фахівців.

До огляду місця події спеціаліст залучається для виконання таких операцій: виявлення засобів комп'ютерної техніки, її окремих компонентів, документації та інших об'єктів, що можуть містити сліди неправомірних дій; коректного завершення роботи програм; подальшого коректного відключення засобів комп'ютерної техніки від джерел енергопостачання; допомоги слідчому в описі засобів комп'ютерної техніки, її окремих компонентів та документації, що

вилучається; допомоги слідчому у визначенні переліку комп'ютерної техніки або окремих її компонентів, які підлягають вилученню або ізолюванню від вільного доступу; допомоги слідчому в підготовці засобів комп'ютерної техніки до транспортування [152, с. 36].

На робочій стадії етапу безпосереднього проведення огляду місця події кожен об'єкт підлягає детальному обстеженню. На цьому етапі важливо встановити, чи зберігає комп'ютер інформацію, яку можна плідно й цілеспрямовано використати в огляді (різні плани приміщень, паролі, коди доступу, шифри тощо). З цією метою спеціаліст проводить експрес-аналіз комп'ютерної інформації шляхом перегляду змісту дисків, файлів із текстовою і графічною інформацією.

На стадії фіксації ходу та результатів огляду необхідно визначити за допомогою спеціаліста, з урахуванням використання комп'ютера як знаряддя злочину чи джерела доказів, які носії криміналістично значущої інформації слід вилучити. Потрібно вилучати ті носії, які містять або з найбільшою імовірністю можуть містити докази вчиненого злочину. Такими *носіями криміналістично значущої інформації* є: а) системні блоки комп'ютера, в яких установлені жорсткі диски (недоцільно вилучати жорсткі диски окремо від системного блоку), переносні комп'ютери; б) клавіатура (не тільки у випадку виявлення та фіксації на її поверхні слідів), окремі з них можуть самостійно виступати в ролі термінала і мати дискові накопичувачі; в) принтери (саме оснащені платами пам'яті, у яких зберігаються завдання для друку); г) машинні носії інформації (гнучкі дискети, лазерні компакт-диски, магнітні стрічки) [110, с. 145].

Загальний огляд електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, працівникам правоохоронних органів часто доводиться мати справу із технічними засобами, які використовуються злочинцями у якості

знарядь та засобів вчинення злочинів. Серед таких засобів найчастіше зустрічаються:

– стаціонарні персональні комп'ютери (робочі станції або сервери);

– ноутбуки та нетбуки;

– планшети;

– бортові комп'ютери автомобілів;

– телевізори із функцією SMART;

– GPS-навігатори;

– носії цифрової інформації (диски, дискети, флеш-носії тощо);

– периферійне обладнання (принтери, сканери тощо);

– мобільні комп'ютерні пристрої із функцією телефону.

Враховуючи особливості роботи із наведеними пристроями, а також відповідне апаратне та програмне забезпечення, використовуване для їх огляду, відповідний процес можна умовно розділити на чотири види:

1) огляд ЕОМ носіїв та периферійних пристроїв;

2) огляд мобільних пристроїв:

– із функцією телефону;

– автомобільних пристроїв;

3) огляд побутових пристроїв («розумних речей»);

4) огляд інших пристроїв.

Перед проведенням відповідного огляду важливо правильно підібрати інструментарій оглядача. При цьому слід пам'ятати, що швидкий розвиток технологій, а також велика кількість умов, які виникають під час огляду ЕОМ, з чисто практичної точки зору унеможливлюють так звану сертифікацію відповідних апаратних та/або програмних засобів. Це підтверджується і правозастосовною практикою провідних західних країн.

В Україні така сертифікація також не проводиться, зважаючи на її недоречність. Так само в процесі огляду потрібно намагатися уникати використання програм, наявних у системі, що підлягає огляду, адже потім буде складно підтвердити правильність їх роботи.

Тому, враховуючи українське законодавство, видається правильним акцентувати увагу на двох важливих аспектах. По-перше, використовувані засоби мають бути з відповідною відкритою ліцензією або такими, що перебувають на балансі правоохоронного органу, аби можна було у будь-який час перевірити коректність їх роботи. По-друге, якщо використовується відкрите програмне забезпечення, наприклад, Live-CD під керуванням Linux, то відповідну копію із хеш-сумою диску потрібно долучити у якості додатка до протоколу огляду.

Основні інструменти, які можуть знадобитися для огляду ЕОМ, є наступні: портативний комп'ютер з автономним джерелом живлення; привод CD-ROM (DVD-ROM);викрутки та інший інструмент; комплекти запасних батарей; диски з операційними системами та іншими програмними засобами, накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду, блокувач жорсткого диску та/або набір дублікаторів, польовий комплект експерта криміналіста тощо.

Взагалі, перелік інструментарію залежить від конкретної ситуації. У цьому сенсі, в процесі його підбору, вельми корисними стають регулярно оновлюванні каталоги криміналістичних програмних та апаратно-програмних засобів. Наприклад, перелік криміналістичного програмного забезпечення, протестованого Американським інститутом стандартизації (NIST), можна зайти за адресою http://www.cftt.nist.gov [115].

Після підготовки відповідного інструментарію, який можна вважати підготовчим етапом огляду, проведення інших підготовчих заходів, працівники правоохоронного органу переходять до безпосередньо збирання даних на місці події. урахуванням вивчення сучасної зарубіжної та вітчизняної практики і критичного осмислення даного матеріалу сам алгоритм огляду ЕОМ у загальному вигляді можна представити як на рис. 1 [27].

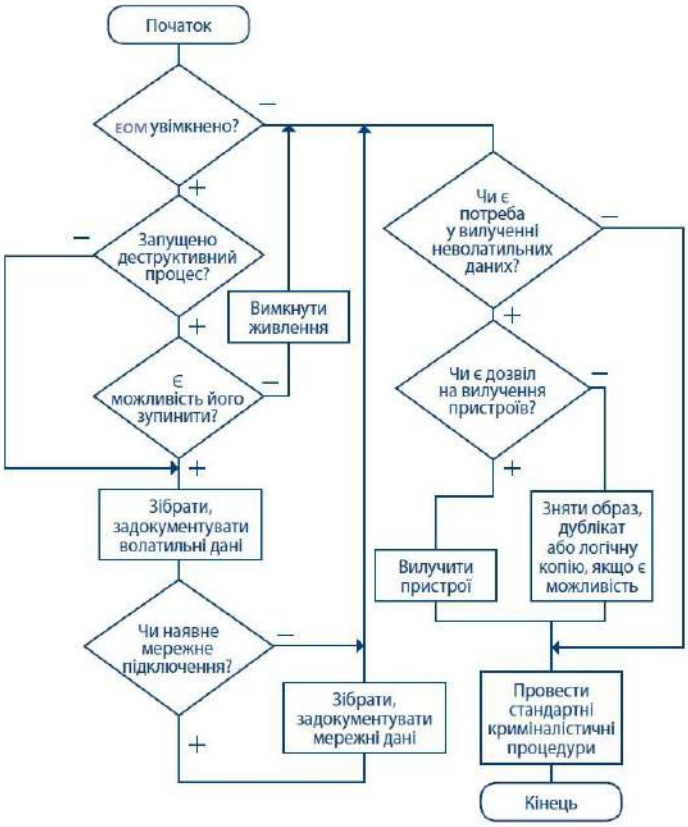

Рис. 1. Загальний алгоритм техніки огляду ЕОМ

Коментуючи окремі елементи цього алгоритму, потрібно зауважити, що на сьогодні в Україні практично не відбувається збирання та документування нестійких волатильних даних (зберігаються в енергозалежних запам’ятовувальних пристроях: оперативній пам’яті, кеші, регістрах), хоча саме волатильні дані часто містять ключі до різних крипто контейнерів, останні повідомлення у мережі та відкриті документи тощо. Так само потрібно звернути увагу на мережні технології віддаленого зберігання даних (хмари, термінали тощо).

Щодо копіювання неволатильних даних, то на теперішній час в світі застосовується три головних способи одержання копій цифрових носіїв, що містять слідову інформацію:

1) створення образу відповідного носія;

2) створення дублікату носія;

3) логічне копіювання окремих даних.

Перший спосіб є більш повільним, водночас за його допомогою працівник правоохоронних органів одразу одержує готовий для дослідження програмними

засобами матеріал, який можна достатньо легко тиражувати для здійснення розподіленого дослідження декількома фахівцями одночасно.

У будь-якому випадку для убезпечення електронних доказів рекомендується робити дві копії цифрового носія, одна з яких є контрольною (еталонною) та зберігається на випадок втрати або пошкодження іншої – робочої копії цифрового носія. Вилучені пристрої та носії потрібно належним чином зберігати та досліджувати. Наприклад, для дослідження мобільних пристроїв потрібно використовувати клітку Фарадея.

Перед зняттям копії більшості цифрових носіїв потрібно одержати геш-значення для вихідного носія інформації (джерела) за алгоритмом SHA-1, SHA-2 або SHA-3. Підрахунок гешу за допомогою алгоритму MD5 проводити не рекомендується, враховуючи можливості знаходження колізій з прийнятною обчислювальною складністю, що неодноразово демонструвалися дослідниками для цього алгоритму.

Слід пам’ятати, що особливості зберігання даних на окремих носіях (флеш-карти, SSD-вінчестери), а також вирівнювання ступеню їх зношеності, призводять до того, що по секторне геш-значення такого носія може не збігатися при наступному підрахунку. У цьому випадку можна говорити лише про можливість підтвердження геш-значеннями так званих «логічних» структур даних, наприклад, окремих файлів тощо.

Перед одержанням дублікату цифрового носія інформації (джерела) потрібно простерилізувати носій, на який будуть копіюватися відповідні дані (приймач). Цей носій, по перше, має бути за ємністю більшим від джерела, по друге, перед створенням дублікату його потрібно заздалегідь стерилізувати, тобто заповнити усі сектори нулями. Окремі дослідники пропонують лише частково стерилізувати носій вже після копіювання даних в частині, що незайнята скопійованими даними. Під час огляду стандартних ЕОМ провести процес стерилізації в операційній системі Windows можна, наприклад, за допомогою X-waysForensics (Winhex). У Linux аналогічна процедура може бути виконана командами:

fdisk –l # перегляд інформації про носії;

dd if=/dev/zero of=/dev/sd[a-z] bs 2048 # заповнення нулями відповідного носія;

killall -USR1 dd # перевірка стану роботи процесу dd (вводиться в іншому терміналі).

Підтвердити перед понятими, що диск є дійсно стерилізованим, можна:

1) в операційній системі Windows за допомогою підрахунку контрольної суми (Cheksum – логічнасума за допомогою операції «або») в програмі X-ways Forensics (Winhex);

2) у Linux з використанням команди пошуку ненульових значень:

grep -a –v ‘0’ /dev/sd[a-z]

у квадратних дужках вказано обрання відповідної літери для диску приймача [93, с. 111–112].

У загальному вигляді вилучені зразки комп’ютерної техніки передаються на дослідження експерту. Базовими нормативно-правовими актами щодо проведення таких експертиз є Закон України «Про судову експертизу» від 25.02.1994 [137], Інструкція про призначення та проведення судових експертиз та експертних досліджень, а також Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень, затверджені Наказом Міністерства юстиції України № 53/5 від 08.10.1998 [129].

Для дослідження інформації, що міститься на комп’ютерних носіях, експерту надається сам комп’ютерний носій, а за потреби комп’ютерний блок (комплекс комп’ютерних засобів, до складу якого входить досліджуваний носій). Для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях. Системні блоки персональних комп’ютерів надаються в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блока до мережі живлення [129].

В окремих випадках слідчий або оперативний працівник за його дорученням може самостійно провести огляд засобів комп’ютерної техніки зі складанням

протоколу огляду речей. У загальному вигляді такий огляд з урахуванням певних міркувань [94, с. 151–152] можна представити так:

1. Аналіз даних, одержаних з оперативних запам’ятовуючих областей, в тому числі буферу обміну

2. Аналіз залишкових слідів в елементах ОС, які вказують на дані, що оброблювались системою:

2.1. дослідження використовуваного програмного забезпечення;

2.2. дослідження елементів системних файлів;

2.3. дослідження та перевірка назв і реквізитів ярликів;

2.4. дослідження файлів історій відповідних програмних засобів;

2.5. дослідження налаштувань Інтернет-браузерів;

2.6. дослідження атрибутів та метаданих файлів, що викликали інтерес під час перевірки.

3. Аналіз безпосередньо файлів з даними, шляхом контекстного пошуку за ключовими фразами:

3.1. дослідження файлів, які зберігаються на цифрових носіях, зокрема:

3.1.1. пошук прихованих та зашифрованих даних;

3.1.2. пошук та перевірка тимчасових файлів;

3.1.3. аналіз специфічних даних, передбачених структурою файлової системи, наприклад, альтернативних потоків даних;

3.1.4. аналіз файлів, що пов’язані з мережною активністю;

3.2. відновлення з послідуючим аналізом видалених файлів, в тому числі:

3.2.1. дослідження залишків файлів в кластерах;

3.2.2. перевірка вільного простору носіїв інформації;

3.2.3. перевірка файлів підкачки, якщо вони мають місце.

Для аналізу зображень, які завантажено з мережних ресурсів, до проведення відповідної експертизи працівникам правоохоронних органів можна застосовувати відповідні сервіси, наприклад, безкоштовний сервіс imageforensic.org.

Завантаживши до нього відповідне зображення можна оперативно дізнатися важливі дані про нього які можуть вказати на особу автора зображення, дату його створення, програмне забезпечення, яке використовувалося для редагування, тощо.

Пошук і вилучення комп'ютерних даних в режимі реального часу

З огляду на важливість отримання волатильних або енергозалежних даних розглянемо цей процес більш детально. Якщо на місці огляду виявлено включені ЕОМ, то необхідно провести вилучення даних в режимі реального часу. Раніше в такій ситуації радили «витягнути шнур живлення із розетки», але вимикання живлення може призвести до втрати цінних для розслідування енергозалежних (волатильних) даних, розірвання віддалених з'єднань, блокування тимчасово розшифрованих і відкритих файлів, тому доцільно проводити збір даних в режимі реального часу.

Оскільки імовірність зміни і навіть перезапису джерел доказів дуже висока. то спеціаліст з криміналістичного аналізу «живих» даних або слідчий повинні мати:

– достатній рівень технічних знань і умінь;

– знання і досвід правильного застосування алгоритмів пошуку і вилучення із мінімальним впливом на систему;

– спеціальний набір перевірених криміналістичних інструментів.

Дуже важливим у процедурі пошуку і вилучення комп'ютерних даних в режимі реального часу є фіксація часу здійснення своїх дій. Якщо на місці огляду немає спеціаліста, то іноді буде кращим знеструмити систему і втратити енергозалежні дані, ніж спотворити джерела доказів, намагаючись їх вилучити із системи без відповідного досвіду і навичок.

Під терміном «енергозалежні дані» розуміються *цифрові дані, щодо яких існує дуже висока ймовірністьтого, що в короткий проміжок часу вони будуть видалені, перезаписані або змінені внаслідок людськогоабо автоматичного втручання.*

Енергозалежні дані дуже нестійкі у часі, і якщо їх не зберегти правильно і швидко, то вони можуть бути втрачені. В сучасних комп'ютерних системах дані часто зберігаються і обробляються не на самому пристрої, а в інших місцях (наприклад, хмарні сховища), доступ до яких регулюється законодавством тієї країни, де вони фізично розташовані.

Розрізняють такі види енергозалежних даних:

1. Енергозалежні дані комп'ютерної системи, наприклад, відкриті мережні з'єднання, запущені процеси, кеш ARP1 і кеш DNS2.

2. Тимчасові дані, які самі по собі не є енергозалежними, але доступ до них можна отримати тільки на місці огляду, наприклад зашифровані томи і віддалені ресурси. Якщо не отримати до них доступ підчас огляду, то вони можуть стати недоступними, зміненими або видаленими.

У енергозалежній пам'яті можуть знаходитися такі дані:

– процеси, що виконуються;

– сервіси, які запущені;

– системна інформація;

– дані про користувачів, які знаходяться в системі;

– логічні порти, що відкриті і прослуховуються;

– кеш ARP (протокол визначення адреси);

– кеш DNS (доменна системи імен);

– інформація про застосування, що автоматично запускаються;

– інформація з реєстру, яка не записана на диск;

– незбереженні документи;

– бінарні процеси і сервіси, в тому числі шкідливі програми, які зберігаються тільки в пам'яті.

Для збереження енергозалежних даних потрібно:

– визначити, вилучити, описати і сфотографувати кожен пристрій, що містить енергозалежні дані;

– ізолювати підозрюваних та інших сторонніх осіб від ЕОМ і не допустити, щоб вони змінили або знищили докази;

– спостерігати за складовими ЕОМ і запобігати будь-який автоматичній зміні або знищенню доказів.

Фізичний доступ

В процесі огляду часто складно визначити стан живлення комп'ютера(включений/виключений). Нижче наведено кілька додаткових порад на цей випадок:

– сфотографуйте комп'ютер, щоб зафіксувати його стан;

– прислухайтеся і придивіться до системи, щоб визначити, чи включений комп'ютер: це можна дізнатися по звуку працюючого вентилятора або обертів дисків, по палаючим світлодіодним індикаторам;

– посовайте мишкою, але не натискайте на кнопки;

– подивіться, чи виводиться на екран заставка або запит на введення логіна для входу в систему;

– сфотографуйте екран, щоб зафіксувати його стан після ваших маніпуляцій.

Якщо виявилося, що комп'ютер включений і на екрані видна заставка, то необхідно:

– спостерігати, що відбувається з екраном під час руху мишки;

– якщо заставка зникла і ви отримали доступ до системи безпаролю, то можна переходити до наступних кроків пошуку і вилучення даних в режимі реального часу (за умови, що у вас є необхідні знання та повноваження);

– якщо система вимагає введення пароля, то опитайте володільця системи; перевірте, чи відображається на екрані підказка паролю; пошукайте папірці з паролем або інші об'єкти, які допоможуть дізнатися пароль.

– якщо вдалося отримати пароль, то увійдіть в систему і переходьте до наступних кроків;

– якщо не вдалося отримати пароль, то існують спеціальні техніки отримання доступу до оперативної пам'яті через інтерфейси FireWire, Thunderbolt або шляхом «холодного перезавантаження» («cold boot»);

– у будь-якому випадку необхідно сфотографувати екран, щоб зафіксувати його стан.

Якщо комп’ютер увімкнений, але на екрані немає заставки/запиту на введення пароля або ж вдалося отримати пароль, то потрібно час від часу рухати мишкою (щоб не допустити активації заставки/блокування екрану) і візуально шукати ознаки:

– знищення даних: слова «delete» («знищити»), «format» («форматувати»), «remove» («видалити»), «copy» («копіювати»), «move» («перемістити»), «cut» («вирізати») або «wipe» («стерти»);

– шифрування;

– входу в систему з віддаленого комп’ютера або пристрою;

– використання хмарних сервісів;

– активного або нерозірваного сеансу спілкування з іншими користувачами або комп’ютерами (це може бути вікно чату або програми для обміну миттєвими повідомленнями);

– роботи камери або веб-камери;

– включених віртуальних машин (можливо в повноекранному режимі).

У будь-якому випадку сфотографуйте екран, щоб зафіксувати його стан.

При зборі комп’ютерних даних в режимі реального часу зміни в системі неминучі, проте потрібно намагатися отримати якомога більше енергозалежних даних, залишивши при цьому якомога менше слідів.

Важливе значення має також і те, в якому порядку здійснюється збір даних, тому необхідно ретельно обміркувати відповідний план дій, де рекомендується застосовувати методи, в основі яких лежить ступінь енергозалежності даних. Для цього доцільно використовувати вже готові сценарії збору даних в режимі реального часу, які можна адаптувати для кожного окремого випадку розслідування, наприклад, флешнакопичувач Microsoft COFEE (поширюється через Інтерпол) містить такі сценарії.

Різноманітні інструменти збору енергозалежних даних для ОС Windows містяться у безкоштовних пакетах:

– Sysinternals, https://docs.microsoft.com/uk-ua/sysinternals/;

– LiveGator (http://orionforensics.com/w_en_page/livegator.php);

– Redline (https://www.fireeye.com/services/freeware/redline.html);

– Win-UFO (http://www.caine-live.net/page2/page2.html);

– DART (http://na.mirror.garr.it/mirrors/deft/dart/DART_v2-2014.7z);

– OSForensics (http://www.osforensics.com/download.html),

а для ОС Linux у спеціальних Live-DVD дистрибутивах:

– Caine Live-DVD with Win-UFO, http://www.caine-live.net/;

– DEFT Live-DVD with DART, http://www.deftlinux.net//.

При виборі програм вилучення живих комп'ютерних даних необхідно враховувати наступне:

– віддавати перевагу програмам із мінімальним розміром файлів;

– програми повинні мати власні виконувані файли і не використовувати файли системи, що оглядається;

– вибирати програми із сценаріями автоматизації;

– бажано, щоб програми мали функцію сортування даних;

– програми повинні збирати виключно енергозалежні дані.

Зібрані енергозалежні дані слід зберігати на підготовлених стерилізованих (усі сектори перед форматуванням заповнюються нулями) зовнішніх носіях. При підготовці програм і пристроїв, які будуть використовуватися для вилучення живих комп'ютерних даних, доцільно виконати наступне:

– підготувати носії з достатнім місцем для запису даних в декількох форматах, наприклад, NTFS, EXT4;

– бути готовим працювати з різними операційними системами, наприклад, Windows, Mac і Linux;

– перевірити наявність працездатного носія із довіреними програмами збору живих даних таобчислити і зафіксувати для цих програм геш-значення за алгоритмом SHA-1 або SHA-2.

Разом із фіксацією енергозалежних даних працюючого комп'ютеру перевіряється наявність віддаленого доступу, при якому данні фізично

зберігаються в інших віддалених місцях. Наприклад, в організаціях дані користувача можуть розміщуватися (зберігатися) централізовано на одному загальному сервері, який забезпечує роботу всіх робочих станцій мережі. Зазвичай зупинити сервер великої організації і вилучити обладнання не представляється можливим внаслідок операційних обмежень або цивільно-правових ризиків. Як правило, дозвіл на обшук поширюється тільки на ті дані, які належать підозрюваному або до яких у нього є доступ, тому слідчий не має відповідних повноважень вилучити дані з усього сервера або загальної мережі.

У таких випадках для отримання доступу до інформації організації рекомендується під час обшуку організувати зустріч з її керівником, представниками юридичного та IT-департаменту, де обговорити детальний план співпраці між усіма сторонами процесу.

Комп'ютерні мережі в будинках/квартирах або в офісах малих/середніх компаній, як правило, складаються з декількох індивідуальних комп'ютерів, загального сервера, який містить: бази даних бухгалтерського програмного забезпечення, настройки мережних ресурсів, домашні каталоги користувачів, і іноді є поштові сервери. У подібній ситуації потрібно налагодити співпрацю із відповідальним за комп'ютерну інфраструктуру організації (якщо він не перейшов в статус підозрюваного).

Інформацію про конфігурацію мережі можна отримати із списків контролю доступу (ACL) або набору правил безпеки [104] маршрутизатора і брандмауера. Для цього потрібно знати логіни і паролі та через адміністративний доступ подивитися відповідні настройки конфігурації. Також конфігурацію мережі можна встановити за допомогою мережних утиліт Live-DVD криміналістичних дистрибутивів. Не зайвим буде намалювати схему мережної інфраструктури, що допоможе побачити зв'язки між досліджуваним комп'ютером і іншою мережею.

Ознаками віддаленого зберігання даних є:

– каталоги спільного доступ на інших комп'ютерах мережі;

– підключені мережні диски з сервера;

– електронні листи зберігаються на поштових серверах IMAP або Exchange Server);

– використовуються хмарні сервіси і хмарні сховища.

Каталоги зі спільним доступом і підключені мережні диски можна подивитися через провідник Windows або безкоштовні інструменти Share Enum від Sysinternals. При їх наявності потрібно створити образ (точна копія із видаленими файлами і зарезервованим простором) диску пам’яті віддаленого пристрою.

Факт віддаленого розташування електронних повідомлень на сервері IMAP [139] або Exchange Server, можна встановити шляхом аналізу параметрів облікових записів відповідних поштових клієнтів. Дані облікових записів POP3 (а іноді і облікових записів IMAP) зберігаються на комп’ютері користувача, не є енергозалежними та не вимагають вилучення в режимі реального часу. Якщо листи на комп’ютері користувача відсутні, то можна спробувати їх завантажити безпосередньо із сервера Exchange Server або попросити про це хостинг-провайдера облікового запису.

Хмарні технології. Важливою особливістю хмарних сервісів є те, що дані зберігаються на віддаленому сервері і часто навіть самому постачальнику хмарного сервісу не просто визначити їх конкретне місце розташування. Хмарні сервіси можуть замінити практично будь-який елемент корпоративної IT-інфраструктури – від текстових редакторів і бухгалтерських програм до повної заміни всіх робочих станцій.

Це означає, що в деяких випадках з офісного комп’ютера не вийде вилучити інформацію, оскільки він є«тонким клієнтом», тобто не має власного жорсткого диску пам’яті і використовує ресурси віртуальної машини хмари. У цій ситуації є свої переваги: технічно процес копіювання віртуальної машини провайдерах марного сервісу дуже простий, але можуть виникнути складнощі із отриманням дозволом на вилучення даних – це залежить від відповідного законодавства країни, де розміщуються дані. Крім того, може бути непросто довести, що процедура отримання даних не порушує законодавство запитуючої сторони.

Ще одна проблема полягає в тому, що дані можуть бути безповоротно втрачені, коли підозрюваний створив віртуальну машину спеціально для вчинення злочину, а після видалив її.

Якщо при огляді комп'ютеру, який має з'єднання із мережею, виникли підозри у використанні хмарних сервісів, то доцільно виконати наступні рекомендації:

– здійсніть пошук ярликів відомих сервісів хмарних технологій на панелі завдань;

– перевірте у настроюваннях системи встановлені програми хмарних сервісів;

– перегляньте назви хмарних сервісів в списку запущених процесів;

– здійсніть пошук загальних каталогів і підключених мережних дисків;

– за допомогою аналізатора протоколів пошукайте в мережі пакети хмарних сервісів;

– перевірте список відкритих портів на предмет підозрілої активності;

– скопіюйте всі дані із віддалених ресурсів незалежно від наявності можливої встановленої синхронізації даних із жорстким диском комп'ютера.

Після завершення вилучення енергозалежних і тимчасових даних потрібно:

– вийняти кабель живлення із пристрою (не із розетки, оскільки може бути встановлено джерело безперебійного живлення) і записати час, коли це було зроблено;

– при наявності підключених змінних носіїв пам'яті вийняти їх, запакувати і підписати;

– фізично від'єднати модем.

– у портативного комп'ютеру вийняти акумуляторну батарею живлення (іноді у відсіку DVD-приводу встановлюють додаткову батарею).

Огляд мобільних засобів комп'ютерної техніки із функцією телефону. Враховуючи широке використання засобів мобільного зв'язку і можливостей мобільних телефонів по зберіганню та обробці інформації все більш важливим завданням для правоохоронних органів стає аналіз вмісту мобільних телефонів

тих осіб, які підозрюються у вчиненні кримінальних правопорушень. Дійсно, адже сучасний мобільний телефон – це фактично маленький комп'ютер, який об'єднує в собі багато різних функцій, серед яких:

– телефонна та адресна книги;

– щоденник зі списком зустрічей і справ;

– пристрій для обміну повідомленнями (SMS, MMS, E-mail);

– записна книжка;

– диктофон;

– фотоапарат та відеокамера;

– програвач мультимедіа;

– і багато інших функцій, включаючи власне здійснення та отримання дзвінків.

Усі перераховані вище дані можуть містити або орієнтуючу інформацію для правоохоронних органів, або доказову інформацію та сліди, що можуть бути проаналізовані за наявності відповідного інструментарію.

Непоодинокими є випадки, коли за допомогою аналітичної обробки даних з мобільних пристроїв вдавалося розкривати неочевидні злочини або злочини минулих років, кількість яких з кожним роком невпинно збільшується.

Слід також зауважити, що зроблені за допомогою сучасних мобільних пристроїв (наприклад, iPhone) фотографії з працюючим функціоналом GPS нерідко містять в собі інформацію про координати місця фотографування, що дозволяє в окремих випадках з'ясувати місцезнаходження шуканої особи.

Більше того у практиці правоохоронних органів траплялися випадки, коли за локалізацією даних з мобільних апаратів вдавалося знаходити викрадене майно, відшукувати безвісти зниклих дітей.

Усе це дає підстави говорити про існуючу потребу більш інтенсивного використання спеціалізованого програмного забезпечення для аналізу інформації з мобільних пристроїв правоохоронними органами України.

Серед таких програм варто відзначити Mobile Phone Examiner Plus (MPE+), яка легко інтегрується з Forensic Toolkit (FTK), «Мобильный Криминалист» від

розробника ЗАТ «Оксиджен Софтвер», яка дозволяє серед іншого відновлювати окремі видалені повідомлення, MOBILedit! від розробника COMPELSON Labs, криміналістичний програмний продукт XRY шведської компанії Micro Systemation.

Здебільшого названі програмні продукти використовують у своїй діяльності експертні служби, але є потреба у їх засвоєнні не лише спеціалістами вузького профілю, але й більшістю слідчих та оперативних працівників [95, с. 143–145].

Огляд мобільних приладів має свої особливості. Найбільш складним елементом у цьому процесі є зняття дампу даних мобільного пристрою, оскільки для цього потрібно мати спеціальні права доступу до нього. Дамп, як правило, знімається програмним шляхом, проте окремі апаратно-програмні комплекси дозволяють проводити зняття фізичного дампу пристроїв безпосередньо з відповідних чіпів (наприклад, UFED, XRY). В окремих випадках корисну допомогу в дослідженні мобільних пристроїв можуть надати фахівці Європолу.

Вказана співпраця здійснюється в рамках Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 [176], ратифікованою відповідним Законом України № 2129-VIII від 12.07.2017. Серед іншого згідно зі ст. 18 вказаної Угоди Україна і Європол пропонують одна одному надання підтримки у створенні та функціонуванні спільних слідчих груп.

Проведення обшуку. При підготовці і проведенні обшуку [5, с. 44] приміщень де знаходиться комп’ютерна техніка, необхідно враховувати специфіку комп’ютерної інформації. Наведемо специфічні тактичні прийоми, врахування яких, на думку автора, забезпечує результативність пошуку і вилучення комп’ютерної інформації [167, с. 145].

Тактика пошуку інформації в комп’ютері полягає в правильному застосуванні криміналістичних прийомів її виявлення. Знання цих прийомів дасть змогу слідчому:

– уникнути знищення або пошкодження розшукуваної інформації;

– правильно зорієнтуватися в складному інформаційному масиві і знайти необхідне;

– правильно зафіксувати в криміналістичному та процесуальному плані вилучену інформацію.

На відміну від традиційних слідів злочину, природа комп'ютерної інформації вимагає шукати нові методи її збору. Сучасний розвиток електроніки дозволяє зберігати великі масиви інформації в незначних за об'ємом пристроях. Електронна сутність самої інформації ставить особливі вимоги до слідчого для підготовки і проведення слідчих дій.

На підготовчому етапі слідчому необхідно оцінити всю наявну інформацію про злочин, що розслідується. На необхідність вилучення криміналістично значущої комп'ютерної інформації можуть вказувати [32, с. 109]:

– вчинення комп'ютерного злочину;

– наявність у підозрюваного (обвинуваченого) в особистому користуванні комп'ютерної техніки;

– наявність у обвинуваченого (підозрюваного) спеціальної освіти в галузі обчислювальної техніки та програмування;

– наявність у потерпілого (в деяких випадках у свідків) спеціальної освіти в галузі обчислювальної техніки та програмування;

– наявність у матеріалах справи документів, що виготовлені машинним способом (відповіді на запити, довідки, які отримані від обвинуваченого або потерпілої сторони);

– викрадення носіїв комп'ютерної інформації;

– отримані під час вивчення особистості обвинуваченого відомості про його захоплення комп'ютерною технікою і програмуванням;

– обвинувачений або підозрюваний часто спілкується з особами «комп'ютерного» оточення та ін. Перелік наведених обставин може бути продовжений, оскільки вони настільки різноманітні, наскільки різноманітна вся людська діяльність. Оскільки комп'ютерна інформація може знаходитися (отже, і бути виявлена) в системному блоці комп'ютера, його конструктивних елементах,

периферійних пристроях та інших носіях комп'ютерної інформації, слідчий, готуючись до проведення слідчої дії, повинен враховувати цей факт.

Перед початком обшуку, в першу чергу, потрібно вжити заходи для запобігання можливого пошкодження або знищення інформації. Для цього необхідно:

– здійснити контроль за безперебійним електропостачанням ЕОМ для попередження випадкового вимкнення машини в момент огляду;

– заборонити торкатися до засобів обчислювальної техніки або до джерел її енергопостачання присутніх при проведенні обшуку осіб, у яких проводиться обшук, або повнолітніх членів їх сім'ї, чи представників організації (якщо обшук проводиться в приміщенні, яке вона займає);

– вилучити всіх сторонніх осіб із території, на якій проводиться обшук і припинити на неї доступ в подальшому;

– перевірити, чи знаходяться на об'єкті вибухові, легкозаймисті, їдкі речовини, сторонні джерела електромагнітного випромінювання та інші речовини і апаратура, які здатні призвести до пошкодження електронно-обчислювальної техніки; якщо так – евакуювати їх.

На стадії *підготовки до обшуку ще до виїзду на місце проведення*, потрібно вирішити організаційні питання. До початку проведення обшуку слід одержати достовірні дані такого змісту [58, с. 14]: марка та конфігурація ЕОМ; наявність локальної мережі або підключення комп'ютера до глобальної мережі Internet; яка кваліфікація користувачів ЕОМ в області програмування та обчислювальної техніки; з'ясувати, чи використовується пристрій автономного та безперебійного живлення і до яких наслідків може призвести вимкнення електроенергії; одержати характеристику колективу співробітників, які обслуговують обчислювальну техніку. Володіння такою інформацією дозволить слідчому вирішити основні завдання для збору доказової комп'ютерної інформації в процесі розслідування [1, с. 92].

Ще до виїзду на місце проведення обшуку потрібно підготувати відповідну комп'ютерну техніку, яка буде використовуватися для зчитування та вилучення

комп'ютерної інформації. Доцільно залучити спеціаліста з комп'ютерних систем (за освітою інженер-програміст, програміст-математик, інженер з технічної експлуатації та ремонту комп'ютерів). Знання спеціаліста будуть необхідні під час підготовки до обшуку, а також для оперативного аналізу інформації і кваліфікованого її вилучення.

Якщо були одержані відомості про те, що комп'ютери об'єднані в локальну мережу, необхідно встановити місце знаходження всіх засобів комп'ютерної техніки, які підключені до цієї мережі. При цьому обов'язково необхідно проводити груповий обшук одночасно у всіх приміщеннях, де встановлені ЕОМ.

Уважно слід поставитися до вирішення питання щодо залучення понятих [190, с. 18]. Насамперед, «обшук» комп'ютерної техніки, вимагає залучення як понятих осіб, які знайомі з роботою ЕОМ. Більшість програмістів вважають, що на сучасному рівні розвитку обчислювальної техніки без участі професіонала знайти «захована» в комп'ютері інформацію без ризику знищення її складно.

На попередній стадії обшуку необхідно відразу після входу в приміщення організувати охорону комп'ютерної техніки, не дозволяти нікому вимикати напругу, торкатися клавіатури, змінювати положення комп'ютера та іншого обладнання. Вимикання електроживлення з метою вилучення обладнання призведе до втрати часової пам'яті комп'ютера (RAM), а також може викликати ускладнення із запуском системи в майбутньому, тому що вона може бути захищена паролями на програмно-математичному чи електротехнічному рівні [70]. Якщо на момент проникнення до приміщення комп'ютер був увімкнений, то він має залишатися у такому стані до обстеження його спеціалістом. Усі спроби особи, яка обшукується, здійснити будь-які маніпуляції з комп'ютером необхідно розглядати як спробу знищення інформації в ЕОМ, і це бажано відтворити в протоколі обшуку.

На оглядовій стадії обшуку необхідно з'ясувати. чи під'єднаний комп'ютер до телефонної мережі за допомогою модему, встановити, чи має місце з'єднання

комп’ютера з обладнанням або обчислювальною технікою за межами цього приміщення.

