КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця

на правах рукопису

НЕДІЛЬКО ЯРОСЛАВ ВАЛЕНТИНОВИЧ

УДК 343.985

ДИСЕРТАЦІЯ
РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Спеціальність 081 Право

Галузь знань 08 Право

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ Я. В. Неділько

Науковий керівник: Костюченко Олена Юріївна, кандидат юридичних наук, доцент

Київ – 2023

АНОТАЦІЯ

Неділько Я. В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 Право. Київський національний університет імені Тараса Шевченка, Київ, 2023.

У дисертації сформульовано наукові висновки, рекомендації, пропозиції, що можуть мати важливе теоретичне значення для криміналістичної науки та бути практично застосованими під час розслідування кримінальних правопорушень, що вчиняють з використанням інформаційних комп'ютерних технологій.

Досліджено генезу «комп'ютерних злочинів», встановлено, що першим задокументованим випадком у світі, пов'язаним зі злочинним використанням комп'ютера, можна визнати протиправні дії програміста М. А. Беннета, який змінив код програмного забезпечення Національного міського банку Міннеаполіса 1966 року. Фундатором дослідження «комп'ютерного злочину» вважають американця Д. Б. Паркера, який у книзі «Crime by Computer» (1976) запропонував визначення поняття «комп'ютерне зловживання» (*computer abuse*). Одним із перших поміж українських вчених на важливості наукового вивчення такого криміногенного явища, як «комп'ютерні злочини», акцентував П. Д. Біленчук 1991 року.

Праці українських вчених-криміналістів, що стосуються проблемних питань розслідування «комп'ютерних злочинів», запропоновано об'єднати в декілька груп за часовими межами: 1) дослідження українських науковців із часу проголошення незалежності України до початку XXI століття (1991–2000 роки); 2) наукові дослідження з методики розслідування «комп'ютерних злочинів», проведені протягом 2001–2014 років; 3) дослідження, здійснені в період з 2014 року й донині.

Визначено, що під кримінальними правопорушеннями, що вчиняються з використанням інформаційних комп'ютерних технологій, слід розуміти використання інформаційних технологій, де є поєднання програмних засобів (software) і вибраного комплексу технічних засобів (hardware) у протиправних цілях.

Синонімічними до поняття «кримінальні правопорушення, що вчиняються з використанням інформаційних комп'ютерних технологій» є терміни «кримінальні кіберправопорушення» та «кіберзлочини».

Поняття «кримінальне кіберправопорушення» використовують згідно з термінологією Кримінального кодексу України, а поняття «кіберзлочин» – як таке, що відповідає міжнародним стандартам, а також його активно використовують у міжнародній практиці.

Запропоновано криміналістичну класифікацію кримінальних правопорушень, які вчиняють з використанням інформаційних комп'ютерних технологій, розглядати за кримінально-правовими та криміналістичними критеріями. За кримінально-правовими критеріями їх можна класифікувати в межах розділів Кримінального кодексу України, за криміналістичними – за особою злочинця, мотивом і метою, особою потерпілого, наслідками тощо.

Розглянуто міжнародно-правові засади розслідування, визначені в міжнародних нормативно-правових актах: Європейській конвенції про взаємну допомогу у кримінальних справах; Декларації ООН про злочинність і суспільну небезпеку; Конвенції ООН проти транснаціональної організованої злочинності; Конвенції про кіберзлочинність.

З'ясовано, що більшість країн гостро реагують на виклики кіберзлочинності, свідченням цього є створення спеціальних структурних підрозділів у системі їхніх правоохоронних органів з розслідування або допомоги в розслідуванні таких протиправних діянь. У цьому контексті міжнародне співробітництво між державами має вагоме значення для ефективного розслідування кримінальних правопорушень, які вчиняють з використанням комп'ютерних інформаційних технологій.

Встановлено, що елементи криміналістичної характеристики досліджуваної категорії кримінальних правопорушень знаходяться в кореляційному зв'язку (імовірних залежностях) між собою, а саме спосіб вчинення – зі слідами вчинення, обстановка – з особою злочинця.