Зазначимо, що час знищення всієї інформації залежить від типу комп’ютера і може коливатися від кількох секунд до десятків хвилин. З огляду на це важливо, щоб власник комп’ютера не запідозрив у тому, що заплановано обшук, а під час проведення цієї слідчої дії не працював за комп’ютером. Обшук доцільно здійснювати в той момент, коли відсутній оператор ЕОМ. Найбільш вдалими є ранкові години – з 6 до 8. За певних обставин обшук можна провести в нічний час, про що необхідно зазначити в постанові.

Після прибуття на місце проведення обшуку необхідно відразу і швидко ввійти до приміщення, тим самим запобігти знищення інформації в комп’ютері. Якщо є потреба і змога, безпосередньо перед входом до приміщення необхідно відключити електроенергію. Але необхідно мати на увазі, що така дія в одному випадку може призвести до вимкнення всієї апаратури, яка є у приміщенні, а в іншому – до пошкодження апаратури та знищення інформації, яка знаходиться в ОЗП комп’ютерів. Відключення електроенергії потрібно проводити зважено й обережно, тому що здійснення цієї операції виправдано за умови, якщо обшук відбувається в будинку, що стоїть осторонь, має велику площу (через що неможливо провести обшук в усіх приміщеннях одночасно) і велику кількість комп’ютерної техніки, яка містить значний обсяг інформації, що цікавить слідство.

Після входу в приміщення на початковому етапі обшуку слід організувати охорону комп’ютерів, які мають важливе значення для слідства. Доступ до комп’ютерів для присутніх у приміщенні має бути обмеженим. Необхідно пам’ятати, що не лише робота за клавіатурою, але й вимкнення-ввімкнення комп’ютера може призвести до зміни і знищення інформації. Тому, якщо в момент проникнення до приміщення комп’ютер був ввімкнений, він має перебувати в цьому стані до того часу, доки його не обстежить спеціаліст. Власника приміщення або оператора ЕОМ не варто допускати до комп’ютера і клавіатури навіть у випадках згоди особи, яка обшукується добровільно видати

інформацію. Усю роботу на комп'ютері повинен виконувати спеціаліст. Спроби особи, яка обшукується, здійснити будь-які маніпуляції з комп'ютером або клавіатурою, зокрема ввімкнення або вимкнення комп'ютера, потрібно розглядати як спробу знищення інформації в ЕОМ, про що бажано зазначити у протоколі обшуку.

На оглядовому етапі обшуку необхідно встановити: чи підключені комп'ютери, які знаходяться в приміщенні, до локальної мережі; чи є вихід до глобальної або регіональної мережі; чи сполучено комп'ютер з обладнанням або обчислювальною технікою поза межами обшукуваного приміщення; чи підключено комп'ютер до телефонної або телетайпної лінії; яке зображення на екрані монітора; чи працюють у цей момент програми на ЕОМ і які саме та ін.

Реалізація визначених завдань передбачає вивчення на екрані монітора зображення і, якщо є можливість, докладний опис його в протоколі. Ознакою того, що комп'ютер знаходиться не в очікувальному режимі введення наступної команди, а виконує раніше задані команди, може бути:

– повідомлення на екрані, яке визначає дію програми, виділення кольором або яскравістю фрази «...іде тестування...» або пункту меню;

– спеціальне зображення на екрані, яке може змінюватися (рухливий рядок, знак);

– мерехтіння індикатора звернення до жорсткого диску, CD-Rom, гнучких дисків (подібний індикатор завжди є на передній панелі системного блока, і його ввімкнення або мерехтливий стан свідчить про те, що йде обмін інформації з носієм), характерне потріскування та шелестіння CD-Rom і магнітних носіїв [32, с. 109].

Детальний етап обшуку найбільш трудомісткий і вимагає високої кваліфікації як спеціаліста з комп'ютерних систем, так і всієї слідчо-оперативної групи. Крім спеціальних операцій із комп'ютером, на цьому етапі передбачено чітку організацію пошукових заходів, спрямованих на пошук схованок, де можуть бути приховані документи і предмети. Такою схованкою може бути і сам комп'ютер, зокрема системний блок.

Не варто обмежуватися пошуком інформації тільки в комп'ютері. Слід уважно оглянути наявну в приміщенні документацію, записи навіть на клаптиках паперу можуть мати значення для вдалого досягнення мети. Це необхідно зробити через те, що програмісти часто не розраховують на свою пам'ять і залишають записи про паролі, електронні ключі, зміни конфігурації системи, особливості побудови інформаційної бази комп'ютера. Багато користувачів зберігають копії своїх файлів на дискетах для запобігання втрати їх при виході комп'ютера із ладу. Тому виявлення будь-яких носіїв інформації повинно спонукати слідчого для їх вилучення, вивчення та використання.

Пошук необхідної інформації у комп'ютерних системах може зайняти кілька годин або й кілька днів. У разі, коли систему неможливо фізично вилучити і перемістити в інше місце, виникає необхідність скопіювати інформацію та комп'ютерні програми на магнітні носії (зробити повні копії окремих машин або окремих дисків тощо). Тому для пошуку і копіювання інформації необхідно зарезервувати час [70, с. 185].

Найбільший інтерес завжди викликає системний блок [73, 29–40]. Він має певну конструкцію, специфіка якої надає можливість утворювати схованки. По-перше, всередині системного блока достатньо вільного місця. Комп'ютери побудовано за модульним принципом, тобто їх складено з окремих плат, а кожну окрему конфігурацію зібрано залежно від певного користувача. Усередині корпусу зарезервовано місце для розширення і нарощення можливостей комп'ютера шляхом установки на материнській платі додаткових плат. Це й зумовлює існування додаткового простору всередині корпусу системного блока комп'ютера.

По-друге, системний блок комп'ютера, завдяки його модульній побудові, пристосований до швидкого монтажу і демонтажу без залучення будь-яких додаткових пристроїв (викрутки, гайкових ключів тощо), що сприяє безслідному доступу до вузлів комп'ютера.

По-третє, в комп'ютері використано електронні схеми з малою напругою, яка є безпечною для життя людини. Блок живлення, який завжди вміщено в

захисний кожух, має напругу 220 вольт, а живлення, яке подається на плати, не перевищує 12 вольт, що надає можливість демонтувати корпус системного блока без відключення його від електромережі.

По-четверте, найбільшу плату системного блока – так звану материнську плату – прикріплено затискачами до стінок або низу корпусу, між якими лишається достатньо простору для збереження документів. Для спеціалістів доступ до подібної «схованки» не викликає ніяких ускладнень.

Більшу частину інформації, яку збережено й оброблено в комп'ютері, завжди можна скопіювати на переносні носії інформації: магнітні дискети, СД-диски, магнітні стрічки та переносні вінчестери. Пошук таких носіїв необхідний та обов'язковий. Через те, що дискети мають порівняно малі розміри – до 150 мм в діаметрі й 2 мм в товщину, пошук їх значно ускладнюється. Якщо спеціаліст не має змоги перевірити дискети на місці, їх слід вилучити, дотримуючись усіх процесуальних норм, для подальшого дослідження. Пошук схованок із магнітними носіями (дискетами, стрічками) ускладнено тим, що в ньому не можливо застосовувати металошукач або рентгенівську установку, оскільки це може призвести до знищення інформації. Тому для запобігання випадкового знищення інформації, магнітні носії, зазвичай, зберігаються в захищених металевих коробках.

Якщо до початку обшуку комп'ютер був увімкнений, то на магнітні носії необхідно скопіювати програми та файли даних, які збережено на віртуальному диску [32, с. 109]. Не завжди можливим є терміновий аналіз великого об'єму інформації, яка знаходиться в комп'ютері, тому її слід вилучити для подальшого дослідження, записавши на комп'ютер, який належить оперативно-слідчій групі. Копіювання цієї інформації здійснюється на вбудований у комп'ютері жорсткий диск (вінчестер) або Noote Book. Необхідну інформацію також можна скопіювати на магнітну стрічку за допомогою стримера, який застосовують у тому випадку, коли в обшукуваному приміщенні знаходиться декілька комп'ютерів і для збереження інформації з кожного із них використовують окрему стрічку. Використання стримера можливе лише в момент роботи комп'ютера, з якого

відбувається копіювання [191, с. 22–23]. Якщо у розпорядженні оперативно-слідчої групи немає переносного персонального комп'ютера або стримера, то в цьому випадку достатньо вилучити жорсткий диск (або дискети, якщо їх декілька) з виявленого комп'ютера, дотримуючись усіх процесуальних норм. Бажано момент вилучення жорсткого диску записати на відео. Відсутність у складі оперативно-слідчої групи спеціалістів із комп'ютерної техніки, які здатні кваліфіковано провести демонтаж жорсткого диску, зумовлює вилучення всього системного блока комп'ютера для виявлення та дослідження інформації.

Для лазерного або струйного принтера подібний аналіз майже неможливий [190, с. 27]. В окремих випадках можливе вилучення принтера, хоча ідентифікувати інформацію, надруковану на ньому, за залишеними слідами надто складно порівняно з друкарською машинкою, навіть якщо це буде матричний принтер.

Якщо в приміщенні, яке підлягає обстеженню, знаходиться невелика кількість комп'ютерів або серед спеціалістів виник сумнів щодо можливості дослідження комп'ютерної інформації після вилучення лише системних блоків, то доцільно вилучити всі комп'ютери. Для цього необхідно: попередньо знеструмити їх, упакувати кожен пристрій та з'єднувальні кабелі окремо. Незважаючи на високу вартість комп'ютерів, на більшості із них відсутні заводські або серійні номери, що значно ускладнює їх пошук та ідентифікацію. Відповідний номер завжди є на жорсткому диску, дисководах, магнітних носіях і материнській платі. Оскільки ці вузли є основними з погляду конструювання і найдорожчими з погляду вартості, то ідентифікацію комп'ютерів можна проводити за ними.

У ході обшуку слід звертати увагу на літературу, методичні матеріали про комп'ютерну техніку та програмування. Для проведення обшуку та подальшого огляду речових доказів доцільно залучати спеціаліста, який володіє знаннями і може прочитати інформацію, що міститься на машинних носіях або у пам'яті вилученого комп'ютера, а також певних записів на паперових носіях інформації [70].

Таким чином, наявність і використання оперативної інформації часто може відіграти вирішальну роль у пошуку комп'ютера. Однак успішне подолання системи захисту не вирішує всіх проблем збирання доказів в комп'ютері. Тактичні особливості пошуку комп'ютерної інформації залежать також від функціонального стану комп'ютера та його периферійних пристроїв у момент огляду. Інформацію може бути зафіксовано на постійному носії або збережено в комп'ютері лише на період роботи останньої, тому слідчому необхідно застосовувати різні тактичні прийоми пошуку залежно від того, чи комп'ютер працює в момент початку слідчої дії, чи відключений.

Задіяні для пошуку інформації програми, які не знаходяться в комп'ютері, але використовуються слідчим повинні бути стандартними і про це необхідно відмітити в протоколі обшуку. Якщо для пошуку інформації слідчим були задіяні програмні продукти, які не знаходяться в комп'ютері, про це необхідно також відмітити в протоколі. Такі програми повинні бути стандартними (не змінені самостійно з метою їх вдосконалення), ліцензованими. Контроль за їх роботою повинен бути наочним, тобто всі ключові етапи роботи програми повинні бути зображені на екрані дисплея, і слідчий або спеціаліст повинен коментувати подію [191, с. 22–23]. Максимально активна участь понятих при пошуку інформації важлива ще й тому, що результатом виконання пошукової програми може бути не тільки текстовий або графічний документ, а і аудіо- чи відео-ролик (вербальна або візуальна інформація), документ-презентація, подібний до програми Microsoft PowerPoint та інші нестандартні ситуації. Такий підсумок роботи програми може бути унікальним (неповторним) і зафіксувати таку інформацію можна тільки склавши відповідний протокол (не враховуючи фото -, відео-фіксації). В разі виявлення пошукової інформації, поточне зображення екрану дисплея також необхідно сфотографувати, після чого стандартними засобами переписати інформацію на постійний носій (як правило – це переносний вінчестер чи магнітний диск) або роздрукувати її.

Успіх розслідування кримінальних проваджень про злочини вказаного виду багато в чому залежить від правильної фіксації та вилучення виявлених слідів

злочинної діяльності в процесуальному та криміналістичному плані. Оскільки процесуальний закон основним засобом фіксації визначає протокол слідчої дії, слідчий повинен описати основні фізичні характеристики вилучених пристроїв, магнітних та інших постійних носіїв інформації, серійні номери апаратури, їх видимі індивідуальні ознаки. Якщо одержана машинна роздруківка, то вона повинна оформлятися як додаток до протоколу – підписуватися учасниками слідчої дії. Необхідно вказати тип і вид друкуючого пристрою, а також програмні засоби, за допомогою яких вона виконана. Якщо присутні при проведенні слідчої дії особи (підозрювані, обвинувачені, свідки) наполягають на відтворенні в протоколі конкретних характеристик вилучених апаратних засобів та інформаційної бази, «ці відомості можуть бути записані лише як окремі заяви, тому що фактичні параметри можуть виявитися іншими» [59, с. 23].

На заключному етапі обшуку потрібно скласти протокол, опис до нього, плани та схеми приміщень, а також провести додаткове фотографування та відеозапис.

Проведення допиту. Допит – це слідча (розшукова) дія, змістом якої є отримання та фіксування у встановленій кримінальним процесуальним законом формі показань підозрюваного, обвинуваченого, свідка, потерпілого, експерта, що містять відомості про відомі їм обставини, які мають значення для кримінального провадження [56].

За своєю сутністю допит – це процесуальна дія, яка являє собою регламентований кримінальними процесуальними нормами інформаційно-психологічний процес спілкування осіб, які беруть у ньому участь, та спрямований на отримання інформації про відомі допитуваному факти, що мають значення для встановлення істини [188, с. 265]. Це процес обміну інформацією, процес взаємодії, взаємного сприйняття учасників [187, с. 14].

Допит є не лише однією із найбільш ефективних і поширених слідчих (розшукових) дій, а й фактично виступає необхідною та обов’язковою слідчою (розшуковою) дією у кожному кримінальному провадженні, оскільки є єдиним засобом формування джерела доказів – показання. Таким чином, жодне

кримінальне провадження не здійснюється без проведення допитів, у тому числі під час досудового розслідування. Будучи найбільш поширеною слідчою (розшуковою) дією, допит слугує не лише ефективним засобом збирання доказів, а й виступає засобом перевірки вже зібраних доказів. Так, у тому числі, за допомогою відомостей, одержаних під час допиту, слідчий встановлює наявність чи відсутність події кримінального правопорушення, винуватості особи у його вчиненні та інших обставин предмета доказування (ст. 91 КПК України) [56].

Слід особливо відзначити, що підготовка до проведення допиту має свої особливості і певну специфіку, не враховуючи які, слідчий зіткнеться з низкою труднощів і не матиме можливості результативно провести зазначені слідчі (розшукові) дії. Тактика проведення допиту у кримінальних провадженнях цієї категорії безпосередньо залежить від специфіки механізму здійснення кіберзлочинів і інших як позитивних, так і негативних факторів. Слід враховувати, що допит потерпілих і свідків у кримінальних провадженнях цієї категорії буде відрізнятися від допиту підозрюваних і обвинувачуваних, а особливості, пов'язані з механізмом злочину впливають на вибір тактичних прийомів допиту.

Так, аналіз практики розслідування кримінальних проваджень з кіберзлочинів і результати проведеного опитування слідчих показали, що при проведенні допиту і очної ставки у слідчих часто виникають різного роду труднощі. Наприклад, основні труднощі з якими їм доводилося стикатися в ході розслідування кіберзлочинів, пов'язані з термінологією (87%), вибором тактичних прийомів (24%), встановленням психологічного контакту (17%), інші проблеми (4%).

Готуючись до проведення допиту підозрюваного слідчий має визначити, визначити предмет допиту; сформулювати запитання та визначити порядок їх послідовності; визначити, які докази та матеріали можуть бути використаними під час допиту для викриття підозрюваного; визначити послідовність проведення допитів при наявності кількох підозрюваних. Допит підозрюваного проводиться з використанням тактичних прийомів, які застосовуються під час допиту

обвинуваченого [6, с. 37]. Тактика допиту залежить від моменту проведення допиту та обсягу інформації, якою володіє слідчий.

Підозрюваних осіб рекомендується шукати серед працівників організації, що зазнала несанкціонованого проникнення до автоматизованої системи та комп'ютерної мережі, а саме: технічного персоналу організації; розробників відповідних систем; керівного складу організації; операторів, адміністраторів автоматизованої системи; програмістів, інженерів зв'язку; фахівців із захисту інформації; охоронців; інших осіб, які мають доступ до комп'ютерної мережі та автоматизованої системи [56, с. 57].

При допиті особи, що є підозрюваною [82, с. 250–252], слід з'ясувати: 1) місце помешкання, роботи підозрюваного або навчання та його професію; 2) сферу інтересів, звички, схильності, а також коло знайомих; 3) який рівень його професійної підготовленості; 4) до якої комп'ютерної інформації мав доступ, які операції з інформацією він мав право проводити; 5) які взаємостосунки із співробітниками; 6) який спосіб життя вів підозрюваний; 7) хто його навчив працювати з конкретним програмним забезпеченням; 8) досвід роботи у створенні комп'ютерних програм певного класу конкретною мовою програмування та які мови програмування знає підозрюваний; 9) що відомо йому про вірусні комп'ютерні програми та інші шкідливі програми; 10) які ідентифікаційні коди і паролі закріплені за підозрюваним, включаючи і комп'ютерну мережу; 11) до яких видів програмного забезпечення має доступ підозрюваний; яке джерело походження цих видів програмного забезпечення; 12) яким чином підозрюваному вдалося проникнути до автоматизованої системи та комп'ютерної мережі; 13) яким чином підозрюваний дізнався про пароль (код) доступу до інформації; 14) чи відомі підозрюваному випадки незаконного втручання в роботу комп'ютера, системи та незаконного підключення до комп'ютерної мережі; 15) чи був обмежений доступ підозрюваного в приміщення, де встановлена комп'ютерна техніка і яка саме; 16) чи був ознайомлений він з умовами роботи з інформацією та інструкціями про порядок проведення регламентних робіт; 17) чи були випадки порушення підозрюваним правил внутрішнього розпорядку, а також порядку

виконання робіт та доступу до комп'ютерної інформації; 18) чи надходили до підозрюваного пропозиції про передачу комп'ютерної інформації, програмного забезпечення від інших осіб; 19) чи відомі підозрюваному особи, які виявляли зацікавленість до отримання ідентифікаційних кодів, паролів; 20) які навички має підозрюваний з основ програмування, ремонту та експлуатації засобів обчислювальної техніки; які мови програмування він знає; 21) чи вдавалося підозрюваному підбирати електронні ключі доступу до автоматизованої системи; 22) чи відомі йому спеціальні апаратні та програмні засоби, які дають можливість відключити технічні і програмні засоби захисту автоматизованої системи; 23) чи використовувався комп'ютер та програмне забезпечення лише за призначенням; 24) чи регулярно застосовувалися ефективні антивірусні комп'ютерні засоби; 25) чи користувалися нелегальними (не ліцензійними) копіями комп'ютерних програм; 26) чи відомий підозрюваному алгоритм функціонування вірусної комп'ютерної програми; 27) на яку інформацію та яким чином впливає шкідлива комп'ютерна програма чи технічний засіб та ін.

Видається правомірним зазначити, що на першому допиті підозрюваний може пояснювати факт незаконного проникнення до комп'ютерів, систем та комп'ютерних мереж некримінальними причинами або розповідати про незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж як про факт, що був здійснений за відсутності злочинного умислу. Позитивні наслідки у викритті таких осіб спричинені точністю використання одержаної під час проведення оперативно-розшукових заходів інформації про злочинну діяльність цієї особи, а також пред'явленням предметів і документів, що належать підозрюваному і які використовувалися для незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж.

Допит свідків. Приймаючи рішення про допит певної особи як свідка, слідчий повинен прогнозувати, яку інформацію він може одержати від допитуваної особи [6, с. 37]. Орієнтуючись на це необхідно продумувати комплекс постановки питань. Особливість цієї слідчої дії полягає, насамперед, у предметі допиту, колі осіб, які можуть бути свідками, у способах їх виявлення,

послідовності проведення допиту. Специфічність допиту обумовлена обстановкою вчинення злочину, функціями певних осіб, яких допитують в кримінальному провадженні як свідків [174].

Свідками у розслідуванні незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж можуть бути особи, які спостерігали події злочину (особливо при безпосередньому доступі) або його окремі моменти, а також бачили злочинців в момент скоєння злочину або після того. При проведенні допиту свідків на подальшому етапі розслідування незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж необхідно деталізувати раніше встановлені обставини або з'ясувати факти, які стали відомі при проведенні інших слідчих дій. На допиті свідків перелік питань може бути змінено залежно від особи допитуваного і способу скоєння злочину. Разом із тим у процесі допиту свідків необхідно обов'язково з'ясувати:

– як здійснювався законний доступ до ресурсів ЕОМ, систем та комп'ютерних мереж;

– як міг бути здійснений незаконний доступ до комп'ютерних систем;

– як організовано інженерно-технічний (апаратний) захист автоматизованих систем;

– чи має автоматизована система технологічний зв'язок із іншими мережами; якщо так, то яким чином (система кодів, паролів тощо);

– чи перебували в приміщенні, де знаходиться комп'ютерна техніка, сторонні особи;

– чи зафіксовано випадки роботи співробітників з інформацією, яка не належить до їх компетенції;

– чи були збої в роботі програми, крадіжки носіїв інформації або окремих комп'ютерних пристроїв;

– чи зафіксовано збої в роботі комп'ютерного обладнання, електронних мереж, засобів захисту комп'ютерної інформації;

– хто із співробітників працював у позаурочний час;

– хто цікавився інформацією, яка не стосується його безпосередньої діяльності;

– чи були зафіксовані останнім часом випадки спрацьовування засобів захисту комп'ютерної інформації;

– як часто запускаються антивірусні програми, які результати останніх перевірок;

– як здійснювався доступ до кодів, паролів;

– як організовано антивірусний захист;

– як часто оновлюється програмне забезпечення;

– у який спосіб ведеться облік користувачів комп'ютерних мереж;

– як здійснюється режим доступу персоналу та інших осіб до приміщення;

– яким шляхом придбано комп'ютерну техніку, як проводиться її ремонт та модернізація;

– як на підприємстві, в установі, організації здійснюється робота з інформацією, які шляхи і способи надходження інформації, її обробки та передачі через канали зв'язку;

– у який спосіб міг бути здійснений незаконний доступ до інформації;

– хто є абонентом комп'ютерної мережі, до якої підключені комп'ютери цього підприємства, установи, організації; як здійснюється доступ до мережі;

– хто із користувачів має право на роботу в мережі та ін.

У випадках, коли допитуваний свідок володіє інформацією про факти незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж, доцільно з'ясувати: 1) що відомо про ці факти; 2) чи траплялися раніше і як часто подібні факти на цьому підприємстві, в установі, організації раніше; 3) чи відомі свідкові випадки незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж; якщо так, то за яких обставин їх було скоєно; 4) де під час незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж знаходився свідок; 5) які підстави має свідок вважати, що інформацію скопіював (заблокував, знищив) саме цей підозрюваний,

а не хтось інший; 6) чи могло знищення або перекручення інформації, а також неполадки у роботі ЕОМ, систем ЕОМ або збоїв програмного забезпечення і под. бути наслідком дії іншої особи; 7) з якими особами підозрюваний зустрічався останнім часом, про що вів розмову, які проблеми обговорював; 8) які стосунки у свідка з підозрюваним; 9) чи розповідав підозрюваний про те, хто запропонував йому (у зв'язку з чим у підозрюваного виникло бажання) здійснити незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж; 10) чи здогадувався свідок, яку мету переслідував підозрюваний, коли вчиняв незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж; 11) чи є незаконне втручання підозрюваного в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж підготовкою до скоєння іншого злочину (якого саме, і що відомо про це свідкові); 12) чи міг підозрюваний скористатися своїм службовим становищем для скоєння злочину; 13) які особи мали доступ до інформації, скопійованої (знищеної, заблокованої, перекрученої) підозрюваним; 14) чи можливе вчинення цього злочину однією особою і що для цього потрібно; 15) які особи спроможні надати безпосередню допомогу в незаконному втручанні в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж, а також у реалізації злочинних намірів; 16) кому можуть бути вигідними дії підозрюваного; 17) як виглядає інформація після дій підозрюваного; 18) хто постраждав від дій підозрюваного; 19) хто є власником інформації, скопійованої (знищеної, перекрученої) підозрюваним; 20) чи можливе вчинення подібних дій внаслідок необережної поведінки особи тощо.

На подальшому етапі розслідування незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж виникає необхідність допитати в ролі свідків осіб різних категорій, кожна з яких має свою специфіку. Зокрема, при проведенні допиту операторів ЕОМ необхідно дізнатися про:

– правила ведення операторами журналів, порядок прийому-здачі змін, режим роботи операторів;

– правила експлуатації, зберігання, знищення комп'ютерних роздруківок (листингів) та про категорію осіб, які мають доступ до останніх;

– умови доступу до приміщення, де знаходиться комп’ютерна техніка, та про категорію осіб, які працювали на ній;

– спосіб проведення обліку користувачів комп’ютерної системи тощо.

Також, у процесі допиту програмістів необхідно з’ясувати наступне:

– перелік програмного забезпечення, яке використовується, та його класифікація (ліцензійне, особисте, піратське);

– паролі захисту програм та окремих пристроїв комп’ютера;

– технічні характеристики локальної мережі (якщо вона є), і хто виконує роль її адміністратора;

– порядок придбання програмного забезпечення, його супроводу;

– існування ідентифікаційних програм, наявність у робочих програмах спеціальних файлів-протоколів, що реєструють порядок входження в комп’ютер користувачів, зміст цих файлів;

– чи були написані нові програми і яке їх призначення тощо.

У співробітника, який є відповідальним за інформаційну безпеку, або в адміністратора комп’ютерної мережі (за умови наявності останньої) слідчий з’ясовує: наявність спеціальних технічних засобів для захисту інформації; розпорядок доступу користувачів до комп’ютерної мережі; порядок ідентифікації користувачів комп’ютерів; розпорядок робочого дня користувачів комп’ютерної мережі; порядок доступу співробітників до комп’ютерної техніки поза робочим часом; порядок присвоєння і зміни паролів користувачів; характеристика заходів щодо захисту інформації тощо.

Співробітники, які здійснюють технічне обслуговування обчислювальної техніки, мають надати, якщо це можливо, інформацію про: перелік і технічні характеристики засобів комп’ютерної техніки, що використовується в організації, а також перелік захисних технічних засобів; книгу паролів для доступу до автоматизованої системи; періодичність технічного обслуговування, проведення профілактичних і ремонтних робіт; законність використання того чи іншого програмного забезпечення або технічного засобу; випадки виходу апаратури з

ладу; випадки незаконного підключення до телефонних ліній зв'язку, установки будь-якого додаткового електрообладнання тощо.

Слідчий з'ясовує у начальника обчислювального центра або керівника підприємства, установи, організації як свідка наступну інформацію: чи сертифіковані програми системного забезпечення; яка організаційна структура обчислювального центру; чи діють відомчі правила експлуатації ЕОМ та мережі (локальної, регіональної та віддаленої), який порядок ознайомлення з ними, і як здійснюється контроль за використанням ЕОМ та мережі; яких працівників було звільнено протягом останнього часу і які мотиви їх звільнення; чи були випадки незаконного проникнення в приміщення, де знаходиться комп'ютерна техніка, раніше тощо.

Результати проведеного дослідження показали, що наведені слідчі (розшукові) дії викликають велику складність у роботі практичних працівників, які займаються розслідуванням таких злочинів. Визначені специфічні особливості тактики проведення окремих слідчих дій (огляд місця події, допит свідків, обшуки приміщень, допит підозрюваних) у розслідуванні злочинів цього виду дають можливість підвищити рівень, якість, ефективність розслідування, а також одержати великий об'єм доказової інформації. Також необхідно зазначити, що розробка тактичних особливостей проведення окремих слідчих дій при розслідуванні незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж вимагає подальшого активного наукового дослідження.

Особливістю розслідування злочинів даної категорії є обов'язкове залучення як спеціаліста фахівця (фахівців) у галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку й використання ним, за необхідності, спеціальних техніко-криміналістичних засобів, що загалом обумовлено специфікою виявлення, фіксації та вилучення електронних слідів злочину (опис у протоколі процесуальної дії, фото-, відеофіксація, копіювання на зовнішній носій інформації), а також у деяких випадках прямим згадуванням на це у КПК України (ч. 2 ст. 168). Залежно від конкретної ситуації, це може бути як судовий експерт за

напрямом комп'ютерно-технічної та (або) телекомунікаційної експертизи, так й інші особи, які володіють відповідними спеціальними знаннями та навичками використання техніко-криміналістичних засобів, наприклад, фахівець з експлуатації або створення конкретних програмних засобів або ж з технічної експлуатації і ремонту певного обладнання. Така участь працівників Експертної служби МВС України має бути нормативно врегульована на відомчому рівні (наказ МВС України від 03 листопада 2015 р. № 1339) з обов'язковим залученням комп'ютерно-технічної лабораторії у складі спеціалізованої пересувної лабораторії та спеціалістів відповідного профілю до участі у проведенні оглядів місць подій. За необхідності залучення фахівців недержавних підприємств, установ та організацій таке залучення має бути заздалегідь узгоджено та організовано. У зв'язку із зазначеним, важливим елементом у проведенні слідчих (розшукових) дій є їх підготовчий етап, який дозволяє забезпечити участь потрібного фахівця та наявність необхідних технічних засобів.

2.3. Особливості застосування техніко-криміналістичних засобів при проведенні окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

У науці кримінального процесуального права під негласними слідчими (розшуковими) діями розуміють заходи, що складаються з сукупності пошуково-розшукових, пізнавальних та посвідчувальних прийомів, відомості про факт та методи проведення яких не підлягають розголошенню, проводяться уповноваженим кримінальним процесуальним законом суб'єктом з метою виявлення й закріплення фактичних даних та їх джерел для отримання доказів у кримінальному провадженні та їх перевірки.

Оскільки негласні слідчі (розшукові) дії є різновидом слідчих(розшукових) дій, то їх сутнісні ознаки є тотожними, а саме: негласні слідчі(розшукові) дії є частиною процесуальних дій, що мають пошуково-розшуковий, пізнавальний та посвідчувальний характер; їх проведення передбачене та регламентоване нормами КПК; вони можуть проводитися лише уповноваженими суб'єктами; їх хід та результати фіксуються у відповідних процесуальних документах; вони проводяться з метою виявлення й закріплення фактичних даних і відомостей про їх джерела для отримання доказів у кримінальному провадженні або перевірки цих доказів [155, с. 208].

Видами негласних слідчих (розшукових) дій є: а) аудіо-, відео контроль особи (ст. 260 КПК України); б) накладення арешту на кореспонденцію (ст. 261, 262 КПК України); в) зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України); г) зняття інформації з електронних інформаційних систем (ст. 264 КПК України); ґ) обстеження:публічно недоступних місць; житла чи іншого володіння особи (ст. 267 КПК України); д) установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України); е) спостереження: за особою, річчю або місцем (ст. 269 КПК України); є) моніторинг банківських рахунків (ст. 269-1 КПК України);ж) аудіо-, відеоконтроль місця (ст. 270 КПК України); з) контроль за вчиненням злочину у формах: 1) контрольованої поставки, 2) контрольованої та оперативної закупки, 3) спеціального слідчого експерименту, 4) імітування обстановки злочину (ст. 271 КПК України);е) виконання спеціального завдання з розкриття злочинної діяльності чи злочинної організації (ст. 272 КПК України) [81].

Одночасно з прийняттям чинного КПК України внесено зміни та доповнення до 75 Законів України, зокрема Закону України «Про оперативно-розшукову діяльність». Законодавець звузив підстави для проведення оперативно-розшукової діяльності й доповнив кримінальне провадження інститутом «негласні слідчі (розшукові) дії (глава 21 КПК України)» [177, с. 18; 81]. Так, ч. 1 ст. 246 КПК України визначено, що НСРД – це різновид СРД, відомості про факт і методи проведення яких не підлягають розголошенню, за винятком випадків,

передбачених КПК 181 України [81]. Як зазначав М.Л. Грібов, і ми цілком підтримуємо його думку, криміналістичне забезпечення НСРД – це система заходів з одержання максимальної ефективності цих дій для виконання завдань кримінального провадження [37, с. 39].

Специфіка початку досудового розслідування кримінальних правопорушень щодо розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку полягає в тому, що внести відомості до ЄРДР виявлені кримінальні правопорушення можна лише за наявності достатніх фактичних даних, які вказують на втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, що виступає предметом вчинення злочину, тобто лише після винесення відповідних відомостей.

За результатами анкетування слідчих найчастіше у провадженнях досліджуваної категорії проводяться такі НСРД: зняття інформації з транспортних телекомунікаційних мереж (87 %); установлення місцезнаходження радіоелектронного засобу (62 %); аудіо-, відеоконтроль особи (39 %); зняття інформації з електронних інформаційних систем (31 %); контроль за вчиненням злочину (27 %), обстеження публічно недоступних місць, житла чи іншого володіння особи (19 %).

Відповідно до ч. 1 ст. 250, ч. 4 ст. 268 КПК України установлення місцезнаходження радіоелектронного засобу може бути розпочато до постановлення ухвали слідчого судді, за постановою слідчого, погодженої з прокурором або прокурора, а продовжена лише за наявності ухвали слідчого судді, постановленої за клопотанням прокурора. Загальними умовами проведення згаданих НСРД є такі: неможливість одержати в інший спосіб відомості про злочин та особу, яка його вчинила; проведення виключно за тяжкими або особливо тяжкими злочинами (за виключенням установлення місцезнаходження радіоелектронного засобу, що дозволяється проводити в кримінальних провадженнях за злочинами будь-якого ступеня тяжкості); проведення виключно на підставі ухвали слідчого судді (крім установлення місцезнаходження

радіоелектронного засобу, який у згаданих випадках дозволяється розпочати за постановою слідчого, погодженою з прокурором); проведення за розпочатим кримінальним провадженням (після внесення відомостей до ЄРДР).

Проведення НСРД – *установлення місцезнаходження радіоелектронного засобу* дозволяє вирішити розшукове завдання щодо встановлення факту знаходження в певному місці та в певний час конкретної особи, якій належить (перебуває в користуванні) радіоелектронний засіб (інший радіо-випромінювальний пристрій), активований у мережі оператора рухомого (мобільного) зв'язку [28, с. 38]. Установлення місцезнаходження радіоелектронного засобу проводиться на підставі ухвали слідчого судді, постановленої у порядку, передбаченому 190 ст. ст. 246, 248–250 КПК України. В ухвалі слідчого судді про дозвіл на встановлення місцезнаходження радіоелектронного засобу додатково має бути зазначено ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання. У разі, якщо прокурор відмовляє в погодженні клопотання слідчого до слідчого судді про проведення установлення місцезнаходження радіоелектронного засобу, слідчий, відповідно до ч. 3 ст. 40 КПК України, має право звернутися до керівника органу досудового слідства, який після вивчення клопотання за необхідності ініціює розгляд питань, порушених у ньому, перед прокурором вищого рівня, звертаючись до нього про погодження клопотання до слідчого судді про проведення установлення місцезнаходження радіоелектронного засобу, який протягом трьох днів погоджує відповідне клопотання або відмовляє в його погодженні [81].

Установлення місцезнаходження радіоелектронного засобу (ч. 1 ст. 268 КПК України) (мобільного терміналу систем зв'язку та інших радіо-випромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, тобто мобільного телефону, GSM, UMTS, HSDPA, WiMAX, LTE модемів, що забезпечують бездротовий доступ до мережі Інтернет) дозволяє вирішити розшукове завдання щодо встановлення факту знаходження у певному місці та у певний час конкретної особи або осіб, якій належить (знаходиться у

користуванні) радіоелектронний засіб (інший радіо-випромінювальний пристрій), активований у мережі оператора рухомого (мобільного) зв'язку.

Доцільно провести моніторинг засобів мобільного зв'язку, активованих у місці вчинення злочину:

– встановити з'єднання абонентських номерів (із зазначенням IMEI терміналу), що відбулися у межах дії певної базової станції або її соти (параметри дії LAC-SID) за певний період часу, можливо провести моніторинг та проаналізувати історію їх з'єднання, чи тривало користується абонент телекомунікаційною карткою (SIM-картка, USIM-картка, R-UIM-картка тощо), унікальним ідентифікатором сім-картки (IMSI) тощо (наприклад, за відомим IMEI-кодом мобільного телефону можна встановити номер абонента або номери всіх абонентів, які користувалися цим телефоном у певний час); – звернути увагу на телекомунікаційну картку, що активована зовсім недавно: в день вчинення злочину; за один день до вчинення злочину і до семи днів до вчинення злочину; та один день після вчинення злочину.

Виявивши телекомунікаційну картку, що активована недавно, можливо встановити спосіб попередньо оплаченої послуги, номери карт експрес-оплати (ваучерів поповнення балансу абонента), що дозволяє встановити місця їх придбання, картку поповнення рахунку, номер абонента по карті експрес оплати, місце, час, термінал поповнення рахунків певним абонентом, місце придбання картки поповнення рахунку, факт переміщення коштів з балансу одного абонента на баланс іншого тощо.

У разі ж, якщо для встановлення обставин, що мають значення для кримінального провадження, необхідні відомості про місцезнаходження конкретного радіоелектронного засобу в певному місці та в певний час, слідчий складає клопотання про дозвіл на проведення установлення місцезнаходження радіоелектронного засобу до апеляційного суду, у межах територіальної юрисдикції якого перебуває орган досудового слідства (ст. 247 ПК України), узгоджує його з прокурором та отримує ухвалу слідчого судді про проведення установлення місцезнаходження радіоелектронного засобу або про відмову в

наданні дозволу на його проведення. Таке клопотання має бути укладеним відповідно до ч. 2 ст. 248 КПК України. До клопотання додається витяг з ЄРДР щодо кримінального провадження, у межах якого подається клопотання [103]. За результатами проведення даної НСРД слідчий або особа уповноваженого оперативного підрозділу Національної поліції, якій доручено її проведення, у порядку п. 3 ч. 1 ст. 40, ч. 6 ст. 246 КПК України складає протокол відповідно до вимог ст.ст. 104–107, 252 КПК України, до якого за необхідності долучаються додатки. Протокол про проведення НСРД з додатками не пізніше, ніж через двадцять чотири години з моменту припинення цієї дії передається прокурору. Прокурор вживає заходів щодо збереження отриманих під час проведення НСРД речей і документів, які планує використовувати у кримінальному провадженні (ст. 252 КПК України) [103].

Зняття інформації з транспортних телекомунікаційних мереж є різновидом втручання у приватне спілкування, яке проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження. Воно полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні й фіксації різних видів сигналів, що передаються каналами зв’язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду). Зняття інформації з транспортних телекомунікаційних мереж поділяється на: – контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, зокрема встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв’язок, модемний зв’язок тощо), які передаються телефонним каналом зв’язку, що контролюється; – зняття інформації з каналів зв’язку, що полягає в негласному одержанні, перетворенні й фіксації із застосуванням технічних засобів, зокрема встановлених на

транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються (ч. 1 ст. 263 КПК України) [81].

Під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, працівники підрозділів оперативних підрозділів Національної поліції України залучаються при проведенні:

- аудіо-, відеоконтролю особи (ст. 260 КПК України), якщо є достатні підстави вважати, що розмови певної особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування. Шляхом аудіо- та відеоконтролю особи може здійснюватися спостереження за діями та розмовами окремих осіб у житлі або іншому володінні особи або ж в інших приміщеннях, транспортних засобах, інших місцях, що не є житлом чи іншим володінням особи. Аудіоконтроль полягає у прослуховуванні та фіксації розмов, що відбуваються в зазначених об'єктах, та може здійснюватися епізодично або безперервно на проміжок часу, визначений у рішенні слідчого судді, що надав дозвіл на його проведення (ст. 249 КПК України). Безперервний аудіоконтроль з фіксацією та обробкою отриманої за ним інформації здійснюється, як правило, цілодобово. Відеоконтроль особи здійснюється технічними засобами, що забезпечують негласне візуальне спостереження за діями, розмовами, поведінкою підозрюваного та осіб, які контактують з ним, у зв'язку з їх причетністю до злочину. Проведення цього заходу дозволяє виявляти та фіксувати інформацію, що свідчить про підготовку або вчинення окремими особами незаконних дій з вилученими речовими доказами, з'ясовувати місця збереження, можливість визначення осіб, які відвідують певні місця, та інше, що становить інтерес для слідства.

Аудіо- та відеоконтроль місця (ст. 270 КПК України) шляхом встановлення спеціальних технічних засобів у публічно доступних місцях за наявності відомостей про те, що розмови і поведінка осіб у цьому місці, а також інші події, що там відбуваються, мають значення для кримінального провадження. Аудіо-,

відеоконтроль місця доцільно проводити також у місцях імовірного перебування або появи осіб, які підозрюються у причетності до незаконного втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, з метою фіксації інформації, що може використовуватись у доказуванні на досудовому розслідуванні та в суді.

Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України). Відповідно до Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержанні інформації, зокрема із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютерах), автоматичних системах, комп'ютерній мережі [127].

Зняття інформації з електронних інформаційних систем надає можливість з'ясувати місцезнаходження підозрюваного, коло його злочинних зв'язків, виявлення нових епізодів злочинної діяльності. Така НСРД може здійснюватися шляхом отримання інформації, що оброблялася, зберігається або зберігалася на персональному комп'ютері чи декількох персональних комп'ютерах, об'єднаних у локальну мережу, або ж зовнішніх накопичувачах інформації, що приєднувалися до електронних інформаційних систем. Водночас отримання такої інформації в межах зняття інформації з електронних інформаційних систем можливе лише в разі, якщо жоден з елементів локальної мережі не під'єднаний до глобальної мережі.

Важливо, щоб під час складання клопотання про отримання дозволу на зняття інформації з електронних інформаційних систем слідчий зазначав такі дані: найменування кримінального провадження та його реєстраційний номер; стислий виклад обставин злочину, у зв'язку з розслідуванням якого подають клопотання; правова кваліфікація злочину із зазначенням статті (частини статті) 198 КК України; відомості про особу (осіб), місце або річ, щодо яких необхідно провести НСРД; обставини, що дають підстави підозрювати особу у вчиненні злочину;

обґрунтування строку проведення зняття інформації з електронних інформаційних систем; обґрунтування неможливості отримання відомостей про злочин та особу, яка його вчинила, в інший спосіб; відомості про ідентифікаційні ознаки електронної інформаційної системи; обґрунтування можливості отримання під час проведення цієї НСРД відомостей, які самостійно або сукупно з іншими доказами можуть мати істотне значення для з'ясування обставин злочину або встановлення осіб, які його вчинили. До клопотання слідчого, прокурора додають витяг з ЄРДР щодо кримінального провадження, у межах якого подають клопотання [91, с. 205].

Контроль за вчиненням злочину (ст. 271 КПК України). Контроль за вчиненням незаконного втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж(оперативна закупка, спеціальний слідчий експеримент, імітування обстановки злочину) може здійснюватися у випадках наявності достатніх підстав вважати, що готується вчинення або вчиняється тяжкий чи особливо тяжкий злочин, та проводиться у формах, визначених ч. 1 ст. 271 КПК України. Застосовується така НСРД, як правило, у формі оперативної закупки (78 % опитаних респондентів) і передбачає: використання заздалегідь ідентифікованих (помічених) грошей для передачі вимагачу та попереднє вручення помічених грошей потерпілому в присутності понятих у приміщенні органу поліції; підготовка засобів фото- та відеофіксації ходу і результатів НСРД (із залученням працівників підрозділів ОТЗ).

Обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК України) полягає в таємному проникненні слідчого чи уповноваженої особи без відома власника чи володільця, приховано, під псевдонімом або із застосуванням технічних засобів у приміщення та інше володіння для встановлення технічних засобів аудіо-, відеоконтролю особи або безпосередньо з метою виявлення і фіксації слідів злочину, проведення огляду, виявлення документів, речей, що мають значення для досудового розслідування, виготовлення копій чи їх зразків, виявлення осіб, які розшукуються, або з іншою метою для досягнення цілей кримінального провадження [125, с. 98].

Відтак, слідчий (або за його дорученням уповноважений оперативний працівник) має право обстежити публічно недоступні місця, житло чи інше володіння особи шляхом таємного проникнення в них, зокрема з використанням технічних засобів, з метою: виявити слідову картину злочинного діяння; встановити місцезнаходження документів, грошових коштів; виявити місця, де були виготовлені копії документів; виявити та вилучити зразки для дослідження під час досудового розслідування; виявити осіб, які розшукуються; встановити технічні засоби аудіо-, відеоконтролю особи.

За допомогою цієї НСРД можна встановити відомості про обставини вчинення злочину, що зберігаються у документах або на носіях електронної інформації, зробити їхні копії, або ж знайти самого злочинця, який розшукується, встановити його контакти, співучасників, корупційне прикриття тощо. З набранням чинності КПК України 2012 р. запроваджено нову процедуру одержання дозволів на проведення НСРД за участю слідчого, прокурора, судді, а також уповноваженого оперативного підрозділу.

Важливою передумовою залучення спеціаліста до проведення НСРД під час розслідування злочинів даної категорії правопорушень у випадку, якщо інформація, яка буде досліджуватись, належить до державної таємниці, є наявність у нього допуску до державної таємниці відповідної форми. Саме тому підготовча стадія НСРД є важливим елементом такої дії в ході якої з'ясовується характер інформації та вживаються заходи із залучення відповідного спеціаліста.

З метою підвищення рівня захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій, на нашу думку, потрібно доповнити ст. 254 КПК України положенням такого змісту: «У випадку залучення спеціаліста у протоколі негласної слідчої (розшукової) дії зазначається, що йому роз'яснено його зобов'язання, передбачені ч. 5 ст. 77 КПК України, зокрема щодо нерозголошення відомостей, які стали відомі спеціалісту у зв'язку з виконанням його обов'язків». Оскільки серед положень ст. 104, якою передбачено зміст протоколу, не має норми про відмітку щоодо попередження учасників слідчих (розшукових) дій про їх права та обов'язки.

Щодо техніко-криміналістичних засобів, які застосовуються при проведенні негласної слідчої (розшукової) дії, потребує уточнення ч. 2 ст. 266 КПК України, у якій має бути передбачено: «Первинні носії інформації (за можливості від'єднання такого носія від технічного пристрою) долучаються до протоколу негласної слідчої (розшукової) дії. У всіх інших випадках з отриманої інформації знімається копія, яка долучається до протоколу, з фіксуванням у ньому хеш-суми скопійованих файлів. Відповідно, первинні носії інформації й технічні засоби її отримання повинні зберігатися до набрання законної сили вироком суду з позначенням місця зберігання, відповідальної особи та її попередженням про це в протоколі негласної слідчої (розшукової) дії». Оскільки на сьогодні ці положення мають неточний характер, а тому можуть приводити до проблем правозастосування.

Висновки до розділу 2

1. Аналіз та узагальнення різних праць провідних вчених-криміналістів дає підстави для авторського визначення *поняття техніко-криміналістичних засобів,* що використовуються під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку *як* – систему спеціально виготовлених або пристосованих приладів, пристроїв, пристосувань, інструментів, матеріалів, інформаційних пошукових, ідентифікаційних та інших систем, а також криміналістичних технологій їх застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів, а також здійснення інших дій по виявленню, розслідуванню та попередженню злочинів.

2. Визначено підходи (види) до розуміння техніко-криміналістичних засобів, які використовуються під час розслідування злочинів у сфері

використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, до яких належать: – апаратні засоби мобільної криміналістики; програмні засоби мобільної криміналістики; апаратні блокіратори запису; програмні засоби комп'ютерної експертизи; апаратні засоби відновлення даних; відкрите програмне забезпечення; дистрибутиви на основі Linux.

3. Розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку проводиться за загальними правилами. Завдання слідчого – професійно організувати роботу, правильно використовувати знання спеціалістів у сфері обчислювальної техніки та застосування техніко-криміналістичних засобів для ефективного пошуку інформації в комп'ютері, комп'ютерних мережах і мережах електрозв'язку та правильній її фіксації в криміналістичному плані [168, с. 180].

До специфічних завдань огляду місця події можна віднести огляд і вилучення документів та інформації з автоматизованих охоронних систем відеоспостереження й контролю доступу до електронно-обчислювальних машин, а також пошук, виявлення, огляд, фіксацію і вилучення спеціальних технічних пристроїв, що призначені або пристосовані й запрограмовані для негласного отримання, знищення, копіювання чи модифікації або блокування комп'ютерної інформації. Оглядаючи комп'ютер як окремий об'єкт, варто знати, що дослідженню підлягає насамперед його інформаційна база та так звана „архітектура» комп'ютера. Такий огляд дає змогу з точністю до секунди встановити час увімкнення комп'ютера в будь-який час доби, встановити факт користування поштовими програмами і методи доступу до них, визначити коло кореспондентів, з якими спілкувалися за допомогою цього комп'ютера, дізнатися зміст листування до того ж як текстових повідомлень, так графічного матеріалу та зображень. Враховуючи особливості обстановки, за якої здійснюється слідчий огляд, питання щодо можливості вилучення засобів комп'ютерної техніки та носіїв інформації, способу їх пакування, транспортування і зберігання

комп'ютерних об'єктів розв'язується слідчим залежно від конкретного випадку і з урахуванням думки спеціаліста.

4. Оскільки відображенням об'єктивної сторони складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є поряд з «традиційними» й інформаційні сліди, важливим аспектом проведення слідчих (розшукових) дій є те, що інформація або доступ до неї можуть бути втрачені після відключення електронного пристрою (енергозалежні дані, спеціальні програми для знищення даних тощо) або ж зберігатися на серверах чи пристроях, що розташовані в іншому місці, у тому числі поза межами проведення слідчої (розшукової) дії та навіть поза межами України (використання зовнішніх пристроїв збереження даних, хмарних сховищ тощо). У зв'язку з цим, існує потреба в проведенні кваліфікованого виявлення, фіксації та вилучення такої інформації або ж її носіїв, ужитті заходів щодо недопущення стороннього (зовнішнього) впливу на електронні сліди злочину (наприклад, відключення електроенергії, віддаленого доступу до файлів та керування системою тощо), готовності органів розслідування оперативно проводити слідчі (розшукові) дії в інших місцях, де може зберігатися цифрова інформація.

5. У кримінальних провадженнях даної категорії проводяться такі НСРД: зняття інформації з транспортних телекомунікаційних мереж і спостереження за особою, річчю або місцем (візуальне спостереження) – дають змогу встановити вхідні, вихідні дзвінки на мобільний телефон підозрюваного, визначити його поточне місцеперебування (власника мобільного телефону) або іншої особи, яка ним користується, простежити переміщення особи і пристрою в часі та просторі; обстеження публічно недоступних місць, житла чи іншого володіння особи, за допомогою якого виявляють та фіксують сліди вчинення злочину; досліджують місце утримання дітей; забезпечують збереження доказів, які, за наявною інформацією, можуть бути знищені до їх вилучення процесуальним шляхом; встановлюють осіб, які розшукуються; установлення місцезнаходження радіоелектронного засобу – фіксація факту перебування в певному місці та в

певний час особи, яка користується радіоелектронним засобом чи іншим пристроєм, який випромінює радіохвилі й активований у мережі оператора рухомого (мобільного) зв'язку (як у режимі реального часу, так і в конкретний період); аудіо-, відеоконтроль особи, спрямований на фіксацію поведінки, розмов і місця перебування осіб, яких підозрюють у скоєнні злочину; зняття інформації з електронних інформаційних систем, що надає можливість отримати інформацію, розміщену особою у соціальних мережах, тематичних форумах; контроль за вчиненням злочину здійснюється у випадках наявності достатніх підстав вважати, що готується втручання до ЕОМ (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку, та проводиться у формах, визначених ч. 1 ст. 271 КПК України.

РОЗДІЛ 3.
СУДОВІ ЕКСПЕРТИЗИ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

3.1. Види та можливості судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Визначення основних напрямів державної політики у сфері інформаційної безпеки є вкрай актуальним для сучасної України. Враховуючи стрімкий прогрес у сфері поширення та розвитку інформаційно-комунікаційних технологій, ми повинні чітко усвідомлювати, що нормальна життєдіяльність нашого суспільства багато у чому визначається безпекою його інформаційного середовища.

Пошук нових, більш ефективних способів виявлення та нейтралізації впливів на інформацію, у тому числі у світових відкритих мережах, є природною захисною реакцією суспільства. Україна у цьому контексті не є винятком.

За даними провідних міжнародних організацій, вже сьогодні збитки, завдані кримінальними правопорушеннями у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, можна порівняти з доходами від незаконного обігу наркотичних засобів та зброї. Тільки в США щорічні економічні втрати від цих видів злочинних діянь становлять понад 100 млрд. дол. При чому, багато деліктів у цій сфері залишаються бути прихованими, що характеризує їхню високу латентність [72].

Розкриваючи проблемні питання боротьби з комп'ютерною злочинністю у сучасному світі, можливо виокремити наступні негативні чинники, які притаманні для України, а саме:

– відсутність налагодженої системи правового та організаційно-технічного забезпечення законних інтересів громадян, держави та суспільства у сфері інформаційної безпеки;

– обмежені можливості бюджетного фінансування робіт зі створення правової, організаційної та технічної бази інформаційної безпеки;

– слабка координація дій у боротьбі з комп'ютерною злочинністю правоохоронних органів та недостатня підготовка їх кадрового складу щодо ефективного попередження, виявлення та розслідування таких протиправних діянь;

– недосконала система єдиного обліку правопорушень, скоєних за допомогою засобів інформатизації;

– відставання вітчизняної індустрії інформаційних технологій та їх баз даних від світового рівня.

Таким чином, комп'ютерна злочинність як нова форма антигромадської поведінки становить серйозну загрозу безпеці та нормальному функціонуванню нашого суспільства. Виходячи з цього, на нашу думку, основною метою державної політики у протидії кримінальним правопорушенням у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку має бути взаємодія та координація зусиль експертних структур із правоохоронними органами, а також забезпечення їх необхідною матеріально-технічною базою.

Не секрет, що взаємодія відповідних органів на сьогоднішній день в основному зводиться до епізодичного обміну інформацією. Немає найголовнішого – цілісної системи безперервного відстеження обстановки у сфері забезпечення інформаційної безпеки різних систем та своєчасного (запобіжного) прийняття рішень щодо виявлення та припинення таких видів кримінальних правопорушень. Цілком очевидно, що створення цілісної системи неможливе, якщо не налагоджено ефективної взаємодії вітчизняних експертних структур з експертними та правоохоронними органами зарубіжних країн, які здійснюють боротьбу з комп'ютерною злочинністю. Більше того, будь-яка навіть

найтехнологічніша система не зможе досягти поставленої мети, не будучи забезпечена висококваліфікованими кадрами [138].

Необхідно також зазначити, що процеси щодо ефективного розкриття, розслідування та попередження злочинів вчинених з використанням комп'ютерних можливостей вимагають створення всіх необхідних для цього методичних та технічних засобів. Зважаючи на слабку розробленість відповідного інструментарію, це завдання є першорядним при реалізації заходів щодо адекватної протидії комп'ютерній злочинності. Із зазначеним напрямом тісно пов'язана проблема вдосконалення нормативно-правової бази, недостатня розробленість якої поки що не дозволяє на належному рівні протистояти протиправним діянням у комп'ютерній сфері.

Крім цього, відсутність чіткої кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку створює складності у тлумаченні та застосуванні норм закону, що як наслідок обмежує дії правоохоронних органів з реалізації завдань щодо протидії комп'ютерній злочинності.

Зрештою, одним із головних завдань щодо ефективної боротьби з кримінальними правопорушеннями у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку є проведення комплексу науково-дослідних робіт із удосконалення та створення програмних, програмно-апаратних та технічних засобів, що забезпечать ефективний захист комп'ютерних мереж та їх баз даних.

За даними вітчизняної експертної практики, щороку простежується зростання криміногенної обстановки у сфері використання комп'ютерних технологій. Ця обставина, в першу чергу, свідчить про те, що:

– по-перше, інформація стає предметом злочинного посягання оскільки її використання, розповсюдження або збут дає високі прибутки;

– та по-друге, експертні та правоохоронні органи поступово накопичують досвід боротьби з цими кримінальними правопорушеннями, у зв'язку з цим розробляють більш ефективні способи їх виявлення, розкриття та припинення.

При розслідуванні таких високотехнологічних злочинів все частіше виникає необхідність у виявленні та вилученні слідів та речових доказів, поданих у вигляді інформації в електронно-обчислювальних, телекомунікаційних системах, на магнітних носіях, програмних продуктах та комп'ютерній техніці. У зв'язку з цим, виникає потреба у залученні слідчим в ході досудового розслідування спеціальних знань і навичок використання новітніх інформаційних технологій. Тобто, таких наукових, технічних та інших професійних знань, які не є загальновідомими для слідчого, прокурора, суду та інших учасників процесу.

З цього приводу, ще О.Ф. Коні, у роботі «Суд – наука – мистецтво» відмітив, що судова практика часто змушує вдаватися до спеціальних досліджень, зосереджуючи у яких центр тяжкості справи і звертаючись до сприяння обізнаних людей, тобто експертів з різних спеціальних галузей знань, мистецтв чи ремесел [74, с. 4]. У цьому контексті Б.М. Шавер, у 1940 році наголошував, що ефективне розкриття та розслідування злочинів багато у чому залежить від використання в процесі розслідування знань і досягнень технічних наук [75, с. 68].

Починаючи з кінця 40-х років минулого століття у вітчизняній кримінальній процесуальній діяльності спеціальні знання використовуються у трьох формах, а саме:

– при залученні спеціалістів під час проведення окремих слідчо-процесуальних чи судових дій (ст. 71 КПК України) [81];

– в межах проведення експертиз (ст.ст. 242-245, 332 КПК України);

– під час допиту експерта (ч. 7 ст. 95, ч. 7 ст. 101, ст. 356 КПК України).

У 1949 році А.І. Вінберг вперше порушив питання щодо уведення в кримінальний процес поряд з експертом такої процесуальної фігури, як спеціаліст.

Відповідно до вітчизняного кримінального процесуального законодавства, спеціалістом є особа, яка володіє спеціальними знаннями та навичками застосування технічних або інших засобів і може надавати консультації під час

досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок (ч. 1 ст. 71).

Таким чином, спеціаліст реалізовує свої знання у двох формах, а саме: не процесуальних – усних поясненнях і методичних консультаціях зі спеціальних питань; процесуальних – безпосереднього застосування спеціальних знань та криміналістичної техніки, інших науково-технічних засобів при виявленні, вилученні, закріпленні та дослідженні доказів.

При цьому, основною процесуальною формою щодо залучення та використання наукових, технічних та інших спеціальних знань у кримінальному процесі вважається експертиза, яка ґрунтується на спеціальному дослідженні та відповідному кваліфікованому висновку експерта, який безпосередньо стосується досудового розслідування.

Проведення судової експертизи у вітчизняному законодавстві регламентується: Законом України «Про судову експертизу» від 25.02.1994 № 4038-XII [137]; Кримінальним процесуальним кодексом України (ст.ст. 69, 70, 101, 102, 232, 242-245, 518) [81]; Цивільним процесуальним кодексом України (ст.ст. 72, 73, 102-115, 255, 237, 239, 298) [182]; Положенням про Експертну службу МВС України, затвердженим наказом МВС України від 03.11.2015 № 1343 [131]; Інструкцією про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень від 08.10.98 № 53/5 [129]; Інструкцією про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах від 12.12.2011 № 3505/5 [128].

Відповідно до положень яких, судовою експертизою вважається дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об’єктів, явищ і процесів з метою надання висновку з питань, що є або можуть бути предметом судового розгляду [137]. Дане визначення дає зрозуміти, що призначення судової експертизи у кримінальному процесі має місце тоді, коли для з’ясування конкретних обстави у кримінальному провадженні

потрібні спеціальні галузеві знання, якими володіють відповідні особи – експерти. На цьому наголошує й ст. 242 КПК України (Підстави проведення експертизи) [81], де зазначено, що судова експертиза проводиться відповідною спеціалізованою експертною установою або атестованими судовими експертами, які не працюють у цих установах, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання.

Узагальнення світової практики щодо розкриття та розслідування злочинів, пов'язаних з новітніми інформаційними технологіями свідчить про те, що перелік експертних досліджень, які можуть проводитися у справах про злочини цієї категорії є досить широким. До них можливо віднести традиційні експертизи (трасологічну, дактилоскопічну, техніко-криміналістичну експертизу документів тощо), судово-економічні (бухгалтерську, фінансово-економічну, аудиторську тощо), а також інші види судових експертиз, що відносяться до різних класів.

Така обставина в першу чергу свідчить про те, що розвиток мобільно-комп'ютерних технологій дав широкий спектр цифрових і повністю портативних пристроїв, які отримали назву – гаджет (мобільні телефони, смартфони, комунікатори, кишенькові комп'ютери, ноутбуки, планшетні комп'ютери), їх мобільних додатків (програм для мобільних пристроїв), сервісів (отримання, зберігання, обробка, пошук, передача інформації та ін. за допомогою мобільного пристрою) та засобів мобільного зв'язку (GSM, WAP, GPRS, Bluetooth, Wi.Fi, i.Max), що дозволило здійснювати операції з отримання, обробки та передачі інформації практично у всіх сферах життєдіяльності людини. Таким чином проблема інформаційної безпеки посилилась процесами проникнення практично у всі сфери життєдіяльності суспільства технічних засобів обробки та передачі інформації. Тому, об'єкт та предмет (експертне завдання) судових експертиз під час розкриття та розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку залежить від способу та механізму скоєння та приховування злочину.

Принципово важливе значення для розкриття та розслідування злочинів у сфері використання комп'ютерних технологій, систем та мереж електрозв'язку займають спеціалізовані експертні дослідження. До яких Науково-методичними рекомендаціями з питань підготовки та призначення судових експертиз та експертних досліджень затверджених наказом Міністерства юстиції України від 08.10.1998 № 53/5 було віднесено 1) експертизу комп'ютерної техніки і програмних продуктів та 2) експертизу телекомунікаційних систем та засобів [129], включивши їх до класу інженерно-технічних експертиз, що свідчить про те, що за своїм походженням електронно-обчислювальна техніка відноситься до інженерно-технічних розробок.

Аналіз кримінальних проваджень надав змогу визначити, що типовими видами судових експертиз, які проводяться під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, є: комп'ютерної техніки і програмних продуктів (98% кримінальних проваджень); традиційні криміналістичні (трасологічна, дактилоскопічна, технічна експертиза документів тощо) (18%); телекомунікаційних систем і засобів (5%); судово-економічні (4%); біологічні (2%); а також комплексні (комп'ютерно-технічна та судово-бухгалтерська експертиза, комп'ютерно-технічна та судово-товарознавча експертиза, комп'ютерно-технічна та експертиза об'єктів інтелектуальної власності тощо) (1%) та комісійні експертизи (1%).

Незважаючи на це, починаючи з середини 90-х років минулого століття і до сьогодні у науково-криміналістичній спільності серед вчених та практиків продовжуються відбуватись дискусії щодо визначення видів судових експертиз під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, їх основних завдань дослідження, об'єктів, ідентифікаційного поля, ідентифікаційних завдань та переліку орієнтовних питань, які доцільно ставити перед експертом.

Так, наприклад на сьогодні в спеціальній літературі назви експертизи комп'ютерної техніки і програмних продуктів, так само як і експертизи

телекомунікаційних систем та засобів термінологічно, є нестійкими. Автори, а також слідчі вживають різні найменування експертиз такі як: «комп'ютерна», «програмно-технічна», «комп'ютерно-технічна», «ІТ-експертиза» тощо. На нашу думку, це суттєво ускладнює підбір слідчим необхідного виду експертного дослідження, адже вищезазначені терміни не охоплюють всіх об'єктів дослідження, що також створює труднощі при постановці питань, які виносяться на вирішення експертові.

Досліджуючи це питання В.О. Мещеряков вважає доцільним поділ експертизи комп'ютерної техніки і програмних продуктів на комп'ютерну експрес-експертизу, комп'ютерну стандартну експертизу та комп'ютерну детальну експертизу [96, с. 331]. Справедливо критикуючи цю дефініцію Д.В. Пашнєв поділяє зазначену експертизу на:

– експертизу технічних комп'ютерних засобів, об'єктами якої є персональні комп'ютери (стаціонарні, портативні), інтегровані системи (органайзери), вбудовані системи на основі мікропроцесорних контролерів (імобілайзери, транспондери, круіз-контролери та ін.), будь-які комплектуючі всіх вказаних компонентів (апаратні блоки, плати розширення, мікросхеми та ін.).

– експертизу програмного забезпечення, метою якої є дослідження яка досліджує модулів, пакетів, алгоритмів, вихідних текстів операційних та прикладних програм.

– експертизу даних, яка досліджує всі файли комп'ютерної системи, які не являються програмними модулями і такі, що підготовлені користувачем або самою системою [114, с. 147–149].

Заслуговує окремої уваги й думка М.Г. Щербаковського, який виділяє: експертизу апаратних комп'ютерних засобів та експертиза даних і програмного забезпечення [192, с. 355]. Схожих поглядів притримуються й О.Р. Росинська та В.О. Усов, які зазначають, що у рамках проведення експертизи комп'ютерної техніки і програмних продуктів її можливо поділити на два види:

– технічну експертизу комп'ютерів та його комплектуючих. Проведення якої направлено для вивчення конструктивних особливостей і стану комп'ютера,

його периферійних пристроїв, магнітних носіїв, комп'ютерних мереж, а також причин виникнення збоїв у роботі вищезазначеного обладнання;

– експертизи даних та програмного забезпечення, що здійснюється з метою дослідження інформації, яка зберігалася в комп'ютері та його магнітних носіях [149, с. 173].

Разом з тим, на думку О.І. Мотляха викладена вище точка зору хоча й заслуговує на увагу, однак потребує певного уточнення, оскільки після відокремлення їх у окремий вид експертиз, можуть виникнути певні труднощі у роботі слідчих під час вибору тієї чи іншої експертизи і визначенні категорії запитань, адже межа між ними має умовний характер. Тому, вчений підтримуючи позицію І.В. Гори, В.А. Колесника, А.В. Іщенка поділяє експертизу комп'ютерної техніки і програмних продуктів на:

– судову апаратно-комп'ютерну експертизу, завданнями якої є визначення видів, властивостей апаратного засобу, умов застосування, наявності фізичних дефектів, встановлює причинний зв'язок між можливостями апаратних засобів та результатами їх використання;

– судову програмно-комп'ютерну експертизу, яка визначає загальні характеристики операційної системи, її функціональні властивості, визначає фактичний стан програмного об'єкта, склад відповідних файлів, їх параметри тощо

– судову інформаційно-комп'ютерну експертизу, що встановлює властивості вид інформації у комп'ютерній системі, наявність відхилень від типових об'єктів (шкідливі включення, порушення цілісності тощо), встановлює первісний стан інформації на фізичних носіях тощо;

– судову комп'ютерно-мережеву експертизу, мета якої є визначення властивостей й характеристик апаратного засобу і програмного забезпечення, встановлення місця, конфігурації мережі та її компонентів, відповідності виявлених характеристик типовим для конкретного класу засобів мережної технології тощо [101, с. 183].

Окремої уваги, заслуговує думка Л.П. Паламарчук, яка розглядаючи види судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку виділяє:

– експертизу комп'ютерів і периферійних пристроїв, що проводиться з метою вивчення конструкційних особливостей і стану комп'ютера, його периферійних пристроїв, магнітних носіїв, комп'ютерних мереж, а також причин виникнення збоїв у роботі зазначеного обладнання;

– експертиза машинних даних і програмного забезпечення електронно-обчислювальних машин, яка досліджує вивчення інформації, що зберігається на комп'ютері та його магнітних носіях [110, с. 141]. До останніх можливо також віднести судову експертизу телекомунікаційних систем і засобів, яка є порівняно новим видом експертних досліджень, а тому формування наукових поглядів щодо її проведення та призначення знаходиться на початковій стадії розробок.

Слід також зазначити, що в окремих випадках, під час розслідування злочинів у сфері використання електронно-обчислювальних машин систем та комп'ютерних мереж і мереж електрозв'язку можуть призначатися комплексні та комісійні експертизи. Комплексні експертизи в основному проводяться для вирішення завдань, що відносяться до господарчої, фінансової діяльності установ проводиться комплексна комп'ютерно-технічна та судово-бухгалтерська експертиза. З метою встановлення пристрою, на якому був виконаний документ, порівняння документу з зображенням у файлі установ призначається комплексна комп'ютерно-технічна та судово-технічна експертиза документів. Для вивчення споживчих властивостей, умов зберігання, вартості комп'ютерних засобів, програмного забезпечення проводиться комплексна комп'ютерно-технічна та судово-товарознавча експертиза. Для встановлення джерела походження програмних продуктів, відео-, аудіопродукції призначається комплексна комп'ютерно-технічна та експертиза об'єктів інтелектуальної власності.

Крім цього, дослідження останніх років показують, що все частіше при розслідуванні злочинів у сфері комп'ютерних технологій слідство стикається з

необхідністю експертних досліджень мовної інформації, що передається комп'ютерними мережами. У цих випадках вчені криміналісти рекомендують призначати судово-лінгвістичні експертизи, об'єктом яких, на їхню думку, виступає мовна (текстова) інформація, зафіксована на тому чи іншому матеріальному носії. При цьому справедливо зазначається, що додаткові можливості для збору необхідних доказів можуть дати як сучасні можливості традиційних (судової авторознавчої експертизи), так і відносно нових експертиз, що порівняно недавно сформувалися (семантико-текстуальну експертизу), з метою встановлення екстремістських висловлювань, розпалювання національної, релігійної та расової ворожнечі, порушення прав інтелектуальної власності та ін.

Очевидно, що перед експертним дослідженням має бути чітко визначений його об'єкт та завдання. У зв'язку з цим, необхідно зазначити, що об'єктом криміналістичних досліджень судових експертиз під час розслідування злочинів у сфері використання комп'ютерних технологій є як машинний носій інформації так й сама комп'ютерна інформація, тобто інформація яка знаходиться на самому машинному носієві, а саме:

1) електронно-обчислювальна техніка;

2) програмне забезпечення та допоміжна комп'ютерна інформація необхідна для його функціонування;

3) текстові та графічні документи (стандартні та електронні), виготовлені з використанням засобів автоматизації (обчислювальних систем, засобів передачі даних та копіювання інформації);

4) відео- та звукозапис, візуальна та аудіальна інформація, представлена у форматі мультимедіа;

5) комп'ютерні дані та відомості, представлені у форматах, що забезпечують їхнє автоматизоване зберігання, пошук, обробку та передачу (бази даних);

6) фізичні носії інформації різної природи (магнітні, магнітооптичні, оптичні та ін.);

7) телекомунікаційні системи, засоби, мережі і їх складові частини, а також інформація, що ними передається та обробляється тощо.

Важливу роль у призначенні експертизи під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку набуває правильна постановка питань експерту, які прямо залежать від завдань експертного дослідження. У зв'язку з цим, помилки у постановці питань експерту фактично виступає помилкою у визначенні завдання, що вирішує експертиза. Коло завдань та питань, які можуть бути поставлені експерту, при призначенні комп'ютерних експертиз досить повно розкрито у криміналістичній літературі. Ці рекомендації можуть бути в повному обсязі використані при призначенні даних видів експертних досліджень. Зокрема, до основних можливо віднести ідентифікаційних та не ідентифікаційних (діагностичні чи ситуаційні) завдання, що полягають в/у:

– установленні робочого стану комп'ютерно-технічних засобів;

– установленні обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

– виявленні інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

– установленні відповідності програмних продуктів певним версіям чи вимогам на його розробку;

– визначенні характеристик та параметрів телекомунікаційних систем та засобів;

– встановленні фактів та способів передачі (отримання) інформації в телекомунікаційних системах;

– встановленні фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій;

– визначенні якості надання телекомунікаційних послуг на рівні їх споживання;

– встановленні конфігурації та робочого стану телекомунікаційних систем та засобів;

– встановленні типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів;

– дослідженні алгоритмів обробки інформації та її захисту у сфері телекомунікацій.