Способом вчинення окреслених кримінальних правопорушень слід вважати сукупність послідовних дій суб'єкта (суб'єктів), що охоплюють дії з готування, вчинення та приховування, спрямовані на досягнення певного злочинного результату з використанням інформаційних комп'ютерних технологій.

З огляду на реалії сьогодення, визначено найтиповіші та найпоширеніші способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій: 1) використання шкідливого програмного забезпечення; 2) вчинення DoS/DDoS атак; 3) несанкціонований доступ до інформації; 4) шахрайство, вчинене з використанням інформаційних комп'ютерних технологій; 5) поширення шкідливого (протиправного) контенту (спам, погрози, створення, поширення та збут дитячої порнографії, заклики до вчинення насильства, домагання тощо); 6) порушення авторських чи суміжних прав з використанням інформаційних комп'ютерних технологій; 7) комплекс способів використання інформаційних комп'ютерних технологій як засіб користування кіберпростором для вчинення інших кримінальних правопорушень.

Доведено, що характер залишених електронних слідів залежить від таких факторів: виду операційної системи злочинця та потерпілого, особливостей засобів інформаційних комп'ютерних технологій та їх програмного забезпечення тощо. Водночас обґрунтовано, що під час розслідування кримінальних правопорушень цієї категорії не слід нехтувати матеріальними й ідеальними слідами.

У структурі обстановки як елементу криміналістичної характеристики зазначених протиправних діянь виокремлено: 1) кіберпростір, що передбачає місце, час, віртуальну взаємодію учасників кримінального правопорушення; 2) матеріальне середовище – ділянка території, сукупність різних предметів, поведінка учасників події, психологічні відносини.

Визначено типові ознаки, що характеризують особу кіберзлочинця: 1) загальні (вік, освіта, професія); 2) психологічні (темперамент, характер, інтереси та схильності, мотиви й стиль поведінки, певні психічні відхилення); 3) спеціальні («професійні звички», «почерк» кіберзлочинця).

Констатовано, що планування розслідування зазначених кримінальних правопорушень має відбуватися в письмовій формі. Це зумовлено специфікою таких кримінальних правопорушень, складністю термінології, браком навичок у слідчих з розслідування, необхідністю залучення спеціаліста, а також особливостями проведення слідчих (розшукових) і негласних слідчих (розшукових) дій та організаційних заходів тощо. План розслідування може бути складено як шляхом письмового викладення слідчим його змісту, що є результатом його розумової діяльності, так і за допомогою застосування програмних засобів.

Розглянуто тактичні особливості проведення огляду місця події в кримінальних правопорушеннях, що вчиняють з використанням інформаційних комп'ютерних технологій, аргументовано доцільність запрошення понятих для участі в проведенні огляду місця події з міркувань, що зазначені особи потім можуть бути допитані під час судового розгляду як свідки та своїми показаннями сприятимуть визнанню зібраних (отриманих) доказів допустимими.

Розроблено тактичні рекомендації проведення обшуку: 1) у клопотанні про обшук слід чітко визначити засоби інформаційно-комп'ютерних технологій, які необхідно відшукати, а до проведення обшуку ознайомитися з їх характеристикою; 2) якщо під час обшуку виявлено доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, які не зазначені в ухвалі слідчого судді, але щодо яких є достатні підстави вважати, що інформація, яка на них міститься, має значення для встановлення обставин у кримінальному провадженні, слідчий, прокурор має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них містяться, на місці проведення обшуку. У разі їх вилучення такі речі вважають тимчасово вилученим майном (ч. 6 ст. 236 Кримінального процесуального кодексу України); 3) необхідно встановити психологічний контакт з особою, у якої відбувається обшук; 4) слід зосередити

увагу на всіх пристроях збереження даних (флешки, диски тощо); 5) у разі необхідності провести груповий обшук.

Виокремлено особливості проведення допиту потерпілих і підозрюваних у кримінальних правопорушеннях, які вчиняють з використанням інформаційних комп'ютерних технологій, а також основні питання, що можуть ставити під час допиту потерпілому й підозрюваному в зазначених кримінальних правопорушеннях.