У зв’язку з цим перед експертом можуть бути поставлені такі завдання щодо:

– установлення цільового призначення та функціональних можливостей пристроїв, що входять до складу комп’ютера;

– установлення цільового призначення та функціональних можливостей програмного забезпечення;

– установлення факту розробки та хронології розробки програмного забезпечення;

– установлення факту розробки та хронологічних характеристик виготовлення текстових документів. Виявлення і відновлення умисне знищених текстових файлів різних форматів або їх фрагментів;

– установлення фактів прийому та передачі факсимільних повідомлень за допомогою модемного зв’язку, відновлення текстів і хронології обміну інформацією;

– установлення фактів здійснення фотомонтажу, монтажу відео та аудіо записів. Встановлення авторства і хронологічних характеристик виконання зазначених робіт;

– установлення фактів виготовлення печаток, штампів, бланків і іншої графічної продукції та визначення хронології виготовлення графічних документів;

– встановлення фактів розробки, авторства та хронологічних характеристик відеопродукції (відеофільмів, рекламних роликів тощо), виготовлених з використанням 3D-технологій;

– відновлення та аналіз відеоінформації низької якості, знятої з недостатньою експозицією, недостатньою освітленістю об’єктів або зіпсованої з інших причин;

– відновлення та аналіз аудіо інформації низької якості, записаної в умовах сильного шуму, з недостатньою чутливістю мікрофона, зіпсованої за якимись іншими причинами тощо;

– відновлення та аналіз інформації, що міститься в базах даних (інформаційні системи, бухгалтерія, довідники тощо). Відновлення умисне вилученої інформації або її фрагментів;

– відновлення та аналіз інформації, захищеної від несанкціонованого доступу (подолання кодів, паролів тощо);

– установлення цільового призначення і функціональних можливостей мережних Internet та Intranet – додатків;

– встановлення технологічних сеансів роботи в мережі Internet, виявлення, аналіз і відновлення інформації, отриманої по протоколах HTTP, FTP, UUCP, POP (файли, повідомлення електронної пошти e-mail, відвідування сайтів Internet тощо);

– установлення фактів розробки програмного забезпечення, призначеного для здійснення несанкціонованого доступу до комп'ютерних мереж;

– установлення фактів розробки програмного забезпечення для здійснення несанкціонованого доступу до розподілених баз даних та серверам баз даних;

– установлення фактів виготовлення або наявності на комп'ютері програмного забезпечення, призначеного для несанкціонованого здійснення розрахунків по кредитних картках в областях електронної комерції;

– установлення фактів виготовлення та умисного поширення комп'ютерних вірусів, а також програм, що небезпечні з погляду порушення працездатності комп'ютерних мереж;

– встановлення фактів виготовлення в мережі Internet інформації, зміст і способи поширення якої не відповідають чинному законодавству України (порнографія, відео, фото, тексти і т.п.);

– аналіз безпеки Internet додатків, при виготовленні яких використовуються технології HTML, Java, VBA, XML, ASP, Sybase, Oracle, MS Jet, PostgreSQL і т.п.;

– встановлення фактів несанкціонованого доступу до інформаційних ресурсів корпоративних мереж та мережі Internet. Визначення комп'ютера, з якого здійснюється несанкціонований доступ до інформаційних ресурсів;

– безпека комп'ютерних мереж;

– безпека баз даних;

– оцінка комп'ютерної техніки.

Разом із технікою на експертизу можуть бути також представлені документи, виконані із застосуванням ним засобів комп'ютерної техніки, а також сама така техніка (різні принтери, розмножувальна апаратура та ін.). Як показують проведені наукові дослідження, на сьогоднішній день нерукописні реквізити документів на паперових носіях на 90-95 %, або нанесені за допомогою друкарських пристроїв комп'ютерної техніки (матричні, струменеві, лазерні принтери), або комп'ютерні технології використовувалися для створення поліграфічних та посвідчувальних друкованих форм. У зв'язку з цим у ході розслідування комп'ютерного злочину перед слідством може стояти завдання встановлення суб'єкта, який виконав роздрукований документ, або ідентифікації та діагностики комп'ютерної техніки, що використовується для його виготовлення.

У зв'язку з цим перед експертом можуть бути поставлені такі завдання щодо встановлення:

– виду друкувального пристрою (принтер, сканер-копір, друкарська машина та ін.), його типу (матричне, струменеве, лазерне, друкарське), марки;

– чи вилучений документ вихідною роздруківкою файлу чи це його наступна копия;

– чи виконані вилучені в ході слідства документи на тому самому друкувальному пристрої;

– часу, витраченого виготовлення вилучених документів (при розмноженні великої кількості копій);

– можливості виконання реквізитів документа з використанням засобів комп'ютерної техніки;

– конкретного друкуючого пристрою, на якому виконано документ.

У криміналістичній літературі справедливо зазначається, що вирішити ідентифікаційні завдання під час експертизи документів, виконаних із застосуванням засобів комп'ютерної техніки, не завжди вдається. Це пов'язано багато в чому з тим, що в сучасних пристроях друкуючих навіть різного виду і типу використовуються одні і ті ж друкуючі блоки (картриджі). У зв'язку з цим слід пам'ятати, що вирішити питання про ідентифікацію конкретного друкуючого пристрою після зміни картриджа не завжди можливо. За даною категорією справ можуть бути призначені і традиційні криміналістичні експертизи (дактилоскопічна, трасологічна, техніко-криміналістична експертиза документів, фоноскопічна), судово-економічні експертизи (фінансово-економічна, бухгалтерська), а також інші експертизи.

Іншою важливою вимогою щодо призначення судових експертиз під час розслідування злочинів у сфері використання комп'ютерних технологій є грамотна підготовка об'єктів, що надаються експерту. Одним з основних об'єктів таких експертиз виступають різного роду комп'ютерно-технічні засоби. До останніх можливо віднести: – системний блок комп'ютера; – жорсткий диск; – інші технічні носії інформації (лазерні диски, флеш-карти, сервери та ін.); – інше комп'ютерне обладнання (модеми, сканери, принтери та ін.); – програмне забезпечення та інші програмні об'єкти (наприклад, програми-віруси); – комп'ютерні дані (інформаційні об'єкти); – спеціальна література (з комп'ютерного обладнання, програмування, питань інформаційної безпеки та ін.).

Комп'ютери, по їхньому специфічному призначенню, можуть бути віднесені до знарядь здійснення злочинів, як група приладів (інструментів), використовуваних для виконання деяких робіт. Наприклад: для виготовлення різного роду текстових і графічних документів; розробки і виготовлення програмних продуктів, що забезпечують досягнення злочинного результату; використання комп'ютера, як засобу зв'язку для прийому і передачі різного роду інформації; для несанкціонованого доступу до бази даних, для одержання інформації, яку можливо використовувати надалі в злочинних цілях. У

криміналістичному плані всяка дія викликає утворення слідів, що можуть бути класифіковані. Наявність слідів дозволяє відтворити, тобто змоделювати дії злочинця при здійсненні комп'ютерного злочину й ототожнити слідообразуючий об'єкт (комп'ютер) [111].

Необхідно також зауважити, що визначений перелік об'єктів не є вичерпним та потребує окремого дослідження.

Для дослідження інформації, що міститься на комп'ютерних носіях, експертові надається сам комп'ютерний носій, а також комп'ютерний комплекс, до складу якого входить досліджуваний носій. В деяких випадках можна обмежитися наданням тільки комп'ютерного носія. При можливості необхідно до проведення такого дослідження попередньо проконсультуватись з експертом. Для встановлення відповідності програмних продуктів певним параметрам, а також вартості програмного продукту експертові надається носій з копією досліджуваного програмного продукту і еталонна (дистрибутивна) копія програмного продукту. У разі відсутності дистрибутивної копії програмного продукту не слід відмовлятися від призначення експертизи, оскільки в окремих випадках її можна провести за наявності копії програмного продукту [111].

Для дослідження технічного стану і визначення вартості комп'ютерної техніки експертові надається сама комп'ютерна техніка, а також технічна документація до неї. Вилучення блоків комп'ютерної техніки слід доручати експертові. Для встановлення авторства досліджуваного програмного продукту експертові надаються самі програми у вигляді вихідних текстів, бібліотечних та виконуваних модулів, а також програми (вихідні тексти, бібліотечні та виконувані модулі), що створені особою, щодо якої перевіряється версія, чи вона є автором досліджуваного продукту. Щоб визначити, які саме об'єкти слід надавати експертові в кожному конкретному випадку, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки [Пам'ятка щодо огляду комп'ютерних засобів на місці події, експертиза комп'ютерної техніки і програмних продуктів. URL: http://uasol.com/index.php?aid=2835].

За результатами експертизи експерт складає та підписує експертний висновок. Цей висновок займає важливе місце у системі засобів доказування у кримінальному провадженні. Тому слід зазначити, що специфіка розслідування злочинів у комп'ютерній сфері вимагає від слідчого грамотної і ефективної роботи із збирання та дослідження речових доказів, документів та іншої матеріально відображуваної інформації про злочин, яка в основному на певних електронно-обчислювальних та програмних носіях. Водночас органи розслідування повинні у повному обсязі отримати та задокументувати вербальну криміналістично значиму інформацію задля встановлення причетності тієї чи іншої особи до вчиненого злочину.

3.2. Експертизи комп'ютерної техніки і програмних продуктів та телекомунікаційних систем і засобів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Активне впровадження використання комп'ютерної техніки та комп'ютерних технологій в службову діяльність державних органів і приватних організацій, неухильно супроводжується поширенням кола кримінальних правопорушень, пов'язаних з їх використанням. Боротьба зі злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і електрозв'язку стає все більш актуальною не тільки для всієї світової спільноти, а й для нашої держави, зокрема.

У світі кожного року вчиняються десятки тисяч кримінальних правопорушень з використанням комп'ютерних технологій, програмних засобів та іншого технологічного обладнання. Кожного дня як у звичайних пересічних громадян, так і у глобальних компаній, викрадають персональні та службові дані,

кошти з особистих або господарських банківських рахунків, незаконно збирають конфіденційну та комерційну інформацію, незаконно блокують діяльність тощо.

Так, відповідно до даних авторитетної американської компанії McAfee, що спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS), незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і електрозв'язку протягом 2020 року коштували світовій економіці понад 1 трильйон доларів або 820 мільярдів євро. В порівнянні із 2018 роком, дослідники зазначають приріст у 50 відсотків. Одним з факторів, що посприяв збільшенню кількості кіберзлочинів, є той, що багато працівників цього року перейшли на віддалену роботу через пандемію, спричинену поширенням коронавірусу SARS-CoV-2 (COVID-2019), й мають віддалений доступ до робочих комп'ютерних систем [53].

Саме тому, результативна, своєчасна та ефективна діяльність у правоохоронних органів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку набуває все більшої важливості для забезпечення нормального функціонування державних і приватних органів та організацій, а також захисту громадян.

Одним з ефективних та, беззаперечно, вирішальних засобів (джерел доказової інформації) у розслідуванні таких злочинів є експертиза комп'ютерної техніки і програмних продуктів, що активно використовується правоохоронними органами багатьох країн світу.

Для ефективного використання можливостей судової експертиза комп'ютерної техніки і програмних продуктів під час розслідування кримінальних правопорушень необхідно, на нашу думку, не тільки володіти інформацією щодо можливості вирішення кола питань (що також є важливим), а також щодо її місця в системі судових експертиз.

В Україні здійснення судово-експертної діяльності із проведення судових експертиз та експертних досліджень регламентується Конституцією України, Законом України «Про судову експертизу» та іншими нормативними актами.

У ст. 1, згадуваного вище Закону, зазначено, що судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об’єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду [137].

Так, відповідно до п 1.2.2. Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої Наказом Міністерства Юстиції України від 08.10.1998 р. № 53/5 експертиза комп’ютерної техніки і програмних продуктів віднесена до класу судових інженерно-технічних експертиз [129].

Також, слід зауважити, що іншим нормативним документом, а саме Положенням про Центральну експертно-кваліфікаційну комісію при Міністерстві юстиції України та атестацію судових експертів, затвердженого наказом Міністерства Юстиції України від 03.03.2015 № 301/5, визначено індекси експертних спеціальностей. Відповідно до положень даного Положення визначено індекс 10.9 «Дослідження комп’ютерної техніки та програмних продуктів», який віднесено до виду комп’ютерно-технічних судових експертиз [133].

Отже, за результатами аналізу зазначених вище нормативних документів, можливо визначити, що судова експертиза комп’ютерної техніки і програмних продуктів відноситься є видом виду комп’ютерно-технічних судових експертиз, що входить до класу інженерно-технічних судових експертиз.

Останнім часом активного поширення набувають нові способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, серед яких можливо виокремити: використання так званих програм-здирників, за допомогою яких зловмисники закодовують дані й вимагають викуп за їх розкодування, фішинг та DoS-атаки, крадіжки Email-акаунтів, використання шпигунського програмного забезпечення, а також викрадення криптовалют, як через не санкціонований доступ до віртуальних клієнтських гаманців, так і через онлайн перехоплення здійснення платежів тощо [163, с. 29].

Процес розслідування кримінальних правопорушень у згадуваній сфері досить часто передбачає маскуванням незаконних дій правопорушників та інших пов'язаних із ними осіб. Нерідко елементами маскування використовують зміну віртуальних адрес персональних комп'ютерів, використання динамічних IP-адрес, зміну ідентифікаційних даних окремих елементів комп'ютерних систем, вчинення кримінальних правопорушень через дистанційне керування технічними засобами тощо.

Саме тому, такі різновиди кримінальних правопорушень вирізняє латентний характер, вони залишають обмежену кількість слідів, які є складними для виявлення, фіксації та вилучення. Зазначені обставини зумовлюють необхідність використання сучасних спеціальних знань у сфері комп'ютерних та інформаційних технологій з метою розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. У переважній більшості випадків призначення і проведення комп'ютерно-технічних судових експертиз є необхідною умовою для ефективного розслідування кримінального провадження.

Проблемні аспекти, пов'язані з протидією, виявленням, використанням спеціальних знань і розслідуванням злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вивчали такі провідні вітчизняні науковці, як В.В. Арешонков, В.М. Атаманчук, В.М. Бутузов, А.А. Вознюк, М.В. Гуцалюк, А.В. Іщенко, О. В. Копан, О.В. Кравчук, С.А. Кузьмін, В.І. Осадчий, М.А. Погорецький, А.А. Саковський, Є.Д. Скулиш, О.А. Федотов, В.Г. Хахановський, С.С. Чернявський, Ю.М. Чорноус, Д.М. Цехан, В.П. Шеломенцев, О.М. Юрченко та ін.

Проте слід констатувати, що на сьогодні бракує ґрунтовних досліджень теоретичних і практичних питань, пов'язаних із застосуванням сучасних інформаційних технологій безпосередньо в судово-експертній діяльності під час проведення комп'ютерно-технічних судових експертиз, визначенням їх завдань та об'єктів.

З огляду на сучасні потреби слідчої та оперативно-розшукової практики правоохоронних органів та досвід роботи підрозділів Експертної служби МВС України, до основних завдань судової експертизи комп'ютерної техніки і програмних продуктів [71, с. 128], на нашу думку, слід віднести такі:

– діагностування апаратних засобів комп'ютерної системи;

– визначення функціонального призначення, характеристик і реалізованих вимог, алгоритму й структурних особливостей, поточного стану представленого програмного системного та прикладного забезпечення;

– пошук, виявлення, аналіз й оцінювання кібернетичної інформації (комп'ютерних даних), підготовленої користувачем або створеної програмами для організації інформаційних процесів у комп'ютерній системі [165, с. 306].

Юридичною підставою проведення судової експертиза комп'ютерної техніки і програмних продуктів є постанова слідчого (прокурора, детектива), що винесена на підставі ст. 243 КПК України або ухвали слідчого судді щодо проведення такого виду експертизи [81] у випадках, коли необхідно встановити фактичні дані, що мають значення для розслідуваного кримінального правопорушення та пов'язані із використанням комп'ютерної техніки або обладнання, та за її допомоги проведені певні дії, що можуть бути виявлені за результатом використання спеціальних знань у галузі програмування та комп'ютерних технологій (див. додаток В). Окремо, слід зазначити, що частина друга вище згаданої статті кримінального процесуального законодавства, також надає право стороні захисту залучати до проведення дослідження фахового судового експерта, щоправда на договірних умовах.

Розглядаючи питання об'єктів судової експертизи комп'ютерної техніки і програмних продуктів, хочемо зауважити, що нині немає однозначної думки як серед науковців, так і серед практикуючих спеціалістів щодо даного питання.

На думку вчених В.Г. Гончаренка та І.В. Гори об'єктами даного виду досліджень можуть бути комп'ютерна техніка з носіями інформації (дискети, жорсткі диски, CDR-диски, флеш-карти тощо), периферійні пристрої (принтери, сканери, звукові карти), програмні продукти. Об'єктами цієї експертизи також

можуть бути пристрої, що не є комп'ютерами в класичному розумінні цього слова, наприклад електронні касові апарати, гральні автомати, карт-рідери тощо [42, с. 314–315]

Так, на офіційній інтернет сторінці Незалежного інституту судових експертиз до об'єктів даного виду експертиз відносять комп'ютерну техніку, периферія (сканери, принтери, плотери, тощо), різноманітні носії інформації (магнітні, оптичні, лазерні, тощо), програмне забезпечення, інша інформація, що знаходиться на носіях і в запам'ятовуючих пристроях (постійних та оперативних), а також органайзери, пейджери, мобільні телефони й інші пристрої, що виготовлені і працюють на основі технологій побудови персональних комп'ютерів [102].

Представники Експертної служби МВС України до об'єктів судової експертизи комп'ютерної техніки і програмних продуктів відносять апаратні засоби (системні блоки комп'ютерів та їх комплектуючі, сервери, ноутбуки, жорсткі диски, флеш-накопичувачі, модеми, маршрутизатори та ін.), так і програмні продукти (комп'ютерні програми, бази даних тощо) [43].

В переважній більшості об'єктами судової експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є засобами вчинення злочинів. Проте, є кримінальні правопорушення, при вчиненні яких об'єктом посягання є не так сам матеріальний предмет, а інформація, що в ньому знаходиться або на якому-небудь носії, або ж власне програмне забезпечення.

У ході проведеного нами дослідження [51, с. 87–88], можна дійти висновків, що об'єкти судової експертизи комп'ютерної техніки і програмних продуктів можливо поділити на три основних види:

1) апаратні об'єкти:

- персональні комп'ютери (у будь-яких варіантах виконання);

- периферійні пристрої до персональних комп'ютерів;

- мережеві апаратні засоби (сервери, робочі станції, комутатори, модеми, роутери й інше серверне обладнання);

- інтегровані системи (мобільні телефони тощо);

- будь-які комплектувальні всіх зазначених вище компонентів (апаратні блоки, блоки живлення, плати розширення тощо).

2) програмні об’єкти:

- системне програмне забезпечення (комплекс програм, призначених для управління роботою обчислювальної системи, розподілу її ресурсів, підтримання діалогу з користувачами, надання їм допомоги в обслуговуванні комп’ютера, а також для часткової автоматизації розроблення нових програм. Поділяють на три основні складові: операційні системи, системи програмування, сервісні програми);

- прикладне програмне забезпечення (комплекс програм, призначених для виконання прикладних завдань фахової діяльності людини (виробничі, наукові, навчальні, розважальні тощо);

3) інформаційні об’єкти:

- текстові й графічні файли, створені з використанням комп’ютерів або мобільних пристроїв;

- аудіовізуальні (мультимедійні) дані;

- інформація у форматах баз даних та іншого прикладного програмного забезпечення [165, с. 307].

Зважаючи на різновиди досліджуваних об’єктів судової експертизи комп’ютерної техніки і програмних продуктів, доцільним, ми вважаємо, можливість виділення трьох відносно самостійних підвидів експертних досліджень:

- дослідження комп’ютерної техніки (встановлює обставини та факти, пов’язані із функціонуванням та експлуатацією комп’ютерних систем);

- дослідження програмних продуктів (встановлює обставини та факти, що пов’язані із методологічними, структурними та апаратними особливостями розробки та використання програмного забезпечення);

- інформаційно-комп’ютерні дослідження (встановлює обставини та факти пов’язані з інформаційною обробкою змісту файлових систем, їх збереження та відтворення на комп’ютерних пристроях зберігання).

Важливою складовою успішного результату розслідування злочинів у сфері у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку є оперативність та повнота здобутих джерел доказової інформації.

Тому, під час призначення експертизи комп’ютерної техніки та програмних продуктів необхідно особливу уваги приділяти періоду та підготовки до призначення судової експертизи, а також враховувати, що внаслідок некоректно поставлених запитань, можуть виникати складнощі як в слідчій так і судовій практиці, що в свою чергу призводить до повернення постанови для уточнення ініціатору, або взагалі обгрунтованого повернення матеріалів без їх виконання.

Тому, формулюючи питання судовому експерту, необхідно дотримуються загальних правил і рекомендацій, що ґрунтуються на класичних принципах криміналістики, а саме:

- запитання мають бути максимально конкретизовані та лаконічні;

- запитання повинні ґрунтуватися на попередньо встановлених процесуальним шляхом фактичних обставинах;

- запитання не повинні виходити за межі спеціальних знань експертної спеціальності судових експертів, що здійснюють конкретну судову експертизу комп’ютерної техніки і програмних продуктів;

- розміщення запитань повинно бути в логічній послідовності (спочатку ті, від вирішення яких буде залежати можливість вирішення інших) [169, с. 407].

На вирішення судової експертизи комп’ютерної техніки і програмних продуктів ставляться такий орієнтований перелік питання:

1) Комп’ютер якої моделі надано на дослідження та які є його технічні характеристики (системного блока та периферійних пристроїв)?

2) Які технічні несправності має наданий на дослідження комп’ютер або його окремі блоки та пристрої та яким чином ці несправності впливають на роботу комп’ютера?

3) Чи міститься на даному носії інформація, яка має ключові слова "..." (зміст ключової інформації зазначається індивідуально у кожному випадку)?

4) Чи міститься на даному носії інформація, в якій є дані про вказані в постанові підприємства або організації)?

5) Коли та ким створені досліджувані файли?

6) Чи є дані програмні продукти ліцензійними копіями загальновідомих систем, чи вони є оригінальними розробками?

7) У який період часу створені файли, та яка дата останнього редагування?

8) Чи вносились до програми даного системного продукту, які- небудь корективи, що змінювали виконання певних операцій?

9) Чи містилися на носії файли, що були згодом знищені? Якщо так, то які саме файли та який їх зміст?

10) З якого з наданих комп’ютерів здійснювався вихід у мережу Інтернет, за якими адресами, в який період часу?

11) Чи містяться на досліджуваному комп’ютері програмні продукти, призначені для злому пароля та несанкціонованого доступу до комп’ютерних систем?

12) Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

13) Яким є рівень професійної підготовки в галузі програмування і роботи з комп’ютерною технікою особи, яка виконала дані дії з комп’ютером та програмним забезпеченням?

14) Чи відповідає стиль програмування досліджуваного програмного продукту стилю програмування певної особи?

15) Чи відповідають прийоми і засоби програмування, що застосовувалися при створенні досліджуваного програмного продукту, прийомам і засобам, якими користується даний користувач?

16) Чи містяться в пам’яті наданих на дослідження мобільних телефонів інформація щодо списку контактів, журналу дзвінків, текстових та мультимедійних повідомлень, веб-історії, повідомлень в мережі Інтернет, а також текстових, графічних, відео файлів користувача?

17) Чи наявні на наданих на дослідження об’єктах програми (клієнти) для дистанційного банківського обслуговування (ДБО) типу «Клієнт-банк», «Інтернет-банкінг»? Якщо так, то чи містять вони лог-файли використання вказаних програм?

18) Чи встановлені на наданих на дослідження об’єктах програми, призначені для спілкування в мережі Інтернет («Viber», «Skype», «Telegram», «WhatsApp» та інші)? Якщо так, то чи містять вони інформацію щодо історії повідомлень та дзвінків?

19) Чи містяться на наданих на дослідження об’єктах серед наявних та видалених файлів інформація щодо ключових слів: «****», «***», «**»? Якщо так то які атрибути (дата та час створення, редагування, друку, видалення тощо) файлів, що містять зазначену інформацію? [43].

Для забезпечення вичерпності висновку судового експерта необхідно забезпечити максимально повний та завершений перелік поставлених на запитань. Проте, вважаємо, що є недопустимим механічне відтворення в документі про призначення експертизи (постанова, ухвала) загального списку запитань, що можуть вирішуватися зазначеним видом судових експертиз.

Тому, вважаємо, що формулюючи питання для вирішення в межах експертизи комп’ютерної техніки та програмних продуктів необхідно дотримуватись таких основних вимог:

- використання загальноприйнятого понятійного апарату (не вживати жаргонні та напівпрофесійні термінологічні одиниці (наприклад, «вінчестер», «логи та паси», «железо» тощо).

- запитання формулюють максимально чітко, щоб судовий експерт мав можливість надати однозначну відповідь. Вони не повинні стосуватися етапів дослідження інформації (опис характеристик носіїв інформації та особливостей

розміщення інформації на них, відновлення й дослідження інформації серед знищених файлів є обов'язковим етапом дослідження інформації), мати довідкове, правове спрямування та виходити за межі компетенції судового експерта певної експертної спеціальності (спеціальних знань).

- запитання мають відповідати чинній методичній і технічній базі, доступній судовому експерту, бути спрямованими на встановлення конкретних обставин події, що належить до предмета доказування, формулюватися так, щоб витрати (фінансові, технічні, часові тощо) на проведення дослідження, коли виконують конкретні завдання розслідування, були мінімальні.

За результатами аналізу судово-експертної практики, можливо виокремити ряд **типових помилок**, що допускають ініціатори проведення експертиз комп'ютерної техніки та програмних продуктів, що як наслідок ускладнює або унеможливлює її проведення. Зокрема:

1) в ході слідчої дії оглядаються та вилучаються не всі об'єкти, які містять інформаційні сліди злочину (23% опитаних респондентів);

2) об'єкти вилучаються, зберігаються чи транспортуються без дотримання відповідних правил (10%);

3) на експертизу надаються об'єкти, які апріорі не можуть містити інформації, що має значення для розслідування, або які з об'єктивних причин неможливо належно дослідити (7%);

4) на вирішення експертизи ставляться питання, які не відносяться до обставин справи або ж є некоректними (35%);

5) однією постановою (ухвалою) призначають експертизи за різними видами об'єктів або ж за їх надмірною кількістю (17%).

Для усунення недоліків (помилок), пов'язаних з проведенням слідчих (розшукових) дій під час розслідування злочинів даної категорії та призначенням експертизи комп'ютерної техніки та програмних продуктів, які ускладнюють або унеможливлюють проведення такої експертизи, потрібні комплексні заходи, що передбачають: 1) постійне підвищення кваліфікації осіб, які здійснюють досудове розслідування злочинів; 2) за можливості до призначення експертизи проведення

огляду об’єктів із залученням фахівця в галузі використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, що дозволить встановити наявність даних, які можуть мати доказове значення у кримінальному провадженні, та у цілому вирішити питання про доцільність подальшого призначення експертизи; 3) узгодження переліку питань за конкретними об’єктами з фахівцями в галузі використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, оптимізацію кількості таких питань та об’єктів, які надаються на експертизу; 4) збільшення кількості наукових розробок та відповідно кількості науково-практичних та методичних видань за вказаною проблематикою; 5) нормативно-правове закріплення різновидів судових експертиз, які проводяться Експертною службою МВС України, визначення питань, які ними можуть бути вирішені, а також вимог до наданих на експертизу матеріалів; 6) розроблення окремого порядку залучення вузькопрофільних спеціалістів (судових експертів) до виконання традиційних експертиз, які безпосередньо не пов’язані з дослідженнями комп’ютерної техніки, але в процесі їх проведення виникає потреба в дослідженні цифрових носіїв інформації та (або) інформаційних слідів на віддалених пристроях збереження даних, серверах, хмарних сховищах тощо.

Окремо слід зазначити, що комп’ютерні системи (особливо сервери) оперують такою кількістю інформації, що за своїми обсягами може дорівнювати, або навіть перевищувати університетські та академічні бібліотеки. А отже, питання щодо визначення та встановлення всього масиву баз даних, що є на ньому, є некоректним, так само як і завдання щодо його роздруківки.

Також слід звертати увагу, що в межах проведення експертизи комп’ютерної техніки та програмних продуктів не вирішуються питання щодо правомірності дій користувачів; ліцензійність програмних продуктів; вартість комп’ютерної техніки та програмних продуктів, оскільки такі питання виходять за межі завдань, що стоять перед даним видом судових експертиз.

Окрім зазначеного, судовий експерт за даним напрямом не розв'язує питання, що не мають змістовного навантаження, наприклад:

– яке цільове призначення інформації;

– чи міститься носії інформація про фінансово-господарську діяльність підприємств;

– хто може використовувати комп'ютер;

– чи наявна на носію контрафактне програмне забезпечення.

З метою оптимізації навантаження на судових експертів за напрямом експертизи комп'ютерної техніки і програмних продуктів, скорочення термінів їх виконання та підвищення якісної ми пропонуємо запровадити **алгоритм підготовчих заходів** під час призначення судових експертиз комп'ютерної техніки та програмних продуктів:

1. Перед призначенням експертизи необхідно провести попередній огляд об'єктів із залученням фахівців (зокрема Експертної служби МВС України) для встановлення наявності даних, що можуть мати доказове значення в кримінальному провадженні, і вирішення питання про доцільність подальшого призначення експертизи

2. Узгодити з фахівцями (судовими експертами) перелік запитань за конкретними об'єктами й оптимізувати їх кількість. Ставити такі запитання, які стосуються безпосередньо об'єктів дослідження в конкретному кримінальному провадженні, виключаючи запитання юридичного змісту й такі, вирішення яких не потребує спеціальних знань.

3. Визначати першочерговість і пріоритети дослідження наданих на експертизу об'єктів.

4. У разі об'єктивної необхідності дослідження значного обсягу різноманітної комп'ютерної техніки (понад 10 одиниць) варто призначати експертизи, поділяючи об'єкти дослідження на групи, або проводити окремі експертизи за кожним об'єктом дослідження [166, с. 25–26]

На нашу думку, врахування запропонованих рекомендацій ініціаторами проведення судових експертиз комп'ютерної техніки і програмних продуктів

неодмінно призведе до зменшення кількості обґрунтованих повернень матеріалів без виконання та зменшить терміни проведення експертних досліджень, що надасть можливість представникам правоохоронних органів оперативно встановлювати істину в кримінальних провадженнях.

Експертиза телекомунікаційних систем (обладнання) і засобів є порівняно новим видом експертного дослідження, що полягає у дослідження цифрових та аналогових приладів з метою встановлення технічних параметрів та стану об'єкта, визначення функціонального призначення (див. Додаток Г).

Згідно загального визначення точки зору всі судові експертизи розподіляються на класи (типи), роди, види та різновиди (підвиди).

Експертиза телекомунікаційних систем (обладнання) і засобів як один із видів експертного дослідження в галузі інформаційних технологій відноситься до класу інженерно-технічних.

До основних *завдань* даного виду експертизи належить:

– визначення характеристик та параметрів телекомунікаційних систем та засобів, у тому числі засобів мобільного зв'язку;

– встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах;

– встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій;

– визначення якості телекомунікаційних послуг;

– встановлення технічного стану телекомунікаційних систем та засобів;

– встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів;

– дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій [129].

Об'єктами дослідження телекомунікаційних систем та засобів є телекомунікаційні системи, засоби, мережі, їх складові частини та інформація, що ними передається, приймається та обробляється [129].

Відповідно до Закону України «Про телекомунікаційні системи», *телекомунікаційні системи* є комплекс програмного та апаратного обладнання, який з'єднаний один із одним в один ланцюг, що здійснює передачу даних з однієї точки в іншу.

Сьогодні виділяють такі основні *різновиди інформаційно-телекомунікаційних мереж*:

– analog transmission (аналогова передача) – передача сигналу, який аналогічний вихідному;

– asymmetric communications (засоби асиметричного зв'язку) – двосторонній зв'язок, в якому обсяг трафіку сильно відрізняється в залежності від напрямку;

– broadband (широкосмуговий) – передача даних по мережі з широкою смугою пропускання.

Телекомунікаційними засобами є технічні засоби телекомунікацій, призначені для маршрутизації, комунікації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, дротових, оптичних чи інших електромагнітних систем між кінцевим обладнанням. Перелік технічних засобів, які можуть застосовуватися в телекомунікаційних мережах відповідно до Закону України «Про телекомунікації» визначається Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформації.

Типові питання, які вирішує експертиза телекомунікаційних систем та засобів:

– якій тип, марка, модель телекомунікаційного засобу (системи)?

– які технічні характеристики (параметри) має телекомунікаційний засіб?

– в який спосіб виготовлений технічний засіб (кустарним шляхом, у заводських умовах)?

– чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт)?

– чи підлягає неробочий технічний засіб відновленню?

– яким є час безперервної роботи технічного засобу?

– які характеристики підключень до мережі має телекомунікаційний засіб?

– з яких частин складається технічний засіб та яке їхнє призначення?

– чи можна за його допомогою здійснювати негласне зняття інформації і якої саме (акустичної, візуально-оптичної, інформації з радіоефіру, з каналів зв'язку, інформації, яка зберігається на матеріально-речовинних носіях)?

– чи створений технічний засіб спеціально з метою негласного отримання інформації?

– в який спосіб технічний засіб дозволяє негласно отримувати інформацію?

– з якої відстані за його допомогою можна здійснювати зняття інформації?

– у який час доби за допомогою даного технічного засобу можна здійснювати зняття інформації?

– якою є кількість абонентів, інформацію від яких дозволяє одночасно негласно отримувати технічний засіб і якими є їхні характеристики (запрограмовані номери телефонів, частоти радіоподовжувачів, специфічні методи закриття каналів передачі інформації тощо)?

– чи здійснює технічний засіб телекомунікаційну функцію?

– чи потребує застосування технічного засобу додаткових засобів телекомунікації (ретрансляторів)?

– на яку відстань технічний засіб може передавати отриману інформацію і яким чином (по дротовому, радіохвильовому, інфрачервоному, ультразвуковому каналові, по закритому чи відкритому каналові, із застосуванням певних частотних діапазонів та видів модуляції тощо)?

– чи є можливим дистанційне керування роботою технічного засобу?

– чи є можливим керування роботою пристрою через засоби телекомунікації?

– чи може технічний засіб фіксувати отриману інформацію і на який тип носія (аудіо-, відеокасету, оптичний чи магнітооптичний диск, дискету, мікросхему тощо)?

– чи необхідне проникнення особи на контрольований об'єкт для впровадження технічного засобу?

– чи був застосований зазначений технічний засіб?

– чи здійснений аудіозапис (відеозапис) на носіях (аудіо-, відеокасетах тощо), вилучених у кримінальному провадженні, за допомогою зазначеного технічного засобу?

– чи мав місце факт доступу до телекомунікаційної системи та в який спосіб?

– чи здатний технічний засіб в процесі функціонування долати систему технічного захисту інформації (ТЗІ)?

– чи дозволяє технічний засіб долати певну систему ТЗІ?

– чи позначається на параметрах технічного засобу робота в умовах дії певної системи ТЗІ і яким чином?

– чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб?

– чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб?

– чи є ознаки втручання в роботу телекомунікаційної системи?

– чи змінювались користувачем телекомунікаційної системи (мережі) налаштування окремих пристроїв, як саме і в який час?

– чи можливо використання телекомунікаційного засобу (обладнання) для вказаних цілей?

– чи могли апаратні засоби об’єднуватись у телекомунікаційну мережу та за якими ознаками?

– яка причина непрацездатності телекомунікаційної системи?

– який загальний характер підключень до телекомунікаційної мережі виконував об’єкт (телекомунікаційна система, засіб)?

– за допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі?

– яка топологія апаратних засобів, об’єднаних у телекомунікаційну систему?

– чи відповідає телекомунікаційна система технічній документації?

– які шляхи маршрутизації даних в телекомунікаційній системі?

– за яким алгоритмом обробляється чи оброблена інформація телекомунікаційним засобом (системою)? [43].

3.3. Оцінка та використання результатів судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Специфіка кримінальних проваджень, пов'язаних з розслідуванням злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку вимагає широкого використання спеціальних знань, без яких слідчому неможливо розібратися в причинах і характері скоєного.

Необхідність застосування наукових, технічних та інших знань у кримінальному процесі пов'язана з тим, що розслідування злочинів є складним процесом пізнання об'єктивної дійсності. А отже, в процесі розслідування події злочину, від слідчого та інших учасників кримінального процесу вимагається застосування спеціальних знань та навичок у певних видах діяльності.

Зміст поняття «спеціальні знання» може бути найбільш повно розкрито тільки в контексті з елементами процесу доказування. Доказування в кримінальному судочинстві здійснюється на основі законів логіки і за допомогою доказів, якими є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність, чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [42, с. 47] .

Існують різні підходи до визначення характеристики знань, це будь-які професійні знання, сукупність знань в певній галузі науки, техніці чи мистецтві, професійні знання, що відповідають сучасному рівню розвитку пізнання в науці, мистецтві чи ремеслі, систематизовані наукові знання, знання які не відносяться

до загальновідомих, знання які засновані теорією і закріплені практикою наукових знань, теоретичні знання, сукупність відомостей, будь-які знання, неправові, науково-професійні знання, знання які притаманні різним видам професійної діяльності тощо [161, с. 54].