Акцентовано на необхідності під час планування допиту використовувати можливості штучного інтелекту, який слідчий, дізнавач, прокурор зможуть використовувати як для підготовки до допиту, так і під час його проведення. Штучний інтелект буде рекомендувати, які питання ставити залежно від виду та специфіки розслідування кримінального правопорушення, і спрямовувати перебіг допиту в ефективному напрямі.

Обґрунтовано значущість залучення спеціаліста в кримінальних правопорушеннях цієї категорії, а також проведення експертизи комп'ютерної техніки та програмних засобів.

Ключові слова: інформаційні комп'ютерні технології, інформаційні відносини, кримінальні кіберправопорушення, кіберзлочин, нейронна мережа, електронний доказ, досудове розслідування, планування розслідування, судовий контроль, допит підозрюваного та потерпілого, застосування заходів забезпечення, використання спеціальних знань.

ABSTRACT

Nedilko Ya. V. Investigation of criminal offenses committed using information computer technologies. – Qualification scientific work on the rights of a manuscript.

Dissertation for the degree of Doctor of Philosophy (PhD) in specialty 081 «Law». Taras Shevchenko National University of Kyiv, Kyiv, 2023.

The dissertation contains scientific conclusions, recommendations, and suggestions that can be of great theoretical importance for forensic science and can be practically applied in the investigation of criminal offenses committed using information computer technologies.

The historical genesis of «Computer Crimes» is investigated and it is established that the first documented case in the world related to the criminal use of a computer can be considered the illegal actions of programmer M. A. Bennett, who changed the software code of the National City Bank of Minneapolis in 1966. One of the first founders of the study of «computer crime» in the world can be considered the American D. B. Parker, who in his book «Crime by Computer» (1976) gives a definition of the concept of «computer abuse» («computer abuse»). One of the first Russian scientists who in 1991 focused his attention on the importance of scientific study of such a criminogenic phenomenon as «computer crimes» can be considered P. D. Bilenchuk.

It is proposed to combine the research of Ukrainian forensic scientists concerning problematic issues of investigation of «Computer Crimes» into several groups beyond time limits: 1) research of Ukrainian scientists from the time of the declaration of independence of Ukraine to the beginning of the XXI century (1991–2000); 2) scientific research on the methodology of investigation of «computer crimes» in the period from 2001 to 2014; 3) research conducted in the period from 2014 to the present.

It is determined that criminal offenses committed with the use of information computer technologies should be understood as the use of those Information Technologies where there is a combination of software and a selected set of technical means (hardware) for illegal purposes.

The concept of «cybercrime» can also be considered synonymous with «criminal offenses committed using information computer technologies».

Forensic classification of criminal offenses committed using information computer technologies should be considered according to criminal law and forensic criteria.

According to criminal law criteria, it is possible to classify by sections of the Criminal Code of Ukraine.

According to forensic criteria: the identity of the criminal, motive and purpose, the identity of the victim, consequences, and so on.

The article analyzes the international legal bases of Investigation defined in international regulatory legal acts: the European Convention on mutual assistance in criminal matters; the UN Declaration on crime and public danger; the UN Convention Against Transnational Organized Crime; The Convention on cybercrime.

It was found out that foreign countries react sharply to the challenges of cybercrime, as evidenced by the creation of special structural divisions in the system of their law enforcement agencies to investigate or assist in the investigation of these illegal acts. In this regard, international cooperation between states is essential for the effective investigation of criminal offenses committed using computer information technologies.

It is determined that the elements of the criminalistic characteristics of the studied category of criminal offenses are in correlation (probable dependencies) with each other, namely, the method of commission with traces of commission and the situation with the identity of the criminal.

The method of committing certain criminal offenses should be understood as a set of sequential actions of the subject (s), including actions for preparation, Commission and concealment, which are aimed at achieving a certain criminal result using information computer technologies.

Taking into account the realities of today, we can talk about the most typical and widespread methods of committing criminal offenses using information computer technologies: 1) the use of malicious software; 2) the commission of DoS/DDoS attacks; 3) unauthorized access to Information; 4) fraud committed using information computer technologies; 5) the distribution of harmful (illegal) content (spam, threats, creation,

distribution and sale of child pornography, calls to commit violence, harassment, etc.); 6) violation of copyright or related rights using information computer technologies; 7) a set of methods and use of Information Computer Technologies as a means of using cyberspace to commit other criminal offenses.

It is established that the nature of the electronic traces left depends on the following factors: the type of operating system of the criminal and the victim, the features of Information Computer Technologies and their software, and so on. However, when investigating criminal offenses of this category, one should not neglect material and ideal traces.

It is proposed in the structure of the situation as an element of criminalistic characteristics of these illegal acts, it is necessary to distinguish: 1) cyberspace, characterized by the place, time, virtual interaction of participants in a criminal offense; 2) material environment – a section of territory, a set of different objects, behavior of participants in the event, psychological relationships.

Typical features that characterize the identity of a cybercriminal are identified: 1) general (age, education, profession); 2) psychological (temperament, character, interests and inclinations, motives and style of behavior, certain mental deviations); 3) special («professional habits» and «handwriting» of a cybercriminal).

It is investigated that planning the investigation of these criminal offenses should take place in writing. This is due to the specifics of these criminal offenses, the complexity of terminology, the lack of skills of investigators in the investigation, the need to attract a specialist, as well as the characteristic features of conducting investigative (search) and secret investigative (search) actions and organizational measures, etc.

The tactical features of conducting an inspection of the scene of an accident in criminal offenses committed using information computer technologies are considered and the expediency of inviting witnesses to participate in conducting an inspection of the scene of an accident is noted for reasons that these persons can then be questioned during the trial as witnesses, and their testimony will contribute to confirming the collected (received) evidence as permissible.

The expediency of inviting the witnesses to participate in the inspection of the scene for reasons that these persons may then be questioned during the trial as witnesses and their shows will help to confirm the (obtained) evidence of the evidence.

Proposed tactical recommendations for conducting a search: 1) in the request for a search, you should clearly define the means of information and computer technologies that need to be found, and before conducting a search, familiarize yourself with their characteristics; 2) if during the search access or possibility of access to computer systems or their parts, mobile terminals of communication systems is revealed, which are not specified in the decision of the investigating judge, but in respect of which there are sufficient grounds to believe that the information contained on them is relevant for establishing the circumstances in criminal proceedings, the investigator, prosecutor has the right to search, identify and record the computer data contained on them at the place of the search. In case of their withdrawal, such items are considered temporarily seized property (Part 6 of Article 236 of the Criminal Procedure Code of Ukraine); 3) establishing psychological contact with the person who is being searched; 4) pay attention to all data storage devices (flash drives, disks, etc.); 5) if necessary, conduct a group search.

The peculiarities of the interrogation of victims and suspects of criminal offenses committed with the use of information and computer technologies are noted, as well as the main questions that may be asked of the victim and suspect during their interrogation of the specified criminal offenses are highlighted.

We do not rule out using the capabilities of artificial intelligence when planning an interrogation, which the investigator, Inquirer, and prosecutor will be able to use both in preparation for the interrogation and during its conduct. The AI will recommend what questions should be asked depending on the type and specifics of the investigation of a criminal offense and direct the course of questioning in an effective direction.

It is noted about the special importance of attracting a specialist in criminal offenses of this category, as well as about the significant importance of expertise of computer equipment and software tools.

Keywords: information computer technologies, information relations, criminal cyber offenses, cyber crimes, neural network, electronic evidence, pre-trial investigation, investigation planning, judicial control, interrogation of the suspect and the victim, application of security measures, use of special knowledge.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації:

1. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

2. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–174. URL: http://www.lsej.org.ua/1_2019/47.pdf. (Особистий внесок здобувача полягає: автором визначенні ознаки особи кіберзлочинця).

3. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. С. 359– 364. URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf.

4. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*. 2020. Вип. 88. С. 202–212. (Серія «Юридичні і політичні науки»).

5. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Криміналістика і судова експертиза*. 2021. Вип. 66. С. 453–460.URL : http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf.

6. Неділько Я. В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 292–301. DOI: https://doi.org/10.33994/kndise.2022.67.30.