На думку Б.В. Романюка, спеціальні знання – це сукупність науково обґрунтованих відомостей окремого (спеціального) виду, якими володіють особи-спеціалісти у рамках будь-якої професії у різних галузях науки, техніки, мистецтва та ремесла, і, відповідно до норм кримінально-процесуального законодавства, використовують їх для успішного вирішення завдань кримінального судочинства [147, с. 67].

М.Г. Щербаковський стверджує, що спеціальні знання – це професійні знання, отримані в результаті навчання, а також навички, здобуті обізнаною особою у процесі практичної діяльності в різних галузях науки, техніки та інших суспільно-корисних галузях людської діяльності, що використовуються разом з науково-технічними засобами при проведенні експертизи [194, с. 46].

Використання спеціальних знань в слідчій і судовій практиці завжди є цілеспрямованою дією. Цільове призначення спеціальних знань в кримінальному судочинстві має не тільки теоретичне, але і практичне значення. Спеціальні знання, які використовуються в межах кримінального провадження, складають наукові основи слідчої і судової діяльності. Чітке їх застосування на кожній стадії кримінального процесу важливо для правильного розуміння функцій і повноважень осіб, які використовують ті чи інші види знань в передбачених законом процесуальних формах [161, с. 54].

Відомий вітчизняний науковець криміналіст В.К. Лисиченко визначив основні цілі використання науки, техніки та спеціальних знань як: 1) отримання необхідних відомостей, що слугують підставою для прийняття обґрунтованих рішень по справі; 2) використання знань спеціалістів для виявлення, закріплення, вилучення доказів і з’ясування спеціальних питань, що виникають при проведенні слідчих дій; 3) дослідження певних об’єктів і явищ для встановлення обставин, що мають значення для правильного вирішення справи [89, с. 36].

В юридичній літературі існують різні підходи до визначення поняття судової експертизи. Передусім судова експертиза – це поняття, яке має узагальнюючий характер і охоплює різні види експертних досліджень.

Серед ознак судової експертизи виокремлюють наступні: 1) використання спеціальних знань; 2) проведення дослідження з метою встановлення обставин, які мають значення для провадження; 3) наявність спеціального суб'єкта експертизи; 4) визначену процесуальну форму; 5) оформлення результатів у процесуальному документі – висновку експерта [3, с. 10].

Відповідно до чинного кримінального процесуального законодавства України, призначення експертизи розглядається, як один із способів використання спеціальних знань у судочинстві. Тобто, на стадії досудового розслідування, судова експертиза сприяє об'єктивності, повноті та всебічності пізнання події і обставин злочину.

Судова практика показує, що розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку представляє значні труднощі, які мають об'єктивні та суб'єктивні причини. До об'єктивних відносяться особливості слідів електронно-обчислювальних машин, комп'ютерних мереж і мереж електрозв'язку, які обумовлюють складність процесу розслідування. Суб'єктивними причинами можуть бути ті обставини, коли слідчі, прокурори і судді ні психологічно, ні технічно, ні професійно не готові до цілеспрямованого і ефективного розслідування вищезазначеної категорії злочинів.

Тому, на нашу думку, успіх розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, їх судового розгляду обумовлений, в першу чергу, ефективним збиранням та дослідження комп'ютерної інформації, яка містить сліди злочину, тобто зміни комп'ютерної інформації, що знаходиться на носіях і в мережах. Вказані сліди неочевидні, тому, безумовно, їх виявлення, фіксація, вилучення та дослідження потребує використання спеціальних знань.

В якості носія можуть виступати мобільні телефони, смартфони, планшети, портативні комп'ютери, персональні комп'ютери та будь-які зовнішні носії інформації: флеш-пам'ять, зовнішні жорсткі диски та багато інших видів носіїв інформації, які передбачають використання в комп'ютерних технологія.

З розвитком глобальних електронних комп'ютерних мереж набула також поширення практика електронного промислового шпигунства. Саме тому, проблеми розробки систем захисту та збереження приватної, державної, службової та комерційної таємниці набувають сьогодні особливого значення. Багато питань виникає у зв'язку з крадіжками різного роду послуг. Також Інтернет широко використовують торгівці піратським програмним забезпеченням, порнографією, зброєю та наркотиками для вчинення власних злочинних дій, обміну інформацією, координації дій тощо. Електронні мережі, окрім всього, можуть стати об'єктом нападу кібершахраїв та кібертерористів [12, с. 64–68].

Ми погоджуємось із О.В. Курманом, який зазначив, що вести мову про незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку можна за сукупністю умов: 1) володільцем інформації повинні бути визначені умови та правила отримання і обробки інформації; 2) власник (розпорядник) електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи оператор (провайдер) мереж електрозв'язку повинні розробити та впровадити заходи захисту інформації в системі; 3) власник (розпорядник) комп'ютерів, систем та оператор (провайдер) мереж повинні розробити правила роботи системи; 4) між власником (оператором, провайдером) системи та володільцем інформації повинен бути укладений договір щодо захисту інформації в системі; 5) злочинець виконав хоча б одну із операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації [84, с. 245–246].

Враховуючи специфіку кіберзлочинів, можна виокремити місця їх вчинення: фізичне середовище (ділянки місцевості) та електронне середовище (вузли мережі), де розташовані:

– програмно-технічні засоби (носії інформації), що зазнали злочинного впливу, та точки їхнього доступу до певних мереж;

– програмно-технічні засоби, які злочинець використовував опосередковано, та точки їх доступу до певних мереж;

– мережні вузли каналів зв'язку, з використанням яких відбувався обмін інформацією між програмно-технічними засобами злочинця та потерпілого [19, с. 112–113].

Переходячи до дослідження електронного середовища (кіберпростору, як головного місця вчинення кіберзлочину), слід погодитися з Л.П. Зверянською, що при здійсненні даних злочинів може бути декілька місць їх вчинення, а саме:

– робоче місце, робоча станція – місце обробки інформації, яка стала предметом злочинного посягання;

– місце постійного зберігання або резервування інформації – сервер або стример (пристрій запису та зберігання даних на магнітній стрічці);

– місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, що знаходиться в іншій точці, при цьому місце використання може збігатися з робочим, але перебувати поза організацією (наприклад при зломі шляхом зовнішнього віддаленого мережевого доступу);

– місце підготовки злочину (розробка вірусів, програм злому, підбору паролів) чи місце безпосереднього використання інформації (копіювання, поширення, спотворення), отриманої в результаті неправомірного доступу до даних, що містяться на пристрої [49, с. 76].

Необхідно зазначити, що суттєвою особливістю кіберзлочинів є те, що для них відсутнє просторове обмеження і вчинення злочину може виходити за рамки однієї держави. Злочин вчиняється в одній державі, а негативні наслідки настають в іншій. Такі злочини набувають транснаціонального характеру. Тобто, для них є властивим наявність іноземного елемента в криміналістичній характеристиці та в кримінально-процесуальних відносинах під час його розслідування [140].

До того ж, як стверджує П.Д. Біленчук, кінцевою метою кожного комп'ютерного злочину є отримання інформації, яка зберігається, передається,

обробляється на комп'ютері у будь-якому вигляді (закодована або ні) та вміщує дані про сфери людської діяльності, а також запропоновані шляхи для ефективної діяльності по розслідуванню транскордонних, трансконтинентальних, транснаціональних, планетарних комп'ютерних злочинів [10].

Судова експертиза – це проведене судовим експертом з використанням спеціальних знань і відповідно до закону дослідження представлених компетентними органами (особою) об'єктів з метою встановлення фактичних даних у справі, що відображаються у висновку експерта, який є джерелом доказів [194].

Таким чином, значення судової експертизи в розслідуванні злочинів визначається важливістю для справи тих обставин, які можуть бути встановлені за допомогою експертного дослідження. Завдання експерта полягає в тому, щоб представити слідству виявлені на основі спеціальних знань відомості про факти, що дозволяють у сукупності з іншими доказами у справі дати кримінально правову оцінку події, що розслідується, встановити винуваться та обставини злочину.

До того ж, в юридичній практиці, судова експертиза визнається основною формою використання спеціальних знань у кримінальному судочинстві. Водночас при розслідуванні кримінального провадження у тому числі і по злочинам з використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку неприпустима підміна судової експертизи іншими процесуальними та непроцесуальними формами використання спеціальних знань.

Як вказує М.Г. Щербаковський, судово-експертна діяльність – це система процесуальних та організаційних процедур, пов'язаних з проведенням судових експертиз [194]. Згідно зі ст. 3 Закону України «Про судову експертизу» судово-експертна діяльність здійснюється на засадах законності, незалежності, об'єктивності та повноти дослідження [137]. Судовою практикою напрацьовано ще низку принципів проведення судових експертиз. До них зрештою належать компетентність судового експерта, взаємодія суб'єктів судово-експертної

діяльності, дотримання безпеки та прав особи при проведенні експертного дослідження.

Отже, ми вважаємо, що судова експертиза досягає свої мети в тому випадку, коли слідчий, прокурор та суд матимуть можливість належним чином використати висновок експерта у кримінальному провадженні. Необхідним для цього являється те, щоб слідчий, прокурор чи суд тобто суб'єкт який призначив експертизу, чітко усвідомив сутність дослідження та правильно, об'єктивно оцінив висновок експерта.

Відповідно до ст. 94 КПК України, слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному і неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності [81].

Тому, висновки яких доходить експерт у процесі проведення експертизи, повинні ґрунтуватися на всебічному вивченні наданих слідчим об'єктів із залученням спеціальних знань та необхідного комплексу засобів, методів та методик дослідження.

Мета оцінки висновку експерта полягає у визначенні фактів, обставин з метою встановлення яких за допомогою спеціальних знань і була призначена та проведена судова експертиза. Під метою дослідження висновку експерта слід розуміти його безпосереднє сприйняття, вивчення та аналіз його змісту. Метою перевірки висновку є порівняння отриманих експертом даних, проміжних і остаточних висновків з іншими доказами в кримінальному провадженні. В свою чергу, перевірка припускає, проведення таким чином процесуальних дій, спрямованих на визначення вірогідності висновку, яка сприяє встановленню інформації про встановлюваний експертом факт.

Оцінка результатів судових експертиз розглядається як діяльність винятково розумова, логічна, а перевірка і дослідження розуміється як здійснення необхідних практичних дій, хоча при цьому також має місце й розумова діяльність. Однак таке розмежування оцінки, перевірки та дослідження доказів не

вирішує даної проблеми в повному обсязі. На наш погляд, розмежувати оцінку, перевірку та дослідження доказів можна відповідно до мети їх застосування в процесі доказування. Це також стосується й висновку експерта як джерела доказів, що розуміється як результат, отриманий на основі вивчення наданих експерту матеріалів кримінального провадження, проведеного з використанням спеціальних знань.

Є.Г. Коваленко характеризує поняття оцінки доказів, як розумову, логічну діяльність відповідних суб'єктів, що спрямовується на пізнання фактів для встановлення істини по справі, яка здійснюється в певних логічних формах відповідно до закону і правового розуміння за їх внутрішнім переконанням, заснованим на всебічному, повному й об'єктивному аналізі всіх обставин справи в їх сукупності, спрямована на встановлення достовірності та належності допустимості й достатності доказів, їх взаємозв'язку і значення для вирішення питань, що становлять предмет доказування [67, с. 27–28].

На наш погляд, дотримання вимог кримінального процесуального законодавства України відносно оцінки висновку експерта в слідчій і судовій практиці реалізуються недостатньо. Це зумовлено різними чинниками, наприклад: по-перше, надмірною довірою слідчого, прокурора, слідчого судді та суду до висновку експерта; по-друге, неможливістю оцінки наукової обґрунтованості висновку експерта особою, яка не володіє спеціальними знаннями в повному та необхідному обсязі по відношенню до висновку експерта, що виходить від особи, яка володіє такими знаннями. Внаслідок чого, органи правосуддя нерідко обмежуються лише ознайомленнями із висновком експерта, не проводячи його повну та об'єктивну оцінку відповідно до вимог, які передбачає кримінальний процесуальний кодекс.

М.С. Строгович зазначав, що в процесі оцінки висновку експерта судом перевіряються: його обґрунтованість, з'ясовуються дані, з яких виходив експерт, хід дослідження, яке привело експерта до даного висновку, методи, які експерт використав в процесі дослідження, а також висновок співставляється з іншими доказами по кримінальному провадженню [160, с. 58].

В.В. Лук'яненко зазначив, що при здійсненні оцінки висновку експерта необхідно звернути увагу на такі ознаки, як: аналіз дотримання процесуального порядку призначення та проведення експертизи; відповідність висновку експерта завданню; аналіз повноти висновку; оцінку наукової обґрунтованості висновку; оцінку фактичних даних, що містяться у висновку експерта з точки зору їх належності до справи [90, с. 92].

Н.І. Клименко зазначив, що висновок експерта не може бути джерелом доказів, якщо не дотримані процесуальні гарантії його достовірності: вимоги закону, що закріплюють обов'язковість експерта діяти в межах компетенції; проводити повне та всебічне дослідження об'єктів; нести відповідальність; регламентація прав та обов'язків експерта, особи, яка проводить дізнання, слідчого, прокурора, суду, обвинуваченого та інших учасників судочинства; охорона прав та законних інтересів; система перевірки та оцінки обґрунтованості висновку експерта [62, с. 56–57].

Під оцінкою висновку експерта розуміється також перевірка допустимості, дійсності та достатності доказів, наукова обґрунтованість методик, повнота, логічна обґрунтованість дослідження та його доказове значення [148, с. 47]. Крім того, діяльність з оцінки висновку експерта виділяють аналіз структури та змісту висновку з погляду його відповідності юридичному, гносеологічному та етичному критеріям, а також зв'язок та відповідність висновку експерта з іншими доказами в кримінальному провадженні [154, с. 138].

Взявши до уваги матеріалів слідчої та судової практики, Верховний Суд України у Постанові №8 від 30.05.1997 р. «Про судову експертизу в кримінальних і цивільних справах» звертає увагу на те, що при перевірці та оцінці експертного висновку суд повинен з'ясувати:

1) чи було додержано вимоги законодавства при призначенні та проведенні експертизи;

2) чи не було обставин, які виключали участь експерта у справі;

3) компетентність експерта, і чи не вийшов він за межі своїх повноважень;

4) достатність наданих експертові об'єктів дослідження;

5) повноту відповідей на порушені питання та їх відповідність іншим фактичним даним;

6) узгодженість між дослідницькою частиною та підсумковим висновком експертизи;

7) обґрунтованість експертного висновку та його узгодженість з іншими матеріалами справи [136].

Оцінка висновку експерта – пов’язана з тим, що слідчі (розшукові) дії, які проводяться у кримінальному провадженні спрямовані на збирання доказової інформації, яка потім може бути використана під час підготовки та безпосереднього проведення експертного дослідження. А також навпаки – інформація, отримана в результаті проведення судової експертизи, враховується під час планування та проведення наступних слідчих (розшукових) дій [183, с.135].

Також Ю.М. Чорноус з приводу даного питання зазначила, що вказані обставини у сукупності з іншою доказовою інформацією оцінюються у кримінальному провадженні, мають значення для оцінки зібраної інформації, планування проведення слідчих (розшукових) дій.

За цих умов оцінка висновку експерта включає:

1) аналіз дотримання процесуального порядку призначення та проведення судової експертизи;

2) визначення відповідності висновку експерта завданню;

3) встановлення повноти та наукової обґрунтованості висновку експерта;

4) визначення відповідності висновку експерта іншим зібраним у кримінальному провадженні доказам;

5) перевірку належності до кримінального провадження даних, що містяться у висновку [183, с. 136–137].

Отже, оцінка висновку експерта може бути підставою для одного із таких рішень:

- визнання висновку експерта повним та обґрунтованим, тобто таким, що має значення по кримінальному провадженню;

- визнання висновку неповним або недостатньо зрозумілим, призначення додаткової експертизи або допиту експерта;

- визнання висновку експерта необґрунтованим або сумнівним відповідно до його правильності, призначення повторної експертизи або інших процесуальних дій [183, с. 137–138].

Ефективність проведення комп'ютерно-технічної експертизи багато в чому залежить від взаємодії слідчого з експертом.

Взаємодія слідчого з експертом при проведенні судових експертиз може здійснюватись як в процесуальній, так і в непроцесуальній (організаційній) формах. Процесуальна форма взаємодії – це форма, прямо передбачена нормами кримінального процесуального кодексу. Непроцесуальна – регламентована різного роду відомчими актами, або не регламентована законом, але витікає з його змісту та суті, застосовується в силу практики, що склалася.

Взаємодія слідчого з експертом в процесі експертного дослідження здійснюється в тих випадках, коли проміжні його результати потребують зміни або постановки додаткових питань експерту, та у випадку, коли у самого слідчого з'являються нові дані, які повинні бути враховані при проведенні експертизи [86, с. 39–40].

Як вірно вказує М. Г. Щербаковський, що присутність слідчого під час проведення комп'ютерно-технічної експертизи має особливе значення. На жорсткому магнітному носії комп'ютера (вінчестері) або оптичному диску може міститися величезний обсяг різноманітної інформації, що виявляється експертом. Оскільки найбільш поширеним завданням експерта є пошук та виявлення інформації на магнітному носії, то її перелік, а тим більше роздруківка в паперовій формі у висновку експерта може зайняти не одну сотню сторінок. Тому для визначення належності виявлених файлів або інформації, що міститься в них, до розслідуваної справи бажана участь слідчого в проведенні експертизи [193, с. 179–180].

На наш погляд, активна участь слідчого у проведенні експертизи і його тісні контакти з експертом служать тому, щоб експерт може використовувати найновіші

досягнення науки і техніки, у чому, в першу чергу, зацікавлений слідчий, який несе персональну відповідальність за доказування у кримінальному провадженні. Він очікує від експерта об'єктивного і достовірного висновку, а для цього повинні застосовуватись при досліджені об'єктів, які відносяться до електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку не тільки передові (на певний період) методи і науково-технічні засоби, а й ті, які з урахуванням всіх обставин справи та зібраних матеріалів забезпечать об'єктивність дослідження цих об'єктів.

В юридичній літературі проблемі оцінки доказів, в тому числі й висновку експерта, присвячена велика кількість наукових праць. В основу поняття оцінки доказів та оцінки висновку експерта в різний період науковцями досліджувались різноманітні обставини. Підходи до розгляду цього питання залежали в основному від розуміння сутності доказів у кримінальному процесі, при чому оцінку висновку експерта наповнюють різноманітним змістом.

Наша позиція є такою, що враховуючи особливість кримінальних проваджень які відносяться до електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку оцінка результатів експертного дослідження повинна включати наступні позиції:

1) перевірку достатності наданих для експертизи об'єктів, оскільки недостатня їх кількість, особливо у випадку вирішення ідентифікаційного питання, може стати причиною помилкового висновку чи відмови від його дачі;

2) якість об'єктів, що визначається відповідністю зразків для експертного дослідження досліджуваним об'єктам, належними способами вилучення, упакування, збереження, транспортування об'єктів експертизи, правильності вихідних даних для експертного дослідження;

3) перевірка доцільності, правомірності застосованих експертом методики, методів дослідження та оцінку їх наукової обґрунтованості. З цією метою визначається: чи відповідає використана експертом методика поставленим перед ним питанням, чи придатна вона для виявлення необхідних властивостей наданих об'єктів, чи знаходить ця методика застосування в експертній практиці;

4) перевірка повноти проведених досліджень, встановлення всіх ознак об’єктів судової експертизи. Для чого визначається: чи всі процедури і види досліджень стосовно об’єкта виконані згідно з обраною методикою;

5) перевірка правильності опису та інтерпретації встановлених ознак об’єктів. В даному випадку визначається: чи кожна виявлена в перебігу експертного дослідження ознака детально описана та оцінена експертом, як з точки зору відображення властивостей об’єкта, так і з точки зору його значущості для вирішення поставленого питання;

6) перевірка наукової обґрунтованості проміжних і підсумкових висновків, що є логічним завершенням оцінки. Для цього встановлюється: чи зроблені проміжні висновки за результатами проведених досліджень, чи достатньо виявлених ознак для цих висновків, чи є остаточні висновки наслідком сукупної оцінки проміжних;

7) визначення фахової компетентності експерта на підставі всебічного аналізу висновку.

Тому в контексті останніх подій у світі, у сфері інформаційних технологій, проблема боротьби із кіберзлочинністю видається досить актуальною і для України. Дослідження такого елемента, як оцінка та використання результатів судових експертиз під час розслідування кримінальних проваджень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку має велике значення для вдосконалення існуючих та створення нових методів.

За необхідності при оцінці висновку експерта рекомендовано отримувати консультаційно-довідкову допомогу експерта, який проводив експертизу, або залучати спеціаліста у сфері електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, який не приймав участі у збиранні доказів та проведенні досліджень та жодним чином не зацікавлений у результатах провадження.

Оскільки на етапі досудового розслідування обов’язок щодо оцінки зібраних доказів, у тому числі висновків судових експертів, та вирішення питання їх

достатності для завершення розслідування покладається насамперед на слідчих та детективів, то для розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, враховуючи існуючу їх специфіку, на нашу думку, має бути запроваджено відповідну спеціалізацію слідчих Національної поліції України, а також у вимогах до цих посад крім юридичної слід передбачити необхідність професійно-технічної або вищої технічної освіти принаймні початкового рівня (короткого циклу) за відповідним напрямом. Спеціалізація дозволить напрацьовувати досвід розслідування, а вимога до спеціальної освіти буде сприяти високому рівню кваліфікації, що необхідно як для оцінки результатів судових експертиз, так і для повноти, всебічності та об'єктивності розслідування у цілому.

Ми вважаємо, що тільки внаслідок всебічної, взаємопов'язаної оцінки висновку експерта (як з процесуальної сторони, так і зі спеціальної сторони) слідчий або суд зможуть переконатися в його належності, допустимості, достовірності та достатності, а також визначити його значення для кримінального провадження та співставити з іншими доказами, що закріплені у кримінальному провадженні.

Окрім збирання та оцінки доказів, важливим у розслідуванні є правильне використання зібраної інформації. На нашу думку, використання висновків судових експертиз як джерела доказів при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можливо за такими напрямами: 1) забезпечення потреб розслідування: кримінально-правової кваліфікації злочину; висунення версій та їх перевірки; планування та організації розслідування у цілому та окремих слідчих (розшукових) дій; з'ясування фактів (обставин) кримінального правопорушення; збирання та перевірки доказів; обґрунтування процесуальних дій, рішень; 2) забезпечення експертної профілактики кіберзлочинності; попередження слідчих та експертних помилок, призначення та проведення експертизи комп'ютерної техніки та програмних продуктів та інших судових експертиз.

Висновки до розділу 3

1. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є одними із складних антисоціальних явищ у суспільстві, що охоплюють майже усі сфери життєдіяльності людини та безпосередньо торкаються такого поняття як інформаційна безпека. Ефективне розкриття та розслідування цих кримінальних правопорушень в першу чергу потребує якісного залучення до процесу розслідування кваліфікованих фахівців у галузі використання комп'ютерних технологій.

На сьогодні криміналістичною науковою практично не вироблено рекомендацій, які б стосувалися особливостей розслідування і проведення судових експертиз по цим категоріям справ. Пояснюється це перш за все новизною існуючої проблеми, доступністю та стрімким ростом різновидів комп'ютерно-мобільних пристроїв, їх сервісів та засобів мобільного зв'язку.

Логічне завершення розслідуваних злочинів у сфері інформаційно-комп'ютерних технологій залежить від своєчасного і грамотного проведення необхідних експертиз. Окрім традиційних: дактилоскопічних, трасологічних, фоноскопічних, фінансово-економічних, техніко-криміналістичних експертиз документів тощо, важливе значення має спеціалізовані експертизи, які вирішують ряд пошукових діагностичних та ідентифікаційних завдань які стосуються дослідження як електронно-обчислювальної техніки так й криміналістичної інформації яку вони містять.

У зв'язку з тим, що залежно від конкретної ситуації розслідування може існувати потреба в значній кількості експертних досліджень за різними експертними спеціальностями (видами та підвидами судових експертиз), які мають свої особливості, до того ж проводяться інколи різними експертними установами чи підрозділами та в достатньо тривалі терміни, особливого значення набуває послідовність їх призначення, правильність визначення суб'єкта їх проведення, а також підготовки матеріалів. З цією метою важливими є як знання та досвід самого слідчого, який набувається у процесі початкового навчання,

підвищення кваліфікації, службової підготовки, самоосвіти та практичної роботи, так і консультативно-довідкове супроводження розслідування особами, які володіють спеціальними знаннями (слідчі-криміналісти, інспектори-криміналісти, співробітники кіберполіції, судові експерти за напрямами тощо).

2. Основними процесуальними засадами дослідження цієї інформації є проведення експертизи комп'ютерної техніки і програмних продуктів та експертизи телекомунікаційних систем і засобів. Родовим предметом вказаних експертиз є фактичні дані, які встановлюються за допомогою спеціальних знань в галузі комп'ютерних технологій і включають характеристику, властивості технічних комп'ютерно-телекомунікаційних засобів, програм та даних, їх ідентифікацію, особливості функціонування тощо.

У свою чергу, експертизу комп'ютерної техніки і програмних продуктів можливо розділити на два підвиди: – експертизу комп'ютерної техніки та її даних; – експертизу програмного забезпечення.

3. Запропоновано *алгоритм підготовчих заходів* під час призначення судових експертиз комп'ютерної техніки та програмних продуктів: а) перед призначенням експертизи необхідно провести попередній огляд об'єктів із залученням фахівців (зокрема Експертної служби МВС України) для встановлення наявності даних, що можуть мати доказове значення в кримінальному провадженні, і вирішення питання про доцільність подальшого призначення експертизи; б) узгодити з фахівцями (судовими експертами) перелік запитань за конкретними об'єктами й оптимізувати їх кількість. Ставити такі запитання, які стосуються безпосередньо об'єктів дослідження в конкретному кримінальному провадженні, виключаючи запитання юридичного змісту й такі, вирішення яких не потребує спеціальних знань; в) визначати першочерговість і пріоритети дослідження наданих на експертизу об'єктів; г) у разі об'єктивної необхідності дослідження значного обсягу різноманітної комп'ютерної техніки (понад 10 одиниць) варто призначати експертизи, поділяючи об'єкти дослідження на групи, або проводити окремі експертизи за кожним об'єктом дослідження.

Експертиза телекомунікаційних систем (обладнання) і засобів є порівняно новим видом експертного дослідження, що полягає у дослідження цифрових та аналогових приладів з метою встановлення технічних параметрів та стану об’єкта, визначення функціонального призначення.

4. Сутність висновку експерта полягає в тому, що він є заснованим на завданні слідчого, прокурора, слідчого судді або суду, сформульованому в постанові (ухвалі) про призначення експертизи, виклад експертом фактичних даних, що мають доказове значення для справи та які встановлюються ним на основі застосування спеціальних знань в процесі експертного дослідження.

Правильне оформлення висновку експерта як з логічної, так і процесуальної сторони має досить суттєве значення для оцінки його органом слідства, прокурором, слідчим або судом. Достовірно встановлені обставини, які посприяли формуванню висновку експерта, можуть використовуватись як непрямий доказ, що повинен бути оцінений на підставі принципів оцінки доказів, передбачених законом, та на розсуд слідчого, прокурора, слідчого судді або суду може бути покладений в основу своїх рішень.

Повнота проведеного дослідження потребує того, щоб судовий експерт зазначав у такому висновку всі без винятку ознаки, що були виявлені ним під час проведення судової експертизи. Тому експерт повинен, оцінюючи ознаки, щодо речових доказів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку пояснити, чому, на підставі яких даних він прийшов до того чи іншого висновку.

ВИСНОВКИ

У **висновках** дисертації сформульовано наукові положення та отримано результати, які в сукупності розв’язують важливе наукове завдання розроблення теоретичних положень та науково обґрунтованих рекомендацій щодо техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Найсуттєвішими з них є такі:

1. На сучасному етапі питання розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку досить детально розроблені у кримінально-правовій, кримінально процесуальній та адміністративно-правовій науці. Водночас у криміналістиці більшість наукових праць присвячено загальному дослідженню використанню спеціальних знань при розслідуванні злочинів, учинених із застосуванням комп’ютерних технологій, особливостям встановлення обставин, які підлягають доказуванню у справах про комп’ютерні злочини; окремого комплексного дослідження техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку не проводилось.

2. Зміст техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку становлять мета, на досягнення якої спрямовується така діяльність, а також завдання як окремі напрями досягнення такої мети, які полягають у виявленні, збиранні, фіксації доказової інформації; подальшому аналізі такої інформації; залученні до слідчих (розшукових), негласних слідчих (розшукових) дій компетентних осіб; техніко-криміналістичному супроводі, який здійснюється в організаційних і процесуальних формах під час досудового розслідування; оснащенні уповноважених суб’єктів сучасними техніко-криміналістичними засобами; формуванні в таких суб’єктів умінь і навичок практичного застосування криміналістичної техніки. Суб’єктів

техніко-криміналістичного забезпечення за статусом розподілено на індивідуальні (слідчі, дізнавачі, слідчі-криміналісти, спеціалісти, працівники кіберполіції, оперативних та оперативно-технічних підрозділів, експерти) і колективні (слідчо-оперативна група, слідча група, судово-експертні установи, група експертів).

3. Перспективними напрямами використання зарубіжного досвіду боротьби з кіберзлочинами у вітчизняній науці та практиці розслідування злочинів є: удосконалення правового регулювання протидії кіберзлочинам; залучення цивільних фахівців у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку до вирішення завдань техніко-криміналістичного забезпечення розслідування кіберзлочинів (досвід Німеччини); запровадження інституту консультантів, які вивчають обставини конкретного кримінального провадження, аналізують наявну доказову базу і надають рекомендації слідчим щодо доцільності дослідження конкретних речових доказів, визначення виду експертиз та послідовності їх призначення (досвід Великої Британії); налагодження взаємодії правоохоронних та інших державних інституцій у сфері протидії кіберзлочинності (досвід Франції); залучення міжнародної технічної допомоги (зокрема, для проведення транскордонного обшуку в комп'ютерних мережах), пов'язаної з техніко-криміналістичним забезпеченням протидії кіберзлочинам в Україні. Також перспективним і доцільним є запровадження в діяльність судово-експертних установ України «Глобальних керівних принципів лабораторій цифрової криміналістики», підготовлених й опублікованих Інтерполом (INTERPOL Global guidelines for digital forensics laboratories), які схвалені та рекомендовані до впровадження Європейською мережею криміналістичних установ (European Network of Forensic Science Institutes).

4. Техніко-криміналістичні засоби розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – це система спеціально виготовлених або пристосованих приладів, пристроїв, засобів вимірювальної техніки, допоміжного обладнання, інструментів, матеріалів, інформаційних пошукових,

ідентифікаційних та інших систем, криміналістичних технологій їх застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів, а також здійснення інших дій з виявлення, розслідування та попередження злочинів. Видами цих техніко-криміналістичних засобів є апаратні та програмні засоби мобільної криміналістики; апаратні блокиратори запису; програмні засоби копіювання даних; програмні засоби комп'ютерної експертизи; апаратні засоби відновлення даних; відкрите спеціалізоване програмне забезпечення; дистрибутиви на основі Linux.

5. Оскільки відображенням об'єктивної сторони складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є поряд з «традиційними» й інформаційні сліди, важливим аспектом проведення слідчих (розшукових) дій є те, що інформація або доступ до неї можуть бути втрачені після відключення електронного пристрою (енергозалежні дані, спеціальні програми для знищення даних тощо) або ж зберігатися на серверах чи пристроях, що розташовані в іншому місці, у тому числі поза межами проведення слідчої (розшукової) дії та навіть поза межами України (використання зовнішніх пристроїв збереження даних, хмарних сховищ тощо). У зв'язку з цим, існує потреба в проведенні кваліфікованого виявлення, фіксації та вилучення такої інформації або ж її носіїв, ужитті заходів щодо недопущення стороннього (зовнішнього) впливу на електронні сліди злочину (наприклад, відключення електроенергії, віддаленого доступу до файлів та керування системою тощо), готовності органів розслідування оперативно проводити слідчі (розшукові) дії в інших місцях, де може зберігатися цифрова інформація.

Особливістю розслідування злочинів даної категорії є обов'язкове залучення як спеціаліста фахівця (фахівців) у галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку й використання ним, за необхідності, спеціальних техніко-криміналістичних засобів, що загалом обумовлено специфікою виявлення, фіксації

та вилучення електронних слідів злочину (опис у протоколі процесуальної дії, фото-, відеофіксація, копіювання на зовнішній носій інформації), а також у деяких випадках прямим згадуванням на це у КПК України (ч. 2 ст. 168). Залежно від конкретної ситуації, це може бути як судовий експерт за напрямом комп'ютерно-технічної та (або) телекомунікаційної експертизи, так й інші особи, які володіють відповідними спеціальними знаннями та навичками використання техніко-криміналістичних засобів, наприклад, фахівець з експлуатації або створення конкретних програмних засобів або ж з технічної експлуатації і ремонту певного обладнання. Така участь працівників Експертної служби МВС України має бути нормативно врегульована на відомчому рівні (наказ МВС України від 03 листопада 2015 р. № 1339) з обов'язковим залученням комп'ютерно-технічної лабораторії у складі спеціалізованої пересувної лабораторії та спеціалістів відповідного профілю до участі у проведенні оглядів місць подій. За необхідності залучення фахівців недержавних підприємств, установ та організацій таке залучення має бути заздалегідь узгоджено та організовано. У зв'язку із зазначеним, важливим елементом у проведенні слідчих (розшукових) дій є їх підготовчий етап, який дозволяє забезпечити участь потрібного фахівця та наявність необхідних технічних засобів.

6. Важливою передумовою залучення спеціаліста до проведення негласних слідчих (розшукових) дій під час розслідування злочинів даної категорії правопорушень у випадку, якщо інформація, яка буде досліджуватись, належить до державної таємниці, є наявність у нього допуску до державної таємниці відповідної форми. До того ж, з метою захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій, запропоновано доповнити ст. 254 КПК України положенням такого змісту: «У випадку залучення спеціаліста у протоколі негласної слідчої (розшукової) дії зазначається, що йому роз'яснено його зобов'язання, передбачені ч. 5 ст. 77 КПК України, зокрема щодо нерозголошення відомостей, які стали відомі спеціалісту у зв'язку з виконанням його обов'язків».

Щодо техніко-криміналістичних засобів, які застосовуються при проведенні негласної слідчої (розшукової) дії, потребує уточнення ч. 2 ст. 266 КПК України, у

якій має бути передбачено: «Первинні носії інформації (за можливості від'єднання такого носія від технічного пристрою) долучаються до протоколу негласної слідчої (розшукової) дії. У всіх інших випадках з отриманої інформації знімається копія, яка долучається до протоколу, з фіксуванням у ньому хеш-суми скопійованих файлів. Відповідно, первинні носії інформації й технічні засоби її отримання повинні зберігатися до набрання законної сили вироком суду з позначенням місця зберігання, відповідальної особи та її попередженням про це в протоколі негласної слідчої (розшукової) дії».

7. У зв'язку з тим, що залежно від конкретної ситуації розслідування може існувати потреба в значній кількості експертних досліджень за різними експертними спеціальностями (видами та підвидами судових експертиз), які мають свої особливості, до того ж проводяться інколи різними експертними установами чи підрозділами та в достатньо тривалі терміни, особливого значення набуває послідовність їх призначення, правильність визначення суб'єкта їх проведення, а також підготовки матеріалів. З цією метою важливими є як знання та досвід самого слідчого, який набувається у процесі початкового навчання, підвищення кваліфікації, службової підготовки, самоосвіти та практичної роботи, так і консультативно-довідкове супроводження розслідування особами, які володіють спеціальними знаннями (слідчі-криміналісти, інспектори-криміналісти, співробітники кіберполіції, судові експерти за напрямами тощо).

8. Для усунення недоліків (помилок), пов'язаних з проведенням слідчих (розшукових) дій під час розслідування злочинів даної категорії і призначенням експертизи комп'ютерної техніки та програмних продуктів, які ускладнюють або унеможливлюють проведення такої експертизи, потрібні комплексні заходи, що передбачають: 1) постійне підвищення кваліфікації осіб, які здійснюють досудове розслідування злочинів; 2) за можливості до призначення експертизи проведення огляду об'єктів із залученням фахівця в галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що дасть змогу встановити наявність даних, які можуть мати доказове значення у кримінальному провадженні та загалом вирішити питання

щодо доцільності подальшого призначення експертизи; 3) узгодження переліку питань за конкретними об'єктами з фахівцями в галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, оптимізацію кількості таких питань та об'єктів, які надаються на експертизу; 4) збільшення кількості наукових розробок та, відповідно, кількості науково-практичних і методичних видань за вказаною проблематикою; 5) нормативно-правове закріплення різновидів судових експертиз, які проводить Експертна служба МВС України, визначення питань, які вони можуть вирішити, а також вимог до наданих на експертизу матеріалів; 6) розроблення окремого порядку залучення вузькопрофільних спеціалістів (судових експертів) до виконання традиційних експертиз, які безпосередньо не пов'язані з дослідженнями комп'ютерної техніки, але в процесі їх проведення виникає потреба в дослідженні цифрових носіїв інформації та (або) інформаційних слідів на віддалених пристроях збереження даних, серверах, хмарних сховищах тощо.