Наукові праці, в яких опубліковані наукові результати дисертації, у зарубіжних спеціальних виданнях:

7. Nedilko Ya. Tactical Features of Conducting a Search in the Investigation of Cybercrimes. *European Reforms Bulletin.* 2021. № 3. С. 73–77. URL: http://aord.com.ua/wp-content/uploads/2021/11/European-Reforms-Bulletin_3_2021-2.pdf.

8. Неділько Я. В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій. *Knowledge, Education, Law, Management.* 2021. № 8 (44). Vol. 2. С. 119–124. DOI: https://doi.org/10.51647/kelm.2021.8.2.19.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Неділько Я. В. Строки досудового розслідування у контексті змін до кримінального процесуального кодексу України. *Проблеми реформування кримінальної юстиції України* : зб. матеріалів Міжнар. наук.-практ. конф. (Чернівці, 17–18 трав. 2018 р.). С. 198–201.

10. Неділько Я. В. Класифікація особи кіберзлочину як елемента криміналістичної характеристики. *Пріоритетні напрямки розвитку правової системи України* : матеріали Міжнар. наук.-практ. конф. (Львів, 25–26 січ. 2019 р.). С. 112–114.

11. Неділько Я. В. Спосіб вчинення злочину як елемент криміналістичної характеристики кіберзлочинів. *Conceptul de dezvoltare a statului de drept in repiblica Moldova si Ucraina in contextual proceselor de eurointegrare* (Chisinau, 1–2 noiembrie 2019). Chisinau, Republica Moldova, 2019. С. 236–238.

12. Неділько Я. В. Проблемні питання підслідності кіберзлочинів. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці* : матеріали Міжнар. круглого столу (Харків, 12 груд. 2019 р.). Харків, 2019. С. 105–109.

13. Неділько Я. В. Поняття кіберзлочину та особливості його закріплення в національному законодавстві. «*Інтернет речей»: проблеми правового регулювання та впровадження* : матеріали II наук.-практ. конф. (Київ, 29 листоп. 2018 р.). Київ, 2018. С. 112–114.

14. Неділько Я. В. Особливості проведення допиту підозрюваного у кіберзлочинах. *Кримінальний процес та криміналістика: сучасний стан та перспективи* : тези доп. Всеукр. наук.-практ. конф.(Харків, 26 листоп. 2020 р.). С. 252–255.

15. Неділько Я. В. Основні аспекти використання спеціальних знань під час розслідування кіберзлочинів. *Актуальні питання кримінального права, кримінології та судочинства* : матеріали Всеукр. наук.-практ. конф., присвяч. 165-й річниці з дня народж. проф. Л. С. Білогриць-Котляревського (Київ, 15 трав. 2020 р.). Київ, 2020. С. 85–88.

16. Неділько Я. В. Використання штучної нейронної мережі при плануванні розслідування кіберзлочинів. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали II Міжнар. наук.-практ. інтернет-конф. (Київ, 19 листоп. 2020 р.). Київ, 2020. С. 382–385.

17. Nedilko Y. Typical investigative situations at the initial stage of cybercrime investigation. *Актуальні питання розвитку юридичної науки та практики :* матеріали Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених, присвяч. Дню науки Інституту права (Київ, 21 трав. 2021 р.) : у 2 т. Київ, 2021. Т. 2. С. 345.

18. Неділько Я. В. Особливості проведення огляду під час розслідування кіберзлочинів. *Донецький юридичний інститут МВС України: освітні традиції, перевірені часом* : матеріали Міжнар. наук.-практ. конф. до 60-річчя заснування закладу освіти (Маріуполь, 28 квіт. 2021 р.). Маріуполь, 2021. С. 279–292. URL: http://repo.dli.donetsk.ua/bitstream/123456789/1704/1/210512_1543_A5_442pages_i.pdf.

19. Неділько Я. В, Ахтирська Н. М. Особливості встановлення психологічного контакту слідчого з підозрюваним під час допиту щодо кіберзлочинів. *Актуальні проблеми кримінального процесу та криміналістики :*

тези доп. Міжнар. наук.-практ. конф. (Харків, 29 жовт. 2021 р.). Харків, 2021. С. 254–256.