9. Оскільки на етапі досудового розслідування обов'язок щодо оцінки зібраних доказів, у тому числі висновків судових експертів, та вирішення питання їх достатності для завершення розслідування покладається насамперед на слідчих та детективів, то для розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, враховуючи існуючу їх специфіку, має бути запроваджено відповідну спеціалізацію слідчих Національної поліції України, а також у вимогах до цих посад крім юридичної слід передбачити необхідність професійно-технічної або вищої технічної освіти принаймні початкового рівня (короткого циклу) за відповідним напрямом.

Використання висновків судових експертиз як джерела доказів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можливо за такими напрямами: 1) забезпечення потреб розслідування кримінально-правової кваліфікації злочину, висунення версій та їх перевірки, планування й організації розслідування загалом та окремих слідчих (розшукових) дій, з'ясування фактів

(обставин) кримінального правопорушення, збирання та перевірки доказів, обґрунтування процесуальних дій, рішень; 2) забезпечення експертної профілактики кіберзлочинності, попередження слідчих та експертних помилок, призначення і проведення експертизи комп'ютерної техніки та програмних продуктів й інших судових експертиз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агафонов В. В., Филипов А. Г. Криминалистика. Вопросы и ответы: учеб. пособие. 3 изд., испр. и доп. М.: Закон и право, 2002. 224 с.

2. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. 304 с.

3. Актуальні питання призначення та проведення експертиз: наук.-практ. посіб. / за заг. ред. І. І. Присяжнюка. Київ: Нац. акад. прокуратури. 2017. 300 с.

4. Астапкина С. М., Дубровицкая Л. П., Плесовских Ю. Г. Участие специалиста-криминалиста в расследовании преступлений: учеб. пособие. М.: УМЦ при ГУК МВД РФ, 1992. 136 с.

5. Баев О. Я. Тактика следственных действий: монография. Воронеж: ЮЛ, 1992. 348 с.

6. Бахін В. П., Весельський В. К. Тактика допиту: навч. посіб. Київ: НВТ «Правник», 1997. 64 с.

7. Безуглий Л. А. Запобігання незаконному відтворенню та розповсюдженню комп'ютерних програм і баз даних: автореф. дис. ... канд. юрид. наук. Київ, 2013. 19 с.

8. Белкин Р. С. Ленинская теория отражения и методологические проблемы советской криминалистики. М.: Изд-во ВШ МВД СССР, 1970.130 с.

9. Бідняк Г. С. Використання спеціальних знань при розслідуванні шахрайств: дис. … канд. юрид. наук. Дніпро, 2018. 238 с. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/rada/dissertations/19/1.pdf.

10. Біленчук П. Д. Криміналістика нового тисячоліття. *Юридичний Вісник України*. 2017. № 346 (1167). С. 14–15.

11. Біленчук П. Д., Гель А. П., Семаков Г. С. Криміналістична тактика і методика розслідування окремих видів злочинів: монографія. Київ, 2007. 512 с.

12. Біленчук П. Д., Лихова С. Я. Криміналістична характеристика кіберзлочинності. *Актуальні питання судової експертології, криміналістики та*

кримінального процесу: матеріли міжн. наук.-практ. конф. (м. Київ, 5 листоп. 2019 р.) за заг. ред. О. Г. Рувіна, Н. В. Нестор та ін. Київ: КНДІСЕ Мінюста України, 2019. 672 с. С. 64–68.

13. Білобров Т. В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України: дис. … канд. юрид. наук. Київ, 2020. 209 с.

14. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96–102. URL: http://pravoisuspilstvo.org.ua/archive/2020/3_2020/20.pdf.

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

16. Бондар В. С. Проблеми теорії і практики використання спеціальних криміналістичних знань в розслідуванні крадіжок з проникненням у житло: дис. … канд. юрид. наук. Київ, 2008. 227 с.

17. Борьба с преступностью в Интернете (онлайновая преступность). *Інформаційний бюлетень Міжвід. наук.-дослід. центру з проблем боротьби з орг. злочинністю*. 2006. № 7. С. 133–141.

18. Бугаев К. В. О понятии технико-криминалистического обеспечения раскрытия и расследования преступлений. *Криминалистика: актуальные вопросы теории и практики*: сборник материалов Третьего Всероссийского «круглого стола» (17–18 июня 2004 г.) (дополнение). Ростов-на-Дону: РЮИ МВД России, 2004. URL: http://nenuda.ru/o-понятии-технико-криминалистического-обеспечения-раскрыти.html (дата звернення: 10.11.2021).

19. Бутузов В. М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку при проведенні дослідчої перевірки: наук.-практ. посіб. Київ, 2010. 245 с.

20. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп’ютерній злочинності. *Боротьба з організованою*

злочинністю і корупцією (теорія і практика). Київ: МНДЦ, 2009. № 19. С. 240–247.

21. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія / Рада нац. безпеки і оборони України. Київ: КИТ, 2010. 408 с.

22. Бутузов В. М. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2007. № 17. С. 316–325.

23. Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні: дис. канд. юрид. наук. Дніпропетровськ, 2012. 203 с.

24. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.

25. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / уклад. і голов. ред. В. Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2009. 1736 с.

26. Використання спеціальних знань під час розслідування несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку: метод. рек. / С. С. Охріменко, О. С. Тарасенко, О. М. Стрільців. Київ: Нац. акад. внутр. справ, 2017. 64 с.

27. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навч. посіб. / А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов. Київ, 2017. 148 с.

28. Виявлення, припинення та розслідування зловживань владою або службовим становищем в ОВС: метод. рек. О. С. Тулаєв, С. С. Чернявський, А. А. Вознюк та ін. Київ: Нац. акад. внутр. справ, 2014. 130 с.

29. Волынский В. А. Технико-криминалистическое обеспечение раскрытия и расследования преступлений: учеб. пособие. М.: ВНИИ МВД РФ, 1994. 80 с.

30. Гавловський В. Д., Тітуніна К. В. Актуальні питання міжнародного співробітництва у боротьбі з комп'ютерною злочинністю. *Організація протидії у сфері інтелектуальної власності та комп'ютерних технологій*: доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвід. сем. Київ, 2009. С. 36–42.

31. Германия поделится с НАТО своими кибервозможностями. SecurityLab.ru. *Новости*. Электронный ресурс. URL: https://www.securitylab.ru/news/497967.php.

32. Голубєв В. О. Деякі особливості тактики окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Підприємництво, господарство і право*. 2003. № 8. С. 109–112.

33. Голубєв В. О. Кримінологічна характеристика злочинів у сфері використання комп'ютерних технологій. URL: https://www.crime-research.org/library/Gol_tem2.htm.

34. Гончаренко В. И. Научно-технические средства в следственной практике: учеб. пособие. Київ: Вища школа, 1984. 149 с.

35. Гора І. В. Сучасні проблеми техніко-криміналістичного забезпечення розкриття й розслідування злочинів органами Служби безпеки України. *Криміналістика XXI століття*: тези доп. міжнар. наук.-практ. конф. (Харків, 25–26 листоп. 2009 р.). Харків: Право, 2010. С. 120–124.

36. Грамович Г. И. Криминалистическая техника (научные, правовые, методологические, организационные основы): монография. Минск: Акад. МВД Респ. Беларусь, 2004. 214 с.

37. Грібов М. Л. Зміст криміналістичного забезпечення негласних слідчих (розшукових) дій. *Вісник кримінального судочинства*. 2017. № 1. С. 35– 41.

38. Грубий М. В. Шляхи вдосконалення міжнародного співробітництва у сфері протидії кіберзлочинності. *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення*: матеріали всеукр. наук.-практ. конф. (9 груд. 2011 р.). Донецьк, 2012. С. 39–42.

39. Деякі питання надання платних послуг науково-дослідними установами судових експертиз Міністерства юстиції: постанова Кабінету Міністрів України: від 27 лип. 2011 р. № 804. Дата оновлення: 01.09.2021. URL: https://zakon.rada.gov.ua/laws/show/804-2011-п#Text (дата звернення: 01.12.2021).

40. Директива ЕС 2016/1148 Европейского парламента и Совета от 06.07.2016 г. о мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем в рамках Союза. *Доступ к законодательству Европейского Союза*. URL: https://eurlex.europa.eu/eli/dir/2016/1148/oj.

41. Дмитриева Т. Ф. О соотношении понятий «технико-криминалистическое обеспечение» и «технико-криминалистическое сопровождение» раскрытия и расследования преступлений. *Вестник Полоцкого государственного университета*. Серия D. 2010. № 4. С. 251–255.

42. Експертиза у судочинстві України: наук.-практ. посіб. / за заг. ред. В. Г. Гончаренка, І. В. Гори. Київ: Юрінком Інтер, 2015. 504 с.

43. Експертна служба МВС України. Офіційний Інтернет ресурс. URL: https://dndekc.mvs.gov.ua/BD.

44. Єзерський Р. Б. Криміналістична техніка та її роль у розкритті і розслідуванні злочинів: автореф. дис. … канд. юрид. наук. Київ, 2005. 20 с.

45. Єзерський Р. Б. Криміналістична техніка та її роль у розкритті і розслідуванні злочинів: дис. … канд. юрид. наук. Львів, 2005. 254 с.

46. Жевелєва І. С. Зарубіжний досвід взаємодії правоохоронних органів із суб'єктами господарювання у процесі захисту інформації з обмеженим доступом. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 1. С. 140–145.

47. Журба А. І. Особливості предмету доказування у справах про комп'ютерні злочини. автореф. дис. … канд. юрид. наук. Харків, 2008. 17 с. URL: https://otherreferats.allbest.ru/law/00593254_0.html.

48. Захарко А. В. Неізоляційні запобіжні заходи в кримінальному процесі України: дис. … канд. юрид. наук. Дніпропетровськ: Дніпропетровський держ. ун-т внутр. справ, 2010. 229 с.

49. Зверянская Л. П. Проблемы выявления и расследования киберпреступлений: монография. Красноярск. 2016. 176 с.

50. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf.

51. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз: наук.-практ. посіб. / Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін. Київ: ПАЛИВОДА А.В., 2019. 168 с.

52. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / кол. авт.: В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за заг. ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. 238 с.

53. Інтернет ресурс dw.com. URL: https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766

54. Іщенко А. В. Методологічні проблеми криміналістичних наукових досліджень: монографія / за ред. І. П. Красюка. Київ: Вид. НАВСУ, 2003. 359 с.

55. Карпенко Д. О. Техніко-криміналістичне забезпечення розслідування злочинів, пов'язаних з порушенням правил безпеки руху або експлуатації транспорту: дис. ... канд. юрид. наук. Харків, 2017. 201 с.

56. Карпушин С. Ю. Проведення слідчих (розшукових) дій: дис. … канд. юрид. наук. Київ: Нац. акад. внутр. справ, 2016. URL: http://elar.naiau.kiev.ua/bitstream/123456789/1421/1/karpushin_dis.pdf.

57. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину): дис. … канд. юрид. наук. Луганськ, 2002. 175 с.

58. Касаткин А. В. Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дисс. ... канд. юрид. наук. М., 1997. 24 с.

59. Катков С. А. Тактика подготовки и назначения программно-технических експертиз. *МИ МВД РФ*. 1995. № 1. С. 48.

60. Киберготовность Германии 2.0: киберпреступность и охрана правопорядка. *Digital*. URL: https://digital.report/kibergotovnostgermanii-2-0-kiber-prestupnost-i-ohrana-pravoporyadka/.

61. Кибер-преступность. ФБР: URL: https://www.fbi.gov/investigate/cyber.

62. Клименко Н. І. Зміни в правовому регулюванні судово-експертної діяльності. *Криміналістичний вісник*: наук.-практ. зб. / ДНДЕКЦ МВС України; НАВСУ; редкол.: Я. Ю. Кондратьєв (голов. ред.) та ін. Київ: «Чайка», 2005. № 1 (3). С. 56–69.

63. Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672.

64. Коваленко А. В. Класифікація оперативно-технічних засобів у теорії оперативно-розшукової діяльності. *Вісник Нац. ун-ту внутр. справ*. 2004. Вип. 26. С. 28–35.

65. Коваленко В. В. Актуальні проблеми застосування науково-технічних засобів спеціалістами при провадженні слідчих дій: дис. … канд. юрид. наук. Київ, 2004. 253 с.

66. Коваленко В. В. Поняття і сучасна класифікація науково-технічних засобів, використовуваних у судочинстві. Застосування науково-технічних засобів спеціалістами при проведені слідчих дій: монографія. Луганськ: РВВ ЛДУВС, 2007. 208 с. URL: http://www.ukr.vipreshebnik.ru/kriminalistika-ta-kriminologiya/37-ponyattya-i-suchasna-klasifikatsiya-naukovotekhnichnikh-zasobiv-vikoristovuvanikh-u-sudochinstvi.html

67. Коваленко Є. Г. Теорія доказів у кримінальному процесі України: підручник. Київ: Юрінком Інтер, 2006. 632 с.

68. Козак Н. Криміналістичні аспекти поняття «комп'ютерні злочини». *Підприємництво, господарство і право*. 2013. № 2. С. 23–28.

69. Колесниченко А. Н. О первоначальных (неотложных) следственных действиях при расследовании преступления. *Криминалистика и судебная экспертиза*. 1964. № 1. С. 7–9.

70. Комп'ютерна злочинність: навч. посіб. / П. Д. Біленчук, Б. В. Романюк , В. С. Цимбалюк та ін. Київ: Атіка, 2002. 385 с. URL: https://library.nlu.edu.ua/poln_text/knigi/komp_zlo_2002.htm.

71. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. URL: https://library.nlu.edu.ua/POLN_TEXT/KNIGI/KOMP_ZLO_2002.htm

72. Комп'ютерні злочини у США. Центр исследования проблем компьютерной преступности. https://www.crime-research.ru/library/usa_crime.htm.

73. Компьютерные технологии в юридической деятельности: учеб.-практ. пособие / К. Е. Зинченко, Л. Ю. Исмаилова, А. Н. Караханьян и др.; под ред. Н. С. Полевого, В. В. Крылова. М.: МГУ, 1994. С. 25–49.

74. Кони А. Ф. Суд – наука – искусство (из воспоминаний судебного деятеля). Петроград. Полярная звезда. 1923. 68 с.

75. Криминалистика: учеб. пособие / Б. М. Шавер, А. И. Винберг и др. М.: Юрид. изд-во НКЮ СССР. 1940. 200 с.

76. Криминалистика: учебник / под ред. А. Ф. Волынского. М.: Закон и право; ЮНИТИ-ДАНА, 1999. 615 с.

77. Криміналістика: підручник / В. В. Пясковський та ін. Київ: «Центр учбової літератури», 2015. 544 с.

78. Криміналістика: підручник / В. М. Глібко, А. Л. Дудніков, В. А. Журавель та ін.; за ред. В. Ю. Шепітька. Київ: Видавничій Дім «Ін Юре», 2001. 684 с.

79. Кримінальне право України: Особлива частина: підручник / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін.; за ред. В. В. Сташиса, В. Я. Тація; 4 вид, переробл. і допов. Харків: Право, 2010. 608 с.

80. Кримінальний кодекс України: Закон від 05.04.2001 р. № 2341-III. Дата оновлення: 25.11.2021. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 01.12.2021).

81. Кримінальний процесуальний кодекс України: Закон від 13.04.2012 № 4651-VI. Дата оновлення: 25.11.2021. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 01.12.2021).

82. Крылов В. В. Расследование преступлений в сфере информации: учеб. пособие. М.: Городец, 1998. 287 с.

83. Кузнецов В. Комп'ютерна крадіжка: що розуміти під предметом злочину. *Право України*. 1999. № 10. С. 74–76.

84. Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. № 4. 2017. С 245–249. URL: http://pravoisuspilstvo.org.ua/archive/2017/4_2017/part_1/44.pdf.

85. Курман О. В. Тактичні та організаційні особливості початку досудового розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. URL: http://pravoisuspilstvo.org.ua/archive/2019/4_2019/47.pdf.

86. Лапта С. П. Взаємодія слідчого з експертом при проведенні судових експертиз. *Вісн. Нац. ун-ту внутр. справ*. 2003. Вип. 22. С. 39–44.

87. Лисенко В. В., Задорожний О. С. Проблеми виявлення злочинів, пов'язаних з несплатою податків. *Наук. вісн. Нац. акад. Державної податкової служби України*. 2007. № 2 (37). С. 212–219.

88. Лисиченко В. К. Следственный осмотр как специальный метод исследования объектов в процессе доказывания по уголовным делам. *Криминалистика и судебная экспертиза*. 1973. №10. С. 176–182.

89. Лисиченко В. К., Циркаль В. В. Использование специальных знаний в следственной и судебной практике: учеб. пособие. Київ: КГУ, 1987. 100 с.

90. Лукьяненко В. В. Методы государственного управления судебно-экспертной деятельностью. *Теорія та практика судової експертизи і*

криміналістики: зб. матеріалів міжнар. наук.-прак. конф. / Міністерство юстиції України, ХНДІСЕ, АПНУ, НЮАУ ім. Я. Мудрого; редколегія: М. Л. Цимбал, М. І. Панов та ін. Вип. 2. Харків: Право, 2002. С. 92–97.

91. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал*. 2014. № 4. С. 202–205.

92. Маланчук П. М. Порівняння боротьби з кіберзлочинністю в Україні та зарубіжних країнах. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 101–104.

93. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського нац. ун-ту внутр. справ*. 2016. № 3 (74). С. 111–120.

94. Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації. *Інформатизація вищих навчальних закладів МВС України*: матеріали наук.-практ. конф. (м. Харків, 15–16 трав. 2008 р.) / МВС України, Харк. нац. ун-т внутр. справ. Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2008. 160 с. С. 151–153.

95. Манжай О. В., Осятинська І. А. Використання спеціалізованого програмного забезпечення для роботи з мобільними телефонними пристроями. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*: матеріали міжнарод. наук.-практ. конф. (Харків, 12 листоп. 2014 р.) / МВС України, Харк. нац. ун-т внутр. справ. Харків: Права людини, 2014. С.143–145.

96. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: изд-во Воронежского гос. ун-та, 2002. 408 с.

97. Миськів Л. І. Адміністративно-правові засади діяльності вищих навчальних закладів МВС України з питань морально-правового виховання курсантів: дис. … канд. юрид. наук. Харків, 2008. 203 с.

98. Міжнародна політика кіберпростору. EU International Cyberspace Policy. URL: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm

99. Москаленко А. Н. Технико-криминалистическое обеспечение раскрытия преступлений по горячим следам: дис. … канд. юрид. наук. Волгоград, 2002. 211 с.

100. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: автореф. дис. ... канд. юрид. наук. Київ, 2005. 20 с.

101. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних технологій: дис. … канд. юрид. наук. Київ: Академія праці і соціальних відносин Федерації профспілок України, 2005. 221 с.

102. Незалежний інститут судових експертиз. Офіційний Інтернет ресурс. URL: https://nise.com.ua/it-ekspertyza.

103. Нестеров Д. І. Криміналістична характеристика та особливості розслідування за фактами обстрілів (вибухів) у зоні проведення операції об'єднаних сил. дис. … канд. юрид. наук. Маріуполь, 2020. 231 с.

104. Николаев А. Сетевая безопасность: рефлексивные списки доступа Reflexive ACL. 2018. URL: https://blog.learncisco.ru/setevayabezopasnost-refleksivnyie-spiski-dostupa-reflexive-acl/.

105. Нішніанідзе Т. Поняття і сутність техніко-криміналістичного забезпечення розкриття й розслідування сексуальних вбивств. *Право і суспільство*. 2006. Вип. 2. С. 28–31.

106. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту: метод. рек. / О. М. Стрільців, В. В. Крижна, О. В. Максименко та ін.; за заг. ред. Ю. Ю. Орлова. Київ: Нац. акад. внутр. справ, 2014. 80 с.

107. Павлишин Б. О. Поняття «техніко-криміналістичного забезпечення» розслідування злочинів проти життя і здоров'я особи. *Вісник Академії адвокатури України*. 2014. Т. 11. № 3. С. 116–123.

108. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: дис. … канд. юрид. наук. Харків, 2006. 215 с.

109. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: автореф. дис. … канд. юрид. наук. Київ, 2005. 18 с.

110. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дис. … канд. юрид. наук. Київ, 2004. 214 с.

111. Пам'ятка щодо огляду комп'ютерних засобів на місці події, експертиза комп'ютерної техніки і програмних продуктів. URL: http://uasol.com/index.php?aid=2835.

112. Панов А. М. Запобігання кіберзлочинності в Україні: монографія / М. О. Кравцова, О. М. Литвинов; Кримінол. асоц. України. Харків, 2016. 210 с.

113. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій»: автореф. дис. ... канд. юрид. наук. Харків, 2007. 19 с.

114. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій: дис. … канд. юрид. наук. Харків, 2007 228 с.

115. Перелік криміналістичного програмного забезпечення, протестованого Американським інститутом стандартизації (NIST). Інтернет ресурс. URL: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

116. Перлін С. Поняття і види техніко-криміналістичного забезпечення правозастосовної діяльності. *Підприємництво, господарство і право*. № 1. 2020. С. 221–226. URL: http://pgp-journal.kiev.ua/archive/2020/1/41.pdf.

117. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений*. 2019. № 12.1 (76.1). С. 55–59.

118. Пиріг І. В. Теоретичні основи експертної діяльності органів внутрішніх торгівля: монографія. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2011. 312 с.

119. Пілюков Ю. О. Використання інформаційних систем в експертних підрозділах МВС України: дис. … канд. юрид. наук. Київ, 2003. 257 с.

120. Пінчук Н. І. Теоретичні та правові питання і практика криміналістичного забезпечення діяльності нотаріату: дис. … канд. юрид. наук. Київ, 2008. 240 с.

121. Поджаренко К. Є. Криміналістичне забезпечення розкриття і розслідування злочинних порушень прав інтелектуальної власності: дис. … канд. юрид. наук. Київ, 2009. 255 с.

122. Політика інформаційної безпеки як основа управління інформаційною безпекою. URL: http://referatss.com.ua/work/politika-informacijnoi-bezpeki-jak-osnova-upravlinnja-informacijnoju-bezpekoju.

123. Поліція та підрозділи ДСНС отримали нову техніку. Прес-центр МВС. URL: https://mvs.gov.ua/ua/news/12946_Policiya_ta_pidrozdili_DSNS_otrimali_novu_tehniku_FOTO_.htm (дата звернення 21.09.2019).

124. Попов В. И. Осмотр места происшествия: учеб. пособие / В. И. Попов; под ред. В. А. Хвана. М., 1959. 245 с.

125. Практикум з негласних слідчих (розшукових) дій у кримінальному провадженні: навч.-метод. посіб. Харків: Нац. юрид. ун-т ім. Ярослава Мудрого, 2016. 200 с. URL: http://library.nlu.edu.ua/poln_text/posibniki_2016/nmp_164.pdf.

126. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: наказ МВС України від 07.07.2017 р. № 575. Дата оновлення: 03.07.2020. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text (дата звернення: 01.12.2021).

127. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному

провадженні: наказ Генеральної прокуратури України, МВС України, СБ України, Міністерством фінансів України, Адміністрацією ДПС України та Міністерством юстиції України від 16.11.2012 р. № 114/1042/516/1199/936/1681/51. URL: http://zakon4.rada.gov.ua/laws/show/v0114900-12 (дата звернення: 01.12.2021).

128. Про затвердження Інструкції про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах: Наказ Міністерства юстиції України від 12.12.2011 № 3505/5. Дата оновлення: 18.06.2021. URL: https://zakon.rada.gov.ua/laws/show/z1431-11#Text (дата звернення: 01.12.2021).

129. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: Наказ Міністерства юстиції України від 08.10.1998 № 53/5. Дата оновлення: 20.08.2021. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 01.12.2021).

130. Про затвердження Положення про Департамент кіберполіції Національної поліції України: наказ МВС України 10.11.2015 № 85. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 01.12.2021).

131. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України: Наказ МВС України від 03.11.2015 № 1343. Дата оновлення: 29.01.2019. URL: https://zakon.rada.gov.ua/laws/show/z1390-15#Text (дата звернення: 01.12.2021).

132. Про затвердження Положення про організацію діяльності підрозділів дізнання органів Національної поліції України: наказ МВС України від 20.05.2020 р. № 405. URL: https://zakon.rada.gov.ua/laws/show/z0491-20#Text (дата звернення: 01.12.2021).

133. Про затвердження Положення про Центральну експертно-кваліфікаційну комісію при Міністерстві юстиції України та атестацію судових експертів: Наказ Міністерства Юстиції України від 03.03.2015 № 301/5. URL: https://zakon.rada.gov.ua/laws/show/z0249-15#Text (дата звернення: 01.12.2021).

134. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. Дата оновлення: 08.08.2021. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 01.12.2021).

135. Про організацію діяльності слідчих підрозділів Національної поліції України: наказ МВС України від 06.07.2017 р. № 570. Дата оновлення: 17.07.2020. URL: https://zakon.rada.gov.ua/laws/show/z0918-17#Text (дата звернення: 01.12.2021).

136. Про судову експертизу в кримінальних та цивільних справах: Постанова Пленуму Верховного Суду України № 8 від 30.05.1997 р. *Судові експертизи в Україні*: зб. нормат. актів. Київ: Юрінком Інтер, 2002. С. 23–29.

137. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. Дата оновлення: 01.01.2021. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 01.12.2021).

138. Проблеми розслідування комп'ютерних злочинів: звіт. URL: https://www.crime-research.org/library/Zvit_.htm (дата звернення: 01.12.2021).

139. Протокол доступу до електронної пошти Internet Message Access Protocol (IMAP) (дата звернення: 01.12.2021).

140. Пряхін Є. В. Криміналістика: підручник. 3 вид., переробл. та допов. Львів: Львівський держ. ун-т внутр. справ, 2016. 948 с.

141. Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: дис. … канд. юрид. наук. Ірпінь, 2019. 212 с.

142. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. дис. … канд. юрид. наук. Київ. 222 с.

143. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет медійного контенту провайдерами програмних послуг та Інтернетпровайдерами: метод. рек. / О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін. Київ: Нац. акад. внутр. справ, 2017. 44 с.

144. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рек. / О. В. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін. Київ: Нац. акад. внутр. справ, 2016. 56 с.

145. Розслідування кримінальних правопорушень, вчинених у сфері захисту інтелектуальної власності з використанням мережі Інтернет: метод. рек. / О. С. Тарасенко, М. В. Гуцалюк, В. Д. Гавловський та ін. 2 вид., доповн. Київ: Міжвід. наук.-дослід. центр з проблем б-би з орг. злоч. при РНБО України; Нац. акад. внутр. справ, 2021. 74 с.

146. Романенко-Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки. дис. … канд. юрид. наук. Київ, 2021. 255 с.

147. Романюк Б. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у судовому слідстві: монографія. Київ: Нац. акад. внутр. справ, 2002. 196 с.

148. Россинская Е. Р. Судебная экспертиза в уголовном, гражданском, арбитражном процессе: учебник. М.: Право и закон, 1996. 224 с.

149. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза: учебник. М.: Право и закон, 2001. 416 с.

150. Салтевський М. В. Криміналістика (у сучасному вигляді): підручник. Київ: Кондор, 2005. 588 с.

151. Салтевський М. В. Криміналістика: навч.-довід. посіб. Київ: Правник, 1996. 159 с.

152. Салтевский М. В., Щербаковский М. Г., Губанов В. А. Осмотр компьютерных средств на месте происшествия: метод. рек. Харків.: Нац. юрид. акад. України, 1999. 136 с.

153. Сас В. А. Організація і тактика слідчих дій при розслідуванні злочинів, вчинених засудженими до позбавлення волі: дис. … канд. юрид. наук. Київ, 2004. 219 с.

154. Сахнова Т. В. Судебная экспертиза: учеб. пособие. М.: Городец, 2000. 368 с.

155. Сергєєва Д. Б. Негласні слідчі (розшукові) дії: поняття й сутність. *Оперативно-розшукове запобігання корупційним та пов'язаним з корупцією правопорушенням*: матеріали круглого столу (Київ, 24 черв. 2015 р.) / ред. кол. С. С. Чернявський, М. М. Алексійчук, О. В. Хуторянський, І. М. Купранець, В. І. Василинчук. Київ: ФОП Кандиба Т. П., 2015. С. 208-211. С. 208.

156. Скорченко П. Т. Криминалистика. Технико-криминалистическое обеспечение расследования преступлений: учеб. пособие. М.: Былина, 1999. 272 с.

157. Словник української мови: в 10 т. Т. 9. С / редкол.: І. К. Білодід (голова) та ін.; уклад.: І. Р. Вихованець, В. П. Градова, Г. Н. Демчик та ін.; ред.: І. С. Назарова та ін.; АН УРСР, Ін-т мовознавства ім. О. О. Потебні. Київ: Наук. думка, 1978. 916 с

158. Старушкевич А. В. Організація огляду місця події. *Вісник прокуратури*. 2003. № 13. С. 79–85.

159. Стригун Д. Ю. Техніко-криміналістичне забезпечення розкриття та розслідування контрабанди наркотичних засобів: автореф. дис. … канд. юрид. наук. Київ: НАВС, 2011. 19 с

160. Строгович М. С. Материальная истина и судебные доказательства в советском уголовном процессе. М.: АН СССР, 1955. 384 с.

161. Судова експертиза в кримінальному процесі: наук.-практ. посіб. / О. О. Садченко, Н. Д. Кулініч та ін. Київ: Нац. акад. внутр. справ, 2013. 233 с.

162. Сучасна правова енциклопедія / О. В. Зайчук, О. Л. Копиленко, В. С. Ковальський та ін.; за заг. ред. О. В. Зайчука; Ін-т законодавства Верховної Ради України. 2 вид., перероб. і допов. Київ: Юрінком Інтер, 2013. 408

163. 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. *Наук. вісн. Нац. акад. внутр. справ*. 2021. № 3 (120). С. 28–34.

164. Теплицький Б. Б. Використання зарубіжного досвіду техніко-криміналістичного забезпечення розслідування злочинів у сфері використання

комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *KELM*. 2020. № 3-3. С. 112–116.

165. Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. *Наук. вісн. Нац. акад. внутр. справ*. 2018. № 3 (108). С. 303–315.

166. Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Нац. акад. внутр. справ. 2019*. Вип 2. Т. 18. С. 24–32. URL: https://lawjournal.naiau.kiev.ua/index.php/lawjournal/article/view/1069/1079.

167. Теплицький Б. Б. Застосування техніко-криміналістичних засобів при проведенні обшуку під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *Юридична наука*. 2020. № 5. С. 143–148.

168. 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*. 2020. № 6. С. 177–183.

169. Теплицький Б. Б. Практичні проблемні питання призначення комп'ютерно-технічної судової експертизи в кримінальних провадженнях. *Актуальні проблеми криміналістики та судової експертології*: матеріали міжвідом. наук.-практ. конф. (Київ, 22 листоп. 2018 р.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2018. С. 406–409.

170. Теплицький Б. Б. Щодо визначення терміну «техніко-криміналістичне забезпечення розслідування кримінальних правопорушень». *Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності*: збірник матеріалів засідання № 1 постійно діючої Міжнар. наук.-практ. конф. (м. Кропивницький, 24 вер. 2021 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2021.

171. Теплицький Б. Б. Щодо завдань комп'ютерно-технічних експертиз при розслідуванні незаконного зайняття гральним бізнесом в Україні. *Судова експертиза: сучасність та майбутнє*: матеріали круглого столу (м. Львів, 25 січня 2018 р.); за заг. ред. д. т. н. М. О. Кузіна / Львівський науково-дослідний інститут судових експертиз Міністерства юстиції України. Львів, 2019. С. 127–129.

172. Технология восстановления данных. URL: https://www.acelab.ru /dep.pc/SCSItesterHDD.php (дата звернення: 01.12.2021).

173. Тищенко Є. Ф. Розслідування комп'ютерних злочинів: наук.-метод. посіб. Київ: Вид-во НА СБУ, 2010. 124 с.

174. Торгівля людьми в Україні. Проблеми розслідування: навч. посіб. URL: http://megalib.com.ua/content/1178_1_Dopit_svidkiv_i_poterpilih.html.

175. Тютюнник Т. В. Теоретичні та організаційно-технічні основи інформаційного забезпечення судово-балістичної експертизи: дис. … канд. юрид. наук. Харків, 2008. 216 с.

176. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 р., ратифікована Верховною радою України 12.07.2017 р. *Офіційний вісник України*. 2017. № 62. С. 5. Ст. 1901.

177. Ударцов Ю. Протидія корупції та організованій злочинності в умовах дії нового Кримінального процесуального кодексу. *Вісник прокуратури*. 2012. № 12. С. 18–26. С. 18.

178. Участь спеціаліста-криміналіста під час проведення окремих слідчих (розшукових) дій: навч. посіб. / Є. Ю. Свобода, А. В. Кофанов, А. В. Самодін та ін. Вінниця: ТОВ «Нілан-ЛТД», 2018. 432 с.

179. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України. Київ: Істина, 2004. 504 с.

180. Хараберюш І. Ф. Використання науково-технічних засобів в правоохоронній діяльності. *Часопис Академії адвокатури України*. 2011. № 12 (3).

С. 1–7. URL: e-pub.aau.edu.ua/index.php/chasopys/article/view/449 (дата звернення: 01.11.2021).

181. Харитонова О. І. Адміністративно-правові відносини: концептуальні засади та правова природа: теоретичні проблеми: дис. … д-ра юрид. наук. Одеса, 2008. 435 с.

182. Цивільний процесуальний кодекс України: Закон від 18.03.2004 № 1618-IV. Дата оновлення: 05.08.2021. URL: https://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 01.12.2021).

183. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів: монографія. Вінниця: ТОВ «Нілан-ЛТД», 2017. 492 с.

184. Чумак В. В. Європейський досвід реформування правоохоронних органів (на прикладі Естонії). *Підготовка охоронців правопорядку в Харкові (1917–2017 рр.)*: зб. наук. статей та тез допов. на наук.-практ. конф. до 100- річчя підготовки охоронців правопорядку в Харкові (м. Харків, 25 листоп. 2017 р.). Харків: Харків. нац. ун-т внутр. справ, 2017. С. 310–312. URL: http://univd.edu.ua/general/publishing/konf/25_11_2017/pdf/171.pdf.

185. Чумак В. В. Організаційно-правові засади діяльності KNAB Латвії та ДБР України: порівняльний аналіз. *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матеріали XI міжнар. наук.-практ. Інтернет-конф., (м. Одеса, 25 берез. 2019 р.). Одеса, 2018. С. 60– 61.

186. Чумак В. В. Основні напрями та особливості організації діяльності поліції Латвії. *Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі*: матеріали наук.-практ. конф. (Львів, 17 груд. 2015 р.) / МВС України; Львів. держ. ун-т внутр. справ. Львів, 2015. С. 146–149

187. Шапиро Л. Г. Использование специальных познаний при расследовании преступных уклонений от уплаты налогов: автореф. дис. … канд. юрид. наук. Саратов, 1999. 26 с.

188. Шепітько В. Ю. Криміналістична тактика (системно-структурний аналіз): монографія. Харків: Харків юридичний, 2007. 432 с. С. 265.

189. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол.: В. І. Борисов та ін. Харків: Право, 2011. Вип. 21. С. 39–46.

190. Шурухнов Н. Г., Левченко И. П., Лучин И. Н. Специфика проведения обыска при изъятии компьютерной информации. *Актуальные проблемы совершенствования деятельности ОВД в новых экономических и социальных условиях*. М., 1997. С. 27–32.

191. Шурухнов Н. Г., Лучин И. Н. Методические рекомендации по изъятию компьютерной информации при проведении обыска. *Информационный бюллетень следственного комитета МВД РФ*. 1996. № 4 (89). С. 22–28.

192. Щербаковский М. Г. Судебные экспертизы: назначение, производство, использование: учеб.-практ. пособие. Харків: «Эспада», 2005. 544 с.

193. Щербаковський М. Г. Особливості призначення та проведення комп'ютерно-технічної експертизи. *Вісник Нац. ун-та внутр. справ*. 2002. Спецвип. до 10-річчя утворення НУВС. С. 179–183.

194. Щербаковський М. Г. Тактика проведення судових експертиз: лекція Харків: Нац. унів. внутр. справ, 2004. 35 с.

195. Эстония, Польша, Хорватия, Нидерланды, Румыния и Литва создали общие кибернетические войска. *Tadviser*. URL: https://www.tadviser.ru/index.php.

196. Estonia, 5 more EU member states set up Lithuanian-led EU cyber force. URL: https://www.baltictimes.com/estonia__5_more_eu_member_states_set_up_lithuanian-led_eu_cyber_force/.

197. MSAB XR/MSAB XRY Field. URL: https://www.msab.com/ prod-ucts/xry.

198. Susan H. Nycum. The Criminal Law Aspects of Computer Abuse: *Applicability ofthe State Penal Laws to Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1976). *Ulrich Sieber, Computerkriminalität und Strafrecht* (Cologne, Karl Heymanns Verlag, 1977). URL:http:// www.worldcat.org/title/criminal-law-aspects-of-computer-abuse-applicability-of-the-state-penal-laws-to-computerabuse/oclc/654145221/editions?referer=di&editionsView=true.

199. Tableau T35U. URL: https://siliconforensics.com/tableau-t35u-forensic-bridge.html.

200. UFED Touch 2. URL: http://aimtech.ru /catalog/155.

201. Wiebitech Forensic UltraDock v5. URL: https://www.cru-inc.com/products/wiebetech/forensic-ultradock-v5-5.

202. Youtsen M. Research on European Juvenile Delinquency. *HEUNI Publication Series*. 1987. № 7. С. 57−62.

ДОДАТКИ

Додаток А

РЕЗУЛЬТАТИ

узагальнення анкетування слідчих та судових експертів (530 респондентів – 180 слідчих Національної поліції та 350 експертів Експертної служби МВС України), у відсотках

№ з/п	Питання	Слідчі	Судові експерти	Середній
1	2	3	4	5
1	Чи відповідає існуюча методика розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку існуючому рівню злочинності в даній сфері?			
	а) Не відповідає			87
	б) Повністю відповідає			10
	в) Важко відповісти на дане питання			3
2	Які положення методики розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку потребують свого доповнення та доопрацювання?			
	а) Криміналістична характеристика			14
	б) Організація та планування розслідування			62
	в) Особливості проведення окремих слідчих дій			84
	г) Техніко-криміналістичне забезпечення розслідування			64
3	Чи достатнім є рівень оснащеності науково-технічними засобами та інноваційними продуктами вашого підрозділу?			
	а) Цілком достатній	16		
	б) Недостатній	83		
	в) Важко відповісти	1		
4	З якими проблемами ви стикались при проведенні допиту при розслідуванні злочинів			

	даної категорії?			
	а) Пов’язані з термінологією	87		
	б) Вибором тактичних прийомів	24		
	в) Встановленням психологічного контакту	17		
	г) Інші проблеми	4		
5	Які НСРД найчастіше проводяться у провадженнях по злочинах у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку?			
	а) зняття інформації з транспортних телекомунікаційних мереж	87		
	б) установлення місцезнаходження радіоелектронного засобу	62		
	в) аудіо-, відеоконтроль особи	39		
	г) зняття інформації з електронних інформаційних систем	31		
	д) контроль за вчиненням злочину	27		
	е) обстеження публічно недоступних місць, житла чи іншого володіння особи	19		
6	Які судові експертизи найчастіше проводяться у провадженнях по злочинах у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку?			
	а) комп’ютерної техніки і програмних продуктів			98
	б) традиційні криміналістичні (трасологічна, дактилоскопічна, технічна експертиза документів тощо)			18
	в) телекомунікаційних систем і засобів			5
	г) судово-економічні			4
	д) біологічні			2
	е) комплексні (комп’ютерно-технічна та судово-бухгалтерська експертиза, комп’ютерно-технічна та судово-товарознавча експертиза, комп’ютерно-технічна та експертиза об’єктів			1

	інтелектуальної власності тощо)			
	Є) комісійні			1
7	Які типові помилки допускають ініціатори проведення експертиз комп'ютерної техніки та програмних продуктів?			
	а) в ході слідчої дії оглядаються та вилучаються не всі об'єкти, які містять інформаційні сліди злочину		23	
	б) об'єкти вилучаються, зберігаються чи транспортуються без дотримання відповідних правил		10	
	в) на експертизу надаються об'єкти, які апріорі не можуть містити інформації, що має значення для розслідування, або які з об'єктивних причин неможливо належно дослідити		7	
	г) на вирішення експертизи ставляться питання, які не відносяться до обставин справи або ж є некоректними		35	
	д) однією постановою (ухвалою) призначають експертизи за різними видами об'єктів або ж за їх надмірною кількістю		17	

Додаток Б

Рис. 1. *Загальний вигляд пристрою CellebriteUFEDTouch 2*

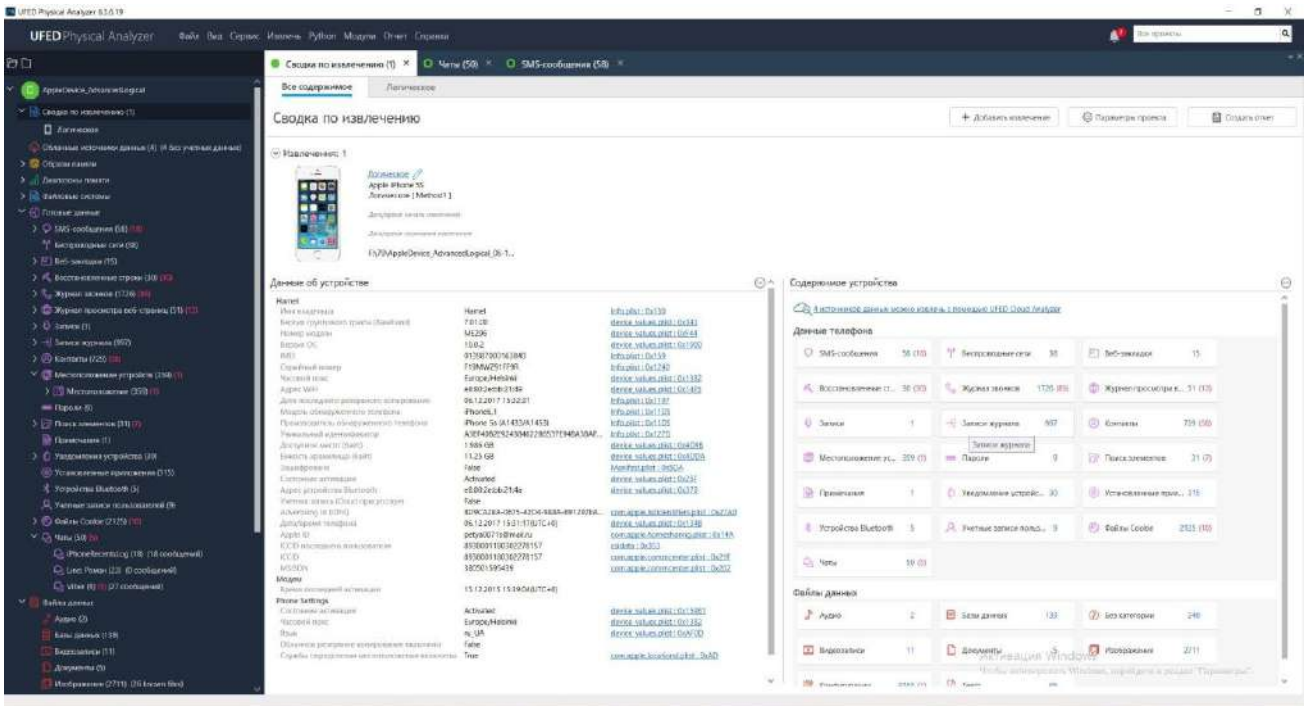

Рис. 2. *Загальний вигляд програмної частини пристрою CellebriteUFEDTouch 2*

Рис. 3. *Загальний вигляд пристрою MSABXRY / MSABXRYField*

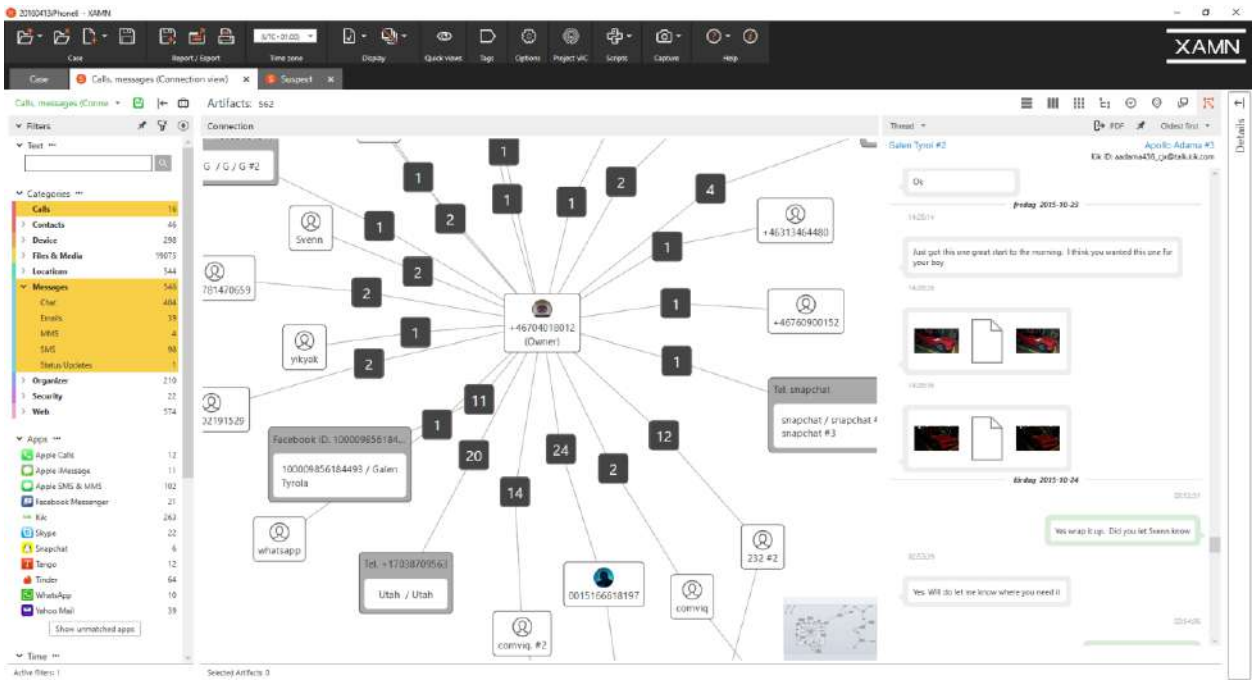

Рис. 4. *Загальний вигляд програмної частини пристрою MSABXRY / MSABXRYField*

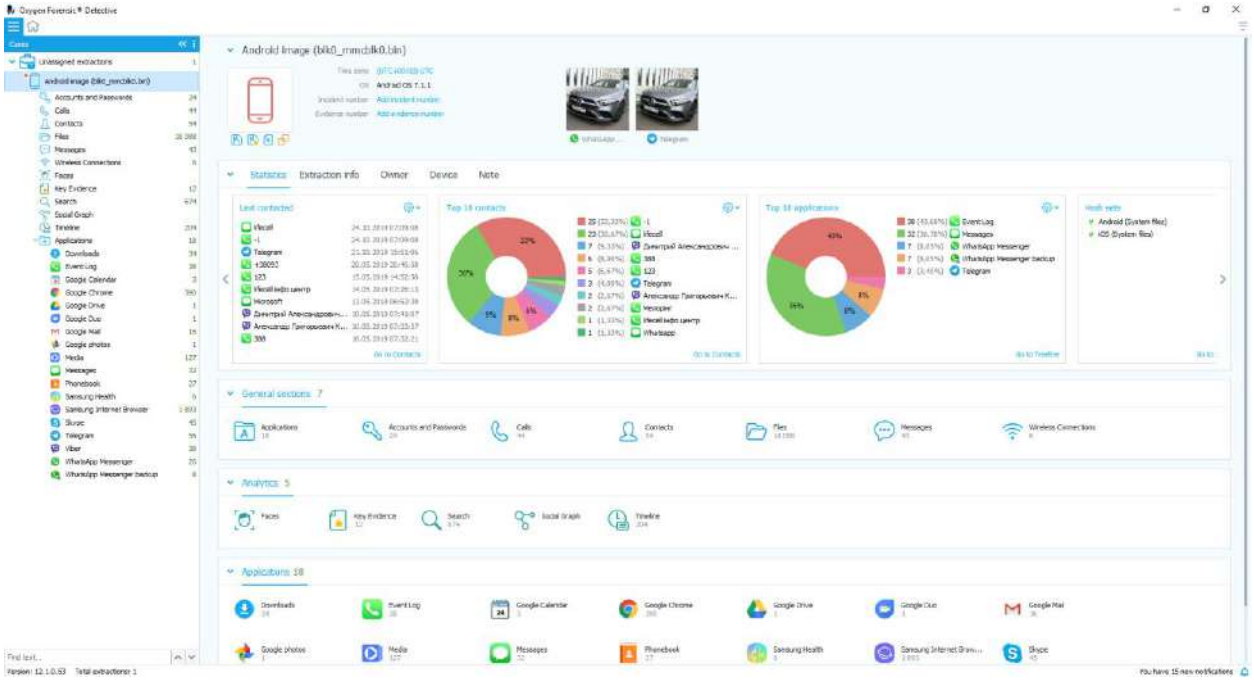

Рис. 5. *Загальний вигляд програмного засобу «Мобільний криміналіст»*

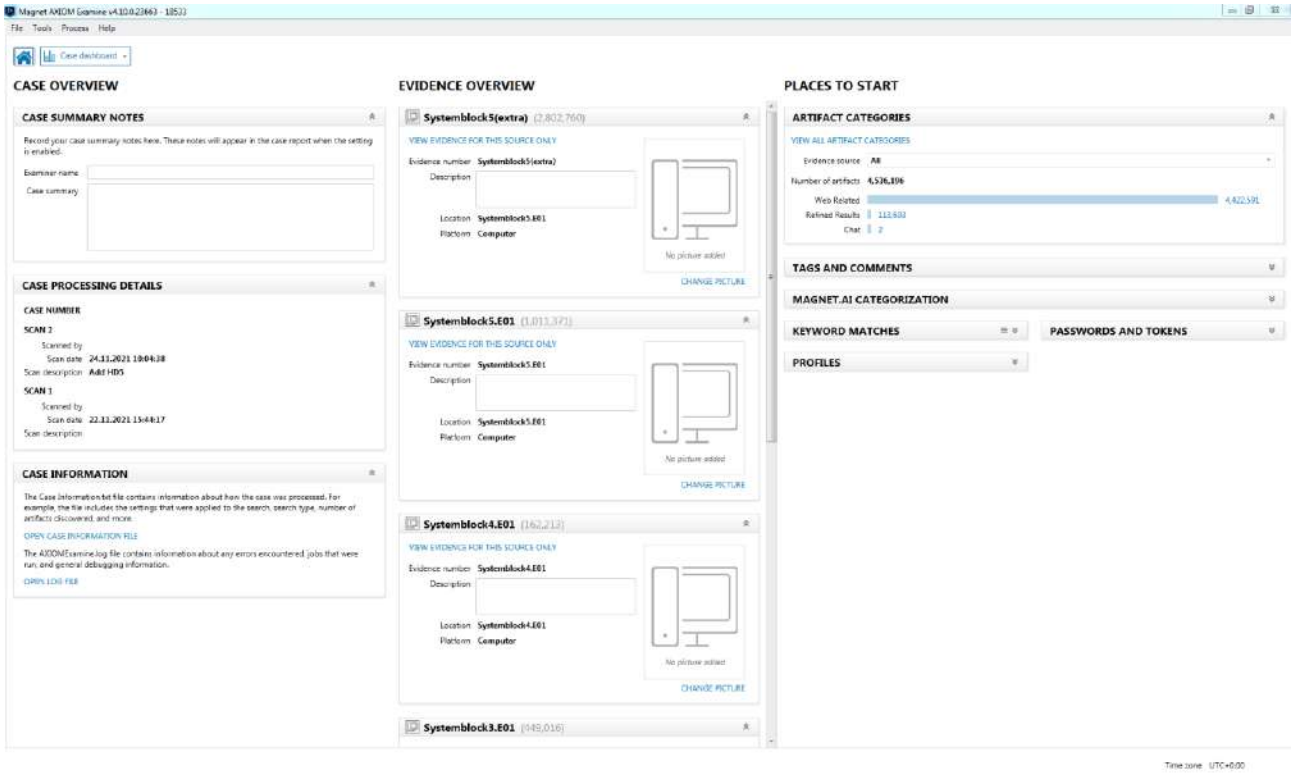

Рис. 6. *Загальний вигляд програмного засобу Magnet AXIOM*

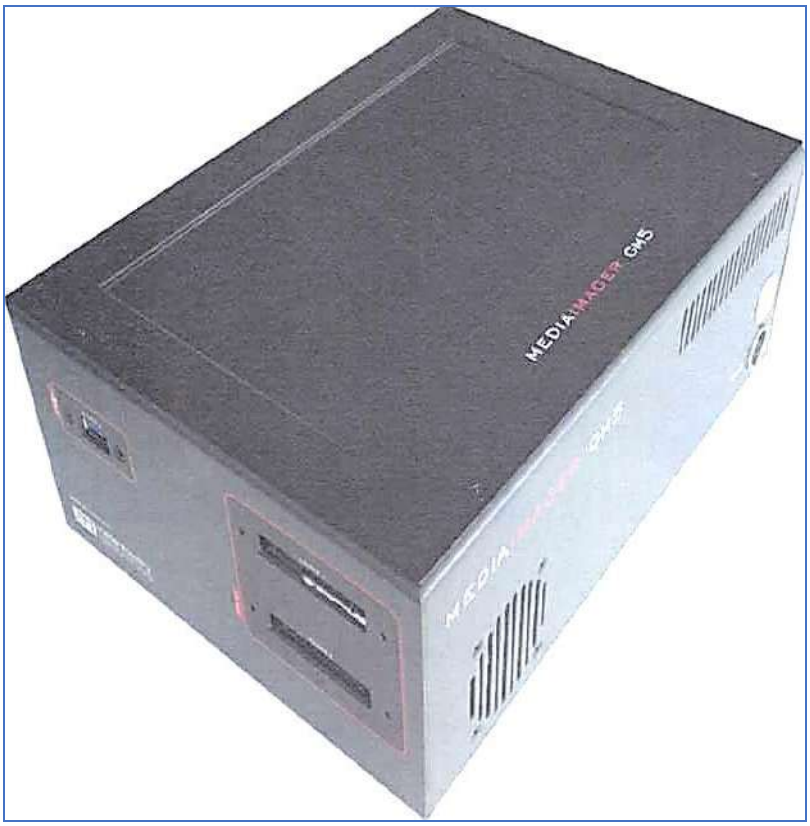

Рис. 7. *Загальний вигляд пристрою Mediaimager GM5*

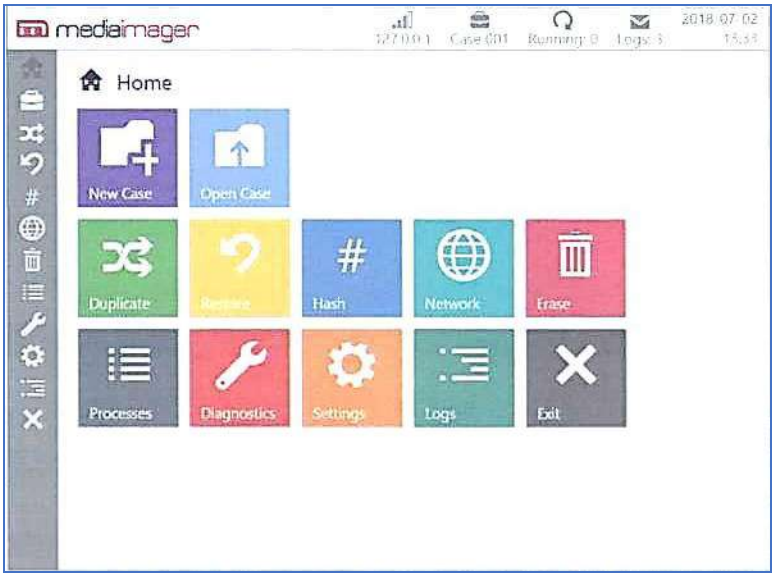

Рис. 8. *Загальний вигляд програмної частини пристрою Mediaimager GM5*

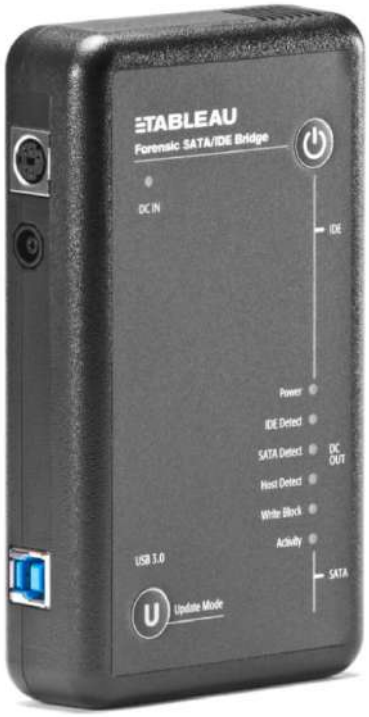

Рис. 9. *Загальний вигляд пристрою Tableau T35U*

Рис. 10. *Загальний вигляд пристрою Tableau Forensic Universal Bridge T356789iu*

Рис. 11. *Загальний вигляд пристрою Tableau Forensic Universal Bridge T356789iu та комплекту додаткових аксесуарів*