20. Неділько Я. В. Використання штучного інтелекту під час розслідування кіберзлочинів. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України* : матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.). Київ, 2022. С. 275–278.

21. Неділько Я. В. Особливості проведення огляду комп'ютерних даних під час розслідування кіберзлочинів в у мовах воєнного стану. *Актуальні питання розвитку юридичної науки та практики :* матеріали Міжнар. наук.-практ. конф. (Київ, 12 трав. 2022 р.). Київ, 2022. С. 288–290.

22. Неділько Я. В. Процесуальна регламентація надання пояснень спеціалістом під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. *Використання цифрової інформації в розслідуванні кримінальних правопорушень* : матеріали Міжнар. наук.-практ. круглого столу (Харків, 12 груд. 2022 р.). Харків, 2022. С. 62–65. DOI: https://doi.org/10.31359/978-966-998-460-9.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕОМ – електронна обчислювальна машина

ЄРДР – Єдиний реєстр досудових розслідувань

ЄСПЛ – Європейський суд з прав людини

КК – Кримінальний кодекс

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

ООН – Організація Об’єднаних Націй

США – Сполучені Штати Америки

ФРН – Федеративна Республіка Німеччина

ШНМ – штучна нейронна мережа

ВСТУП

Актуальність теми. У сучасному світі відбувається стрімкий розвиток інформаційних технологій, що зумовлений науково-технічною революцією початку XXI століття. Більшість суб'єктів суспільних відносин уже не можуть ефективно функціонувати без використання інформаційних технологій, які призначені створювати, зберігати, обробляти, передавати інформацію різних видів і стали невід'ємною частиною життєдіяльності людини.

Активне поширення інформаційних технологій сприяло пришвидшеному розвитку суспільства загалом, водночас спричинило виникнення нового явища криміногенного походження – кримінальних правопорушень, що вчиняють з використанням інформаційних комп'ютерних технологій. Нині це одна з найдинамічніших груп суспільно небезпечних діянь, для вчинення яких не потрібно перебувати в особистому контакті з потерпілою особою, а достатньо мати доступ до засобів інформаційних комп'ютерних технологій.

Протиправне використання інформаційних комп'ютерних технологій може спричинити дезорганізацію роботи державних органів, дестабілізацію фінансово-економічної системи, завдати істотної шкоди безпеці держави й інтересам її громадян. Можна навести приклад здійснення кібератак на об'єкти критичної інфраструктури України, що на тривалий проміжок часу були виведені з ладу, а також використання вірусів «Petya», «Petya/Misha», «WannaCry» тощо, які дестабілізували роботу комп'ютерних систем і мереж різних підприємств та установ, завдавши значних збитків державі. Тому актуальною є необхідність забезпечення ефективної протидії таким загрозам.

Небезпеку, що становлять негативні вияви в контексті розвитку інформаційних технологій, усвідомлює і світова спільнота. Зазначене засвідчує прийняття 23 листопада 2001 року в Будапешті Конвенції Ради Європи про кіберзлочинність, що стала одним із базових міжнародно-правових документів, яку Україна ратифікувала 7 вересня 2005 року. Організація Об'єднаних Націй (ООН), Рада Європи, Європейський Союз та інші міжнародні інституції визнають

небезпеку кіберзлочинності та закликають до міжнародної співпраці в боротьбі із цими протиправними діяннями.

Україна також не стоїть осторонь вирішення проблемних питань протидії кримінальним правопорушенням, що вчиняють з використанням інформаційних комп'ютерних технологій. Позитивним поштовхом у цьому напрямі стали взяті Україною зобов'язання з інтеграції в міжнародну спільноту. Зокрема, на виконання Угоди про асоціацію з Європейським Союзом щодо боротьби з кіберзлочинами протягом 2015–2018 років було прийнято низку нормативних актів, спрямованих на запобігання кримінальним правопорушенням цієї категорії та щодо ефективного їх розслідування. Важливим здобутком у законодавчій сфері можна вважати прийняття 2017 року Закону України «Про основні засади забезпечення кібербезпеки в Україні». Для формування потенціалу стримування кіберзагроз у нашій державі