Рис. 12. *Загальний вигляд пристрою WiebitechForensicUltraDockv5*

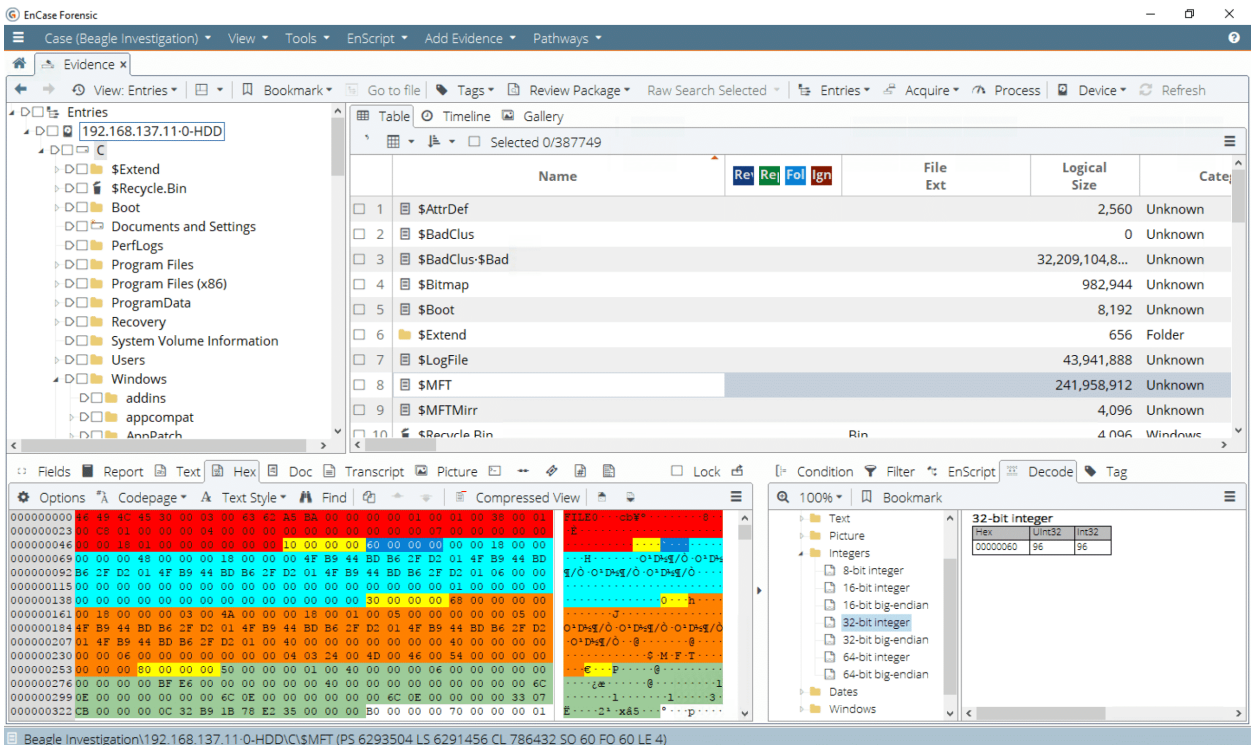

Рис. 13. *Загальний вигляд програмного засобу EncaseForensics*

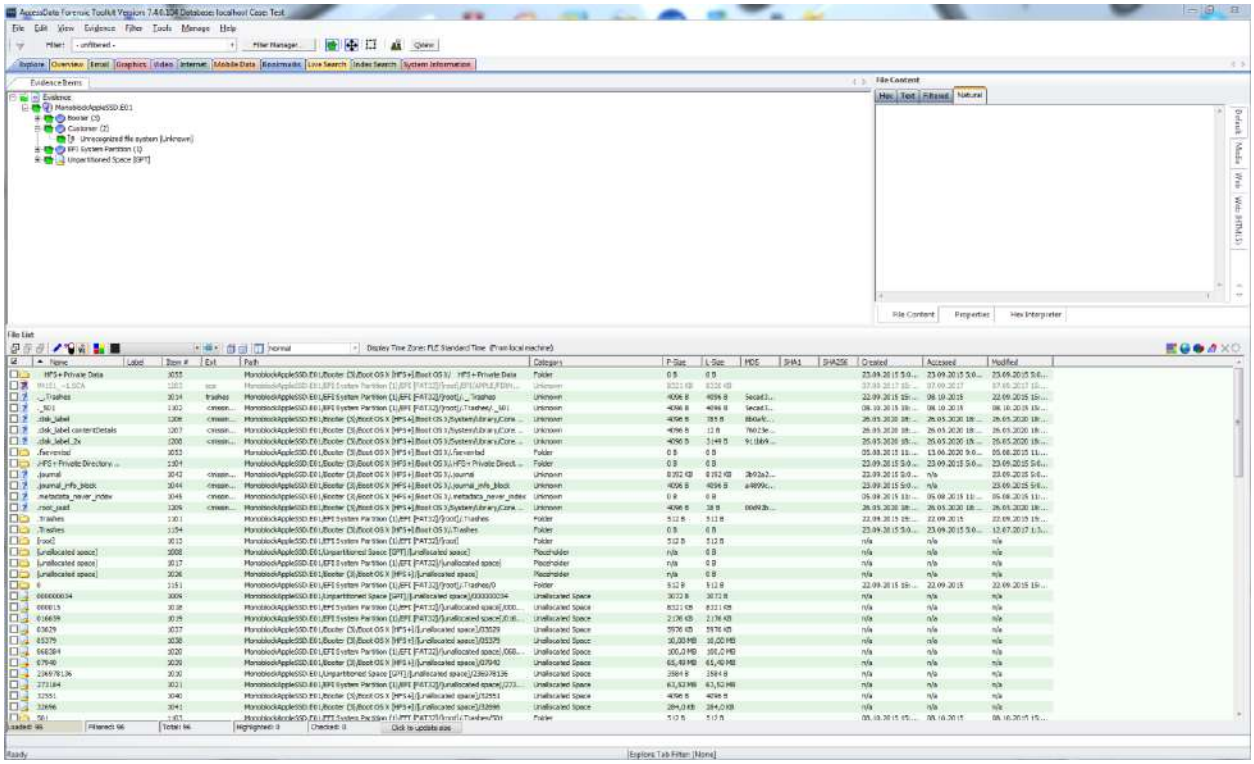

Рис. 14. *Загальний вигляд програмного засобу AccessDataFTK*

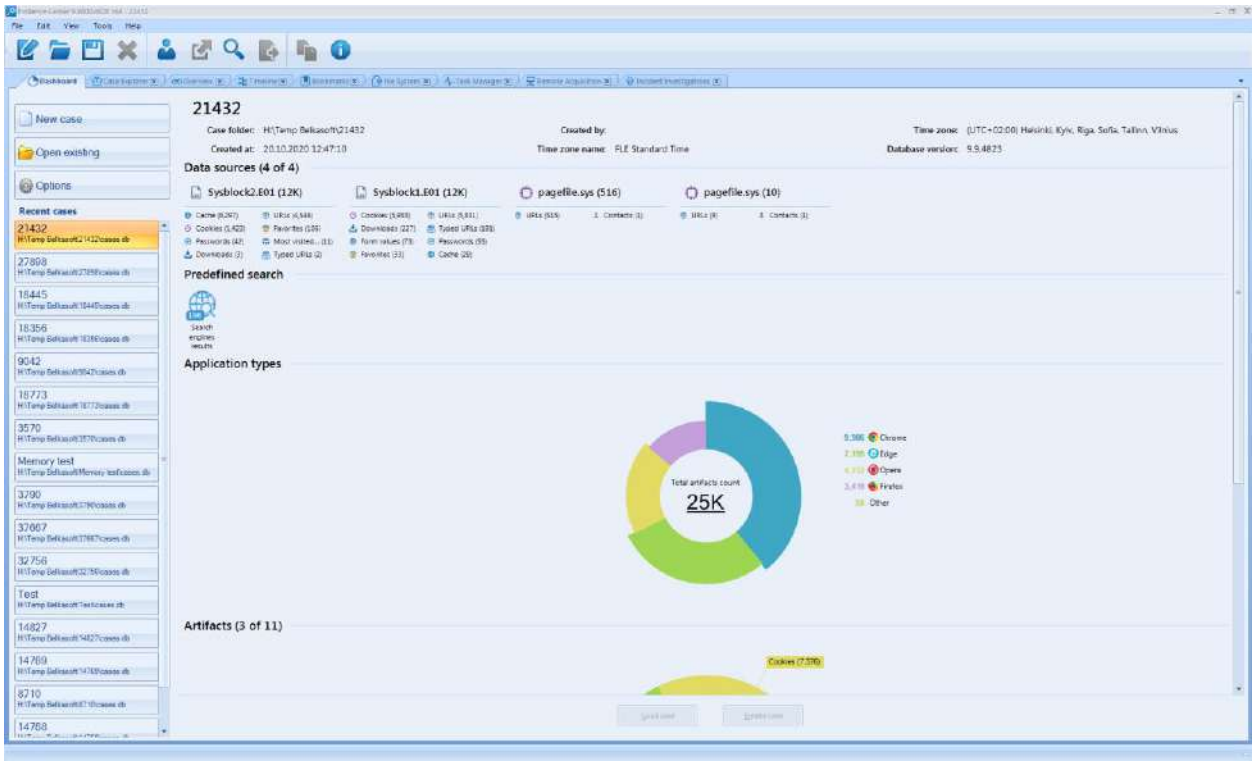

Рис. 15. *Загальний вигляд програмного засобу Belkasoft Evidence Center*

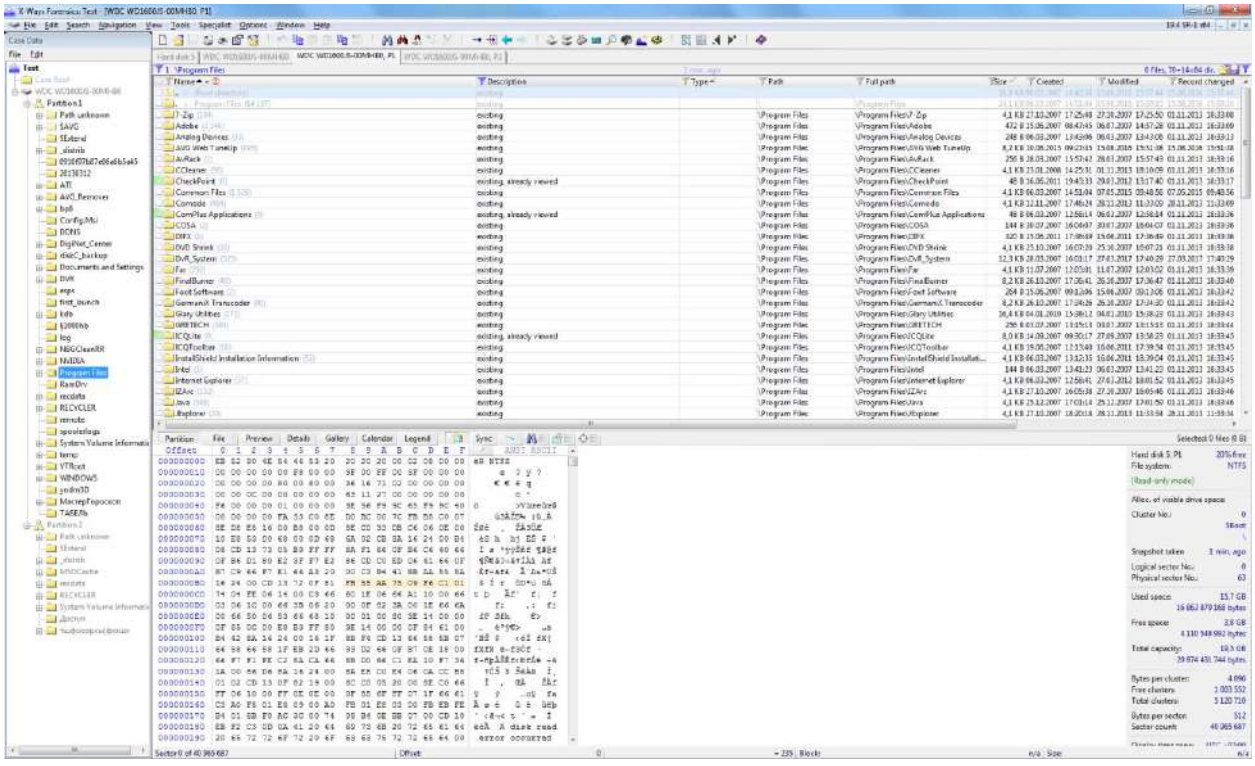

Рис. 16. *Загальний вигляд програмного засобу X-Ways Forensics*

Рис. 17. *Загальний вигляд пристрою PC-3000 Express*

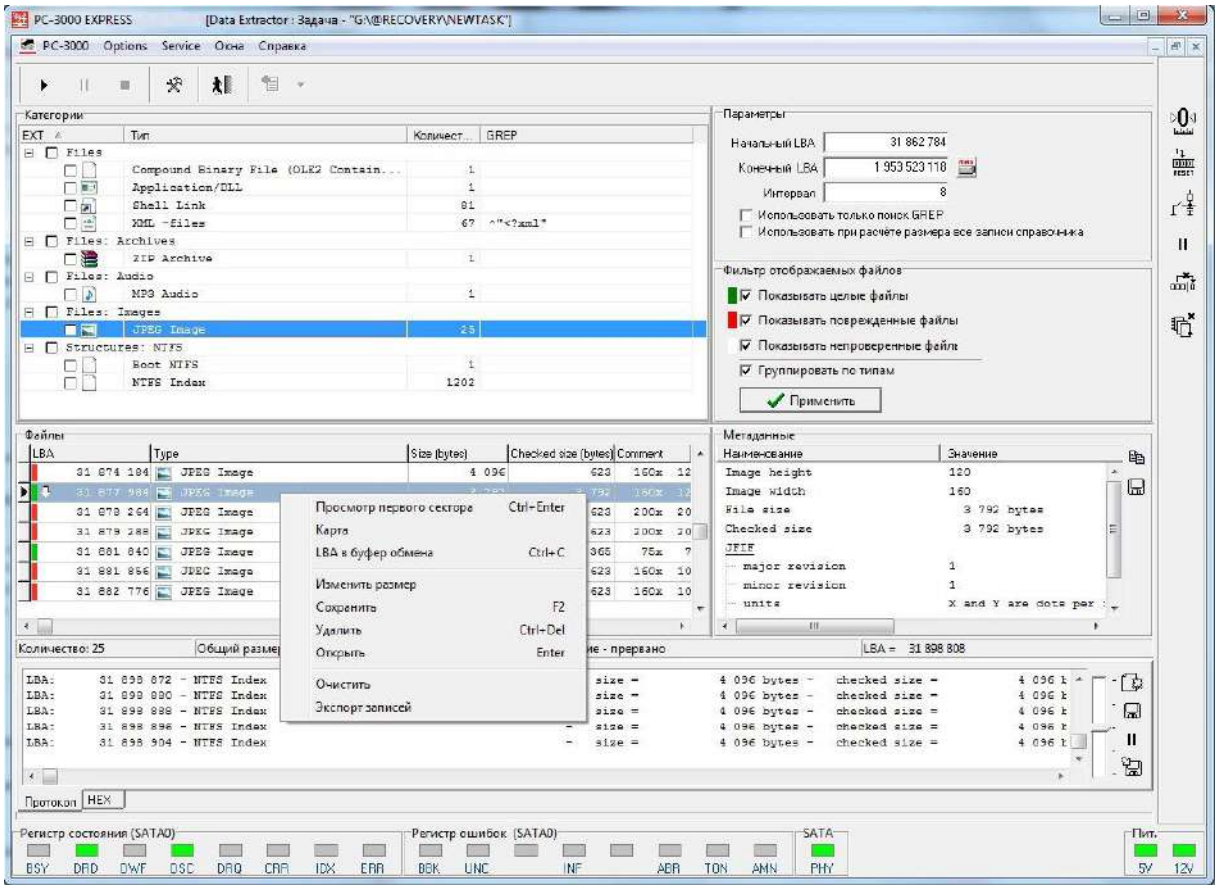

Рис. 18. *Загальний вигляд програмної частини пристрою PC-3000 Express*

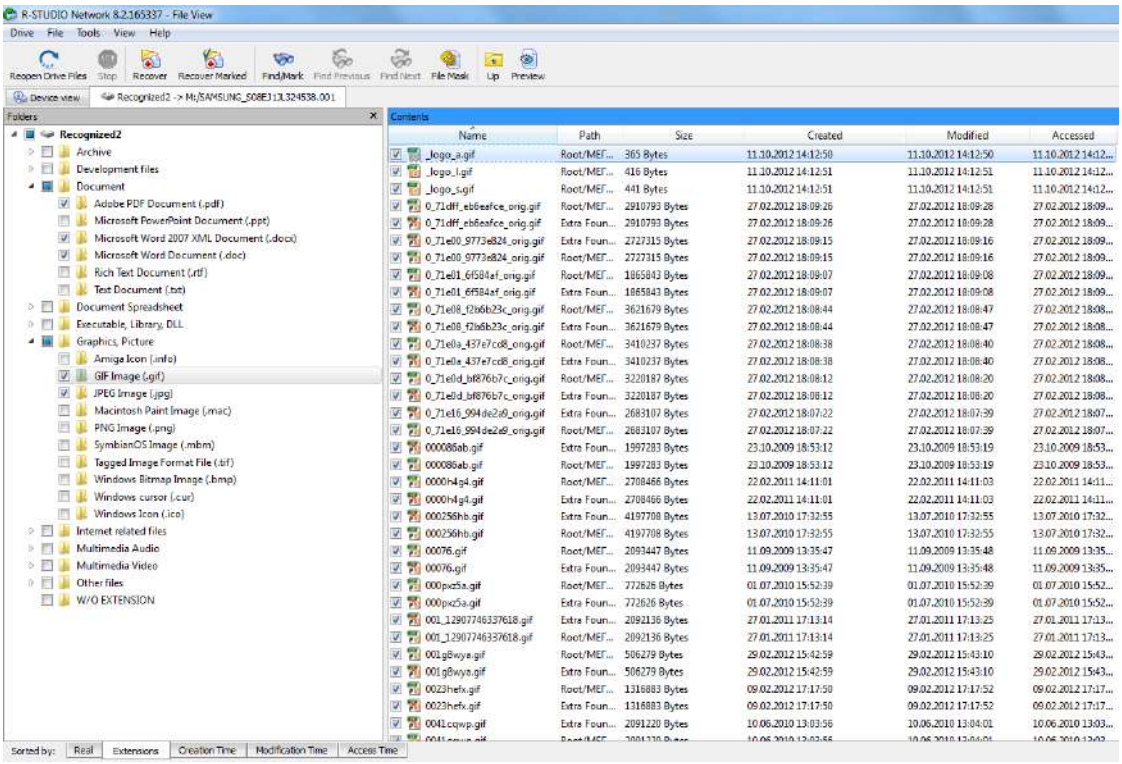

Рис. 19. *Загальний вигляд програмного засобу R-Studio*

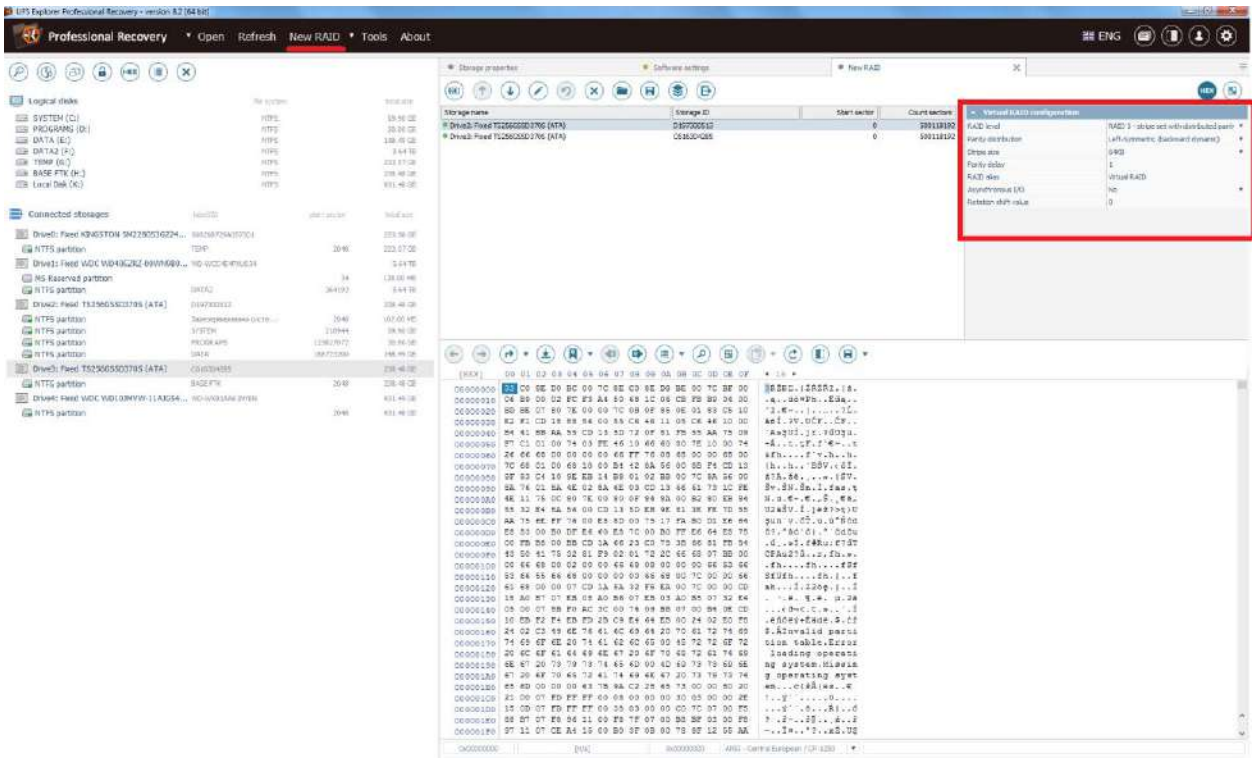

Рис. 20. *Загальний вигляд програмного засобу UFSExplorer*

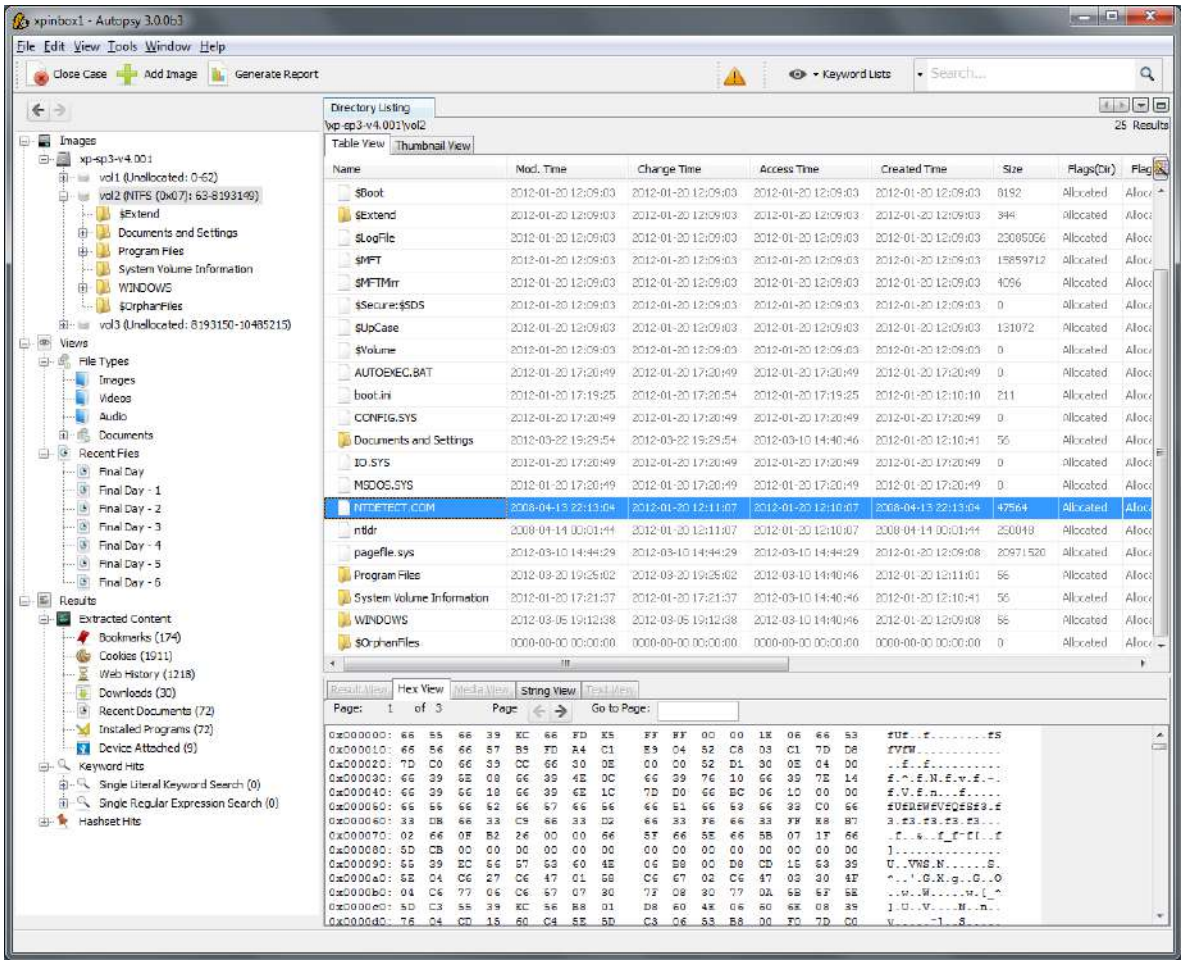

Рис. 21. *Загальний вигляд програмного засобу Autopsy*

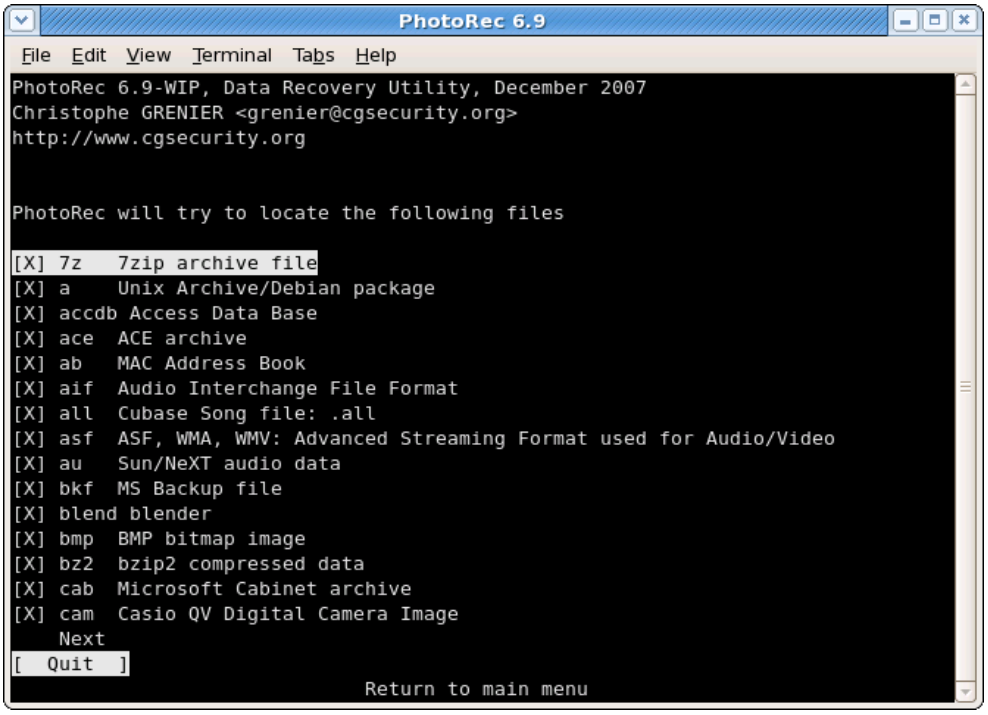

Рис. 22. *Загальний вигляд програмного засобу Photorec*

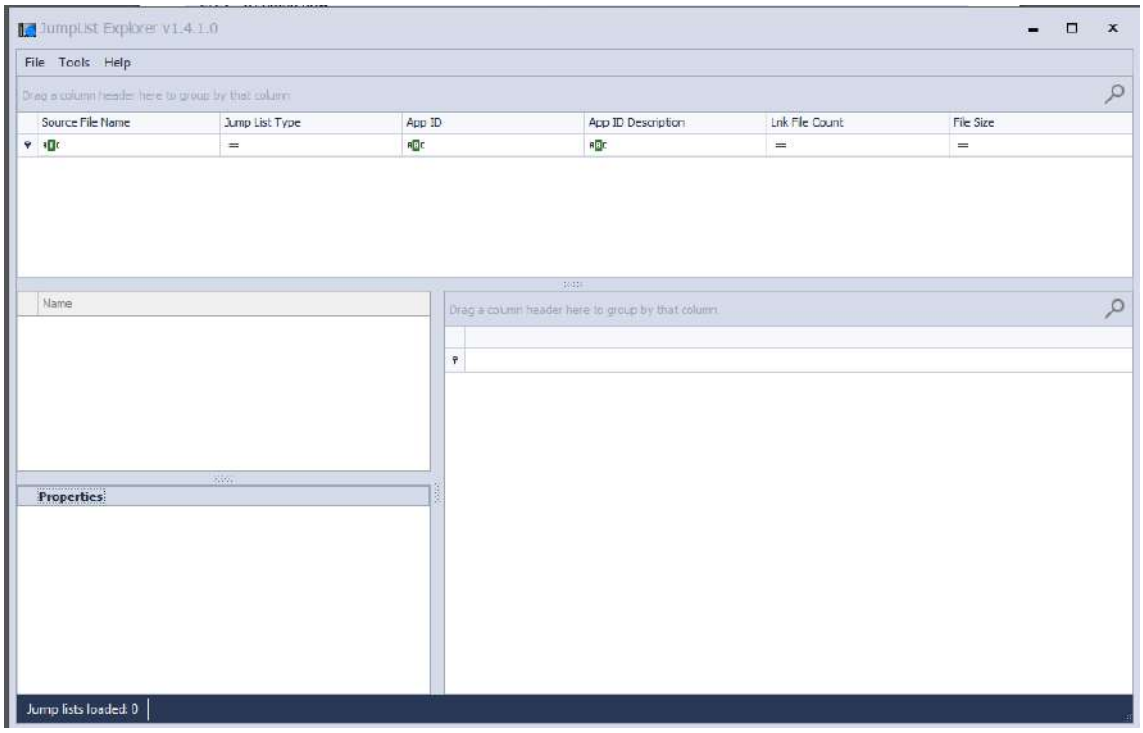

Рис. 23. *Загальний вигляд однієї з утиліт програмного засобу Eric Zimmerman Tools (Kroll Artifact Parser and Extractor (KAPE))*

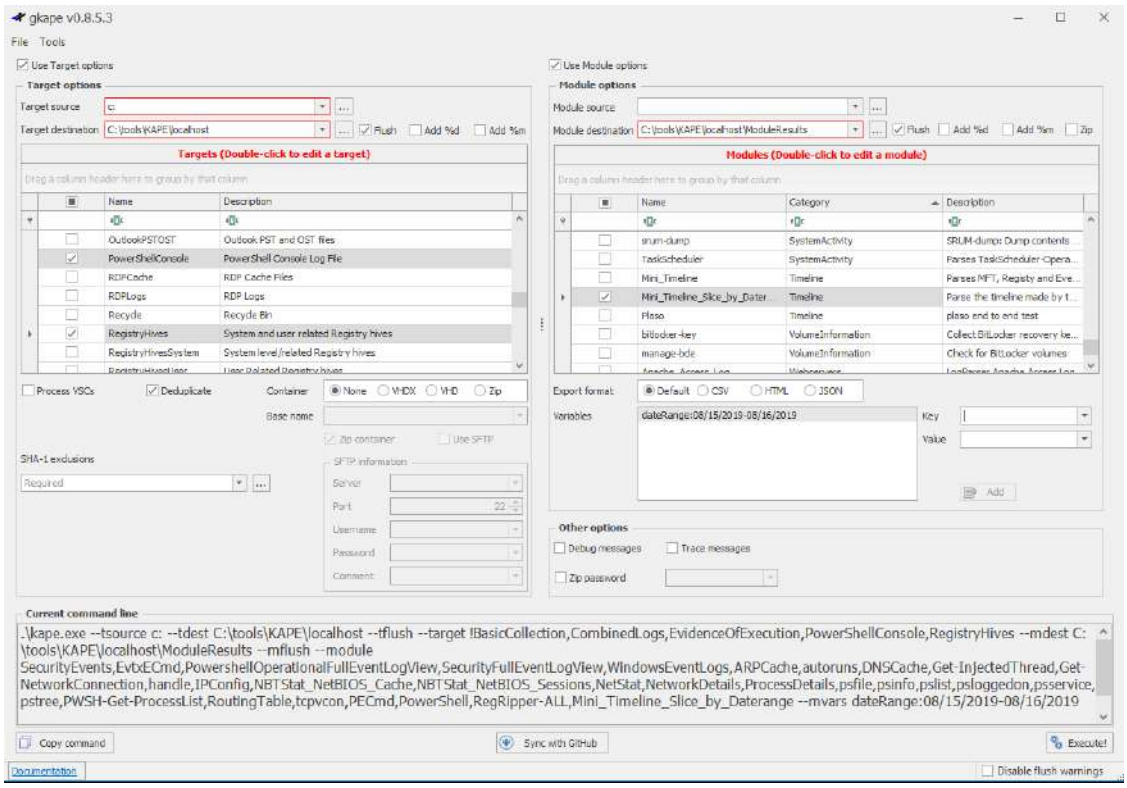

Рис. 24. *Загальний вигляд однієї з утиліт програмного засобу Eric Zimmerman Tools (Kroll Artifact Parser and Extractor (KAPE))*

Рис. 25. *Загальний вигляд Linux-дистрибутиву SIFT*

Рис. 26. *Загальний вигляд Linux-дистрибутиву KaliLinux*

Додаток В

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Богомольця, 10, м. Київ, 01601,
тел. 256-12-82, gsu@police.gov.ua
Ідентифікаційний код 40108578

Директору ДНДЕКЦ
МВС України
Сергію КРИМЧУКУ

03170, вул. Велика Кільцева, 4,
м. Київ

_____ № _____

На № _____ від _____

Про призначення експертизи

Направляю на Вашу адресу постанову про призначення комп'ютерно-технічної експертизи у кримінальному провадженні № _____ для організації проведення зазначеної експертизи.

Додатки: 1. постанова про призначення експертизи на 2 арк;
2. спеціальний пакет № _____

Заздалегідь вдячний за співпрацю, з повагою,
старший слідчий в ОВС
ГСУ Національної поліції України

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ
вул. Богомольця, 10, м. Київ, 01601 тел. (044) 254-93-33, факс (044) 253-6404, gsu@police.gov.ua
Ідентифікаційний код 40108578

П О С Т А Н О В А
про призначення комп'ютерно-технічної експертизи

Старший слідчий в ОВС ГСУ Національної поліції України підполковник поліції , розглянувши матеріали досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № від

В С Т А Н О В И В:

Головним слідчим управлінням Національної поліції України здійснюється досудове розслідування у кримінальному провадженні № від за ознаками кримінальних правопорушень, передбачених ч. 2 ст. 182 та ч. 4 ст. 189 КК України

Досудовим розслідуванням встановлено, упродовж 2017 – 2021 невстановлені особи з використанням веб-ресурсів :

розповсюдження конфіденційної інформації про осіб, які потерпілий чи його близькі родичі бажають зберегти в таємниці.

Крім того, невстановлена група осіб з метою вимагання грошових коштів та майна здійснюють незаконне збирання, зберігання, використання, зміну інформації, створення інформації, яка не відповідає дійсності, зокрема що стосується і приватного життя, про посадових осіб органів державної влади, бізнесменів, політиків, осіб які займають впливове положення у суспільстві, ведуть публічний спосіб життя, та для яких, розповсюдження інформації, що компрометує їх, є небажаною та такою, що завдає збитків, яку в подальшому розповсюджують через мережу підконтрольних веб-ресурсів.

У подальшому, після опублікування такої інформації, невстановлені особи зв'язуються із особами про яких опублікована інформація та вимагають сплату грошових коштів за знищення та припинення публікування такої інформації з використанням веб-ресурсів :

Зокрема, після отримання грошових коштів учасниками злочинної групи, статті та інформація видаляється із веб-ресурсу, однак через деякий час на сайті знову починає з'являтися провокаційна та недостовірна інформація відносно тієї ж особи, тим самим змушуючи її знову звертатись до вказаних осіб для її видалення.

Так, під час досудового розслідування проведено обшуки у осіб причетних до вчинення кримінального правопорушення, за адресою: місто виявлено та вилучено мобільний

Приймаючи до уваги викладене, для з'ясування обставин, що мають значення для кримінального провадження необхідні спеціальні знання, керуючись ст.ст. 110, 242, 243 КПК України,-

П О С Т А Н О В И В:

1.Призначити у даному кримінальному провадженні комп'ютерно-технічну експертизу, проведення якої доручити експертам ДНДЕКЦ МВС України

2. На вирішення експертів поставити наступні питання:

2.1. Чи містяться на мобільному телефоні наданого на експертизу облікові дані (логіни та паролі) користувача для доступу до Інтернет ресурсів?»

2.2. Чи міститься на накопичувачі наданого на експертизу мобільного телефону листи електронної пошти? Якщо так то прошу скопіювати зазначену інформацію на окремий носій.

2.3. «Чи містяться програми обміну повідомленнями в мережі Інтернет "Viber" «Telegram», «WhatsApp", Skype", "ICQ" та інші? Якщо так, то чи містять вони інформацію, щодо історії повідомлень, фото та дзвінків, прошу скопіювати дану інформацію на окремий носій.

2.4. Чи містяться на наданих на дослідження об'єктах серед наявних та видалених файлів інформація щодо ключових слів:

«*.gmail.com» «снять» якщо так які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять вказану вище інформацію? Які атрибути (час друку, редагування, створення, видалення тощо) файлів, фото, що містять вказану вище інформацію?

3. Для дослідження експертам надати мобільний телефон поміщений в спеціальний пакети:

4. На вимогу, надати експертам для ознайомлення матеріали кримінального провадження № .

5. Копію постанови направити експертам ДНДЕКЦ МВС України.

Старший в ОВС ГСУ
Національної поліції України
підполковник поліції

Додаток Г

ПОДІЛЬСЬКЕ УПРАВЛІННЯ ПОЛІЦІЇ ГОЛОВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У МІСТІ КИЄВІ
Вул.. Хорива, 20, м. Київ, 04071

Директору Державного науково-дослідного експертно-криміналістичного центру МВС
Кримчуку С.Г.
03170, м. Київ, вул. Велика Кільцева,4.

_____ № _____
_____ від _____

Направляю на виконання постанову про призначення експертизи по матеріалам досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № _____ від _____ ознаками кримінального проступку, передбаченого ч. 1 ст. 182 КК України, та об'єкт дослідження.

Додатки:

- Постанова про призначення експертизи від _____ на 2 арк.;
- Сейф пакет № _____ із надписами «чорна коробка з пластику «Kusler» (трекер и знак) та сім карта «Київстар»», всередині якого знаходиться об'єкт дослідження;
- Копія протоколу огляду місця події від _____ на 3 арк.

_____ **поліції**
Головного управління
Національної поліції у м. Києві
старший лейтенант поліції _____ _____

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ПОДІЛЬСЬКЕ УПРАВЛІННЯ ПОЛІЦІЇ ГОЛОВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У м. КИЄВІ
04071, м. Київ, вул. Хорива, 20

ПОСТАНОВА
про призначення експертизи телекомунікаційних систем (обладнання) та засобів.

м. Київ

управління поліції Головного управління Національної поліції у м. Києві старший лейтенант поліції , розглянувши матеріали досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № від року, за ознаками кримінального проступку, передбаченого ч.1 ст.182 КК України, -

ВСТАНОВИВ:

Під час досудового розслідування встановлено, що у період часу із р. по , невстановлена особа порушила недоторканість приватного життя О.М., р.н. шляхом прикріплення до автомобіля «Toyota Lantcruiser 100» сірого кольору, , предмета схожого на GPS-трекер із сім карткою мобільного оператора всередині, який було виявлено за адресою: м. Київ,). Предмет схожий на GPS-трекер був виявлений біля переднього правого колеса на днищі автомобіля.

З метою встановлення технічних параметрів та стану об'єкта, визначення функціонального призначення., виникла необхідність у призначенні судово-медичної експертизи, керуючись ст. ст. 110, 242, 243 КПК України, -

П О С Т А Н О В И В:

1.Призначити у кримінальному провадженні № від , експертизу телекомунікаційних систем (обладнання) та засобів, проведення якої доручити експертам Державного науково-дослідного експертно-криміналістичного центру.

2. для вирішення експерту поставити наступні запитання:

1) Чим являється пристрій, наданий на дослідження?

2) Які тип, марка, модель наданого на дослідження пристрою?

3) Яким способом, заводським чи кустарним, виготовлений пристрій?

4) Яке функціональне призначення наданого на дослідження пристрою?

5) Чи в робочому стані знаходиться наданий на дослідження пристрій?

6) Які характеристики підключень до мережі наданим на дослідження пристроєм?

7) Яким чином здійснюється живлення пристрою, наданого на дослідження?

2. Для дослідження експерту направити:

- Сейф пакет № , із надписами «чорна коробка з пластику «Kusler» (трекер и знак) та сім карта «Київстар»», всередині якої знаходиться предмет, схожий на GPS-трекер;
- Копію протоколу огляду місця події від на 3 арк.

Матеріали кримінального провадження № від та додаткові матеріали будуть надані на запит експерта.

3. Також ставлю Вас до відома, що для вирішення питання призначеної постанови не заперечую отримати всі необхідні дані від штатних або позаштатних спеціалістів, відповідно до ст. 69 КПК України.

4. Копію даної постанови направити експертам Державного науково-дослідного експертно-криміналістичного центру.

5. Висновок за результатами проведення експертизи направити до управління поліції Головного управління Національної поліції у м. Києві за адресою: м. Київ, .

Головного управління
Національної поліції у м. Києві
старший лейтенант поліції

Додаток Д

ВЕРХОВНА РАДА УКРАЇНИ
ІНСТИТУТ ЗАКОНОДАВСТВА
04053, Київ, пров. Несторівський, 4, тел. 235 96 01, факс. 235 96 05, e-mail:zak_norm@rada.gov.ua

№22/696-1-15 „16" 05 2019 р.

АКТ

впровадження у практичну діяльність Інституту законодавства Верховної Ради України результатів дисертаційного дослідження Теплицького Броніслава Броніславовича на тему «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»

Повідомляємо спеціалізованій вченій раді, що наукові положення, розроблені здобувачем Національної академії внутрішніх справ Теплицьким Броніславом Броніславовичем під час підготовки дисертаційного дослідження за спеціальністю 12.00.09 «кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» на тему: «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», які стосуються удосконалення вітчизняного законодавства у сфері судово-експертної діяльності, мають необхідний теоретичний та методологічний рівень, наукову та практичну значимість та можуть бути використані Інститутом законодавства Верховної Ради України при підготовці відповідних проектів нормативно-правових актів.

Зокрема, заслуговують на увагу розроблені Теплицьким Б. Б. зміни та доповнення до чинного законодавства України, а саме до Інструкції про призначення та проведення судових експертиз та експертних досліджень і Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, які спрямовані на удосконалення порядку призначення експертизи комп'ютерної техніки і програмних продуктів. Зокрема, запропоновано оновлений перелік типових запитань, що можуть бути поставлені на вирішення експертизи комп'ютерної техніки і програмних продуктів; доповнено положенням про неможливість експертизи вирішувати питання про правомірність дій користувачів електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, ліцензійність програмних продуктів, вартість комп'ютерної техніки та програмних продуктів.

Висновки та рекомендації Теплицького Броніслава Броніславовича прийняті до уваги Інститутом законодавства Верховної Ради України і будуть враховуватись при підготовці експертно-аналітичних матеріалів для відповідних Комітетів Верховної Ради України, з метою удосконалення чинного законодавства України у сфері судово-експертної діяльності.

Директор,
академік НАН України **О. Л. Копиленко**

ЗАТВЕРДЖУЮ
Заступник Голови Національної поліції – начальник Головного слідчого управління, доктор юридичних наук, доцент, заслужений юрист України, полковник поліції

Максим ЦУЦКІРІДЗЕ

16.08 2021 року

АКТ

Про впровадження у практичну діяльність Головного слідчого управління Національної поліції України результатів дисертаційного дослідження здобувача Національної академії внутрішніх справ Теплицького Броніслава Броніславовича на тему: «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»

Уклала комісія у складі:

Голови: начальника відділу методичної роботи та правового забезпечення Головного слідчого управління, кандидата юридичних наук, підполковника поліції Владислава Бурлаки

членів комісії: заступника начальника відділу організаційно-аналітичної роботи Головного слідчого управління, кандидата юридичних наук, майора поліції Наталії Карпенко

старшого слідчого в особливо важливих справах відділу методичної роботи та правового забезпечення Головного слідчого управління, старшого лейтенанта поліції Максима Романова

Комісія відповідно до Положення про організацію проведення НДР і ДКР у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15.05.2007 № 154 склала цей

акт, щодо розгляду матеріалів дисертаційного дослідження здобувача Національної академії внутрішніх справ Теплицького Броніслава Броніславовича на тему: «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність, поданої на здобуття наукового ступеня кандидата юридичних наук.

Вказані матеріали дисертаційного дослідження можуть застосовуватися у практичній діяльності слідчих підрозділів органів Національної поліції під час проведення занять в системі службової підготовки, а також при проведенні семінарів, нарад.

Отримані наукові результати мають як необхідний теоретичний та методологічний рівень, так і практичну цінність, сприятимуть удосконаленню процесуальної діяльності органів досудового розслідування Національної поліції України.

Голова комісії: **Владислав БУРЛАКА**

Члени комісії: **Наталія КАРПЕНКО**

Максим РОМАНОВ

ЗАТВЕРДЖУЮ
Директор Держаного науково-дослідного експертно-криміналістичного центру МВС України
Сергій КРИМЧУК
15 : 04 .2021 р.

АКТ
про впровадження в практичну діяльність Державного науково-дослідного експертно-криміналістичного центру МВС України матеріалів дисертаційного дослідження аспіранта Національної академії внутрішніх справ Теплицького Броніслава Броніславовича на тему «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність»

Комісія у складі: голови комісії – заступника директора ДНДЕКЦ МВС України кандидата юридичних наук Татарнікової Т. О., членів комісії – завідувача лабораторії навчальної та наукової роботи ДНДЕКЦ МВС України кандидата юридичних наук, доцента Косенко С. С., завідувача лабораторії комп'ютерно-технічних та телекомунікаційних досліджень ДНДЕКЦ МВС України Степанця Д.С., склала цей акт про те, що результати дисертаційного дослідження аспіранта Національної академії внутрішніх справ Теплицького Броніслава Броніславовича на тему: «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», мають належний науковий і практичний рівень розроблення проблематики, упроваджені у практичну діяльність Державного науково-дослідного експертно-криміналістичного центру МВС України під час проведення судових експертиз, експертних досліджень, участі як спеціаліста у слідчих (розшукових) діях і професійному навчанні працівників підрозділів Експертної служби МВС.

Голова комісії **Тетяна ТАТАРНІКОВА**

Члени комісії: **Світлана КОСЕНКО**

Дмитро СТЕПАНЕЦЬ

15 04 2021 р.

ЗАТВЕРДЖУЮ
Проректор
Національної академії внутрішніх справ,
доктор юридичних наук,
професор,
заслужений діяч науки і техніки України

Сергій ЧЕРНЯВСЬКИЙ

04. 10. 2021 р.

АКТ
про впровадження результатів дисертації
Теплицького Броніслава Броніславовича
«Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у освітній процес Національної академії внутрішніх справ

Комісія у складі: завідувача кафедри кримінального процесу, доктора юридичних наук, доцента Макарова М.А., завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента Самодіна А.В., старшого наукового співробітника відділу організації наукової діяльності та захисту прав інтелектуальної власності, кандидата юридичних наук Бондаря С.В. склала цей акт про те, що результати дисертації Теплицького Броніслава Броніславовича «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» впроваджені у освітній процес академії.

На основі проведеного аналізу комісія дійшла висновку, що подані наукові праці Теплицького Б.Б. містять науково обґрунтовані теоретичні положення і практичні рекомендації, запроваджені для використання в освітньому процесі Національної академії внутрішніх справ, зокрема у системі професійної освіти слідчих, при викладанні відповідних навчальних дисциплін та під час підготовки навчальних і методичних посібників, підручників, курсів лекцій.

Голова комісії:
доктор юридичних наук, доцент **Марк МАКАРОВ**

Члени комісії:
кандидат юридичних наук, доцент **Артем САМОДІН**

кандидат юридичних наук **Сергій БОНДАР**

Додаток Е

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковано основні наукові результати дисертації:

1. Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. *Науковий вісник Національної академії внутрішніх справ.* 2018. № 3 (108). С. 303–315.

2. Теплицкий Б. Використання зарубіжного досвіду техніко-криміналістичного забезпечення розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *KELM*. 2020. № 3-3. С. 112–116. (Республіка Польща).

3. Теплицький Б. Б. Застосування техніко-криміналістичних засобів при проведенні обшуку під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *Юридична наука*. 2020. № 5. С. 143–148.

4. 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*. 2020. № 6. С. 177–183.

5. Теплицький Б. Б. Сучасні можливості судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Юридичний часопис Національної академії внутрішніх справ.* 2021. № 1 (21). С. 30–37.

6. 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.

які засвідчують апробацію матеріалів дисертації:

7. Теплицький Б. Б. Практичні проблемні питання призначення комп'ютерно-технічної судової експертизи в кримінальних провадженнях. *Актуальні проблеми криміналістики та судової експертології*: матеріали міжвідом. наук.-практ. конф. (Київ, 22 листоп. 2018 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2018. С. 406–409.

8. Теплицький Б. Б. Щодо завдань комп'ютерно-технічних експертиз при розслідуванні незаконного зайняття гральним бізнесом в Україні. *Судова експертиза: сучасність та майбутнє*: матеріали круглого столу (м. Львів, 25 січня 2018 р.); за заг. ред. д. т. н. Кузіна М.О. / Львівський науково-дослідний інститут судових експертиз Міністерства юстиції України. Львів, 2019. С. 127–129.

9. Теплицький Б. Б. Особливості оцінки результатів судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Використання досягнень сучасної науки й техніки в розкритті злочинів* : матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лют. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 223–225.

10. Теплицький Б. Б. Особливості суб'єктної складової техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку. *Кримінальне судочинство: сучасний стан та перспективи розвитку*: матеріали Всеукр. наук.-практ. конф. (Київ, 28 трав. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 384–387.

11. Теплицький Б. Б. Щодо визначення терміну «техніко-криміналістичне забезпечення розслідування кримінальних правопорушень». *Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності:* зб. матеріалів засідання № 1 постійно діючої Міжнар. наук.-практ. конф. (м. Кропивницький, 24 верес. 2021 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2021. С. 71–74.

які додатково відображають наукові результати дисертації:

12. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп’ютерно-технічних судових експертиз: наук.-практ. посіб. / Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін. Київ: ПАЛИВОДА А.В., 2019. 168 с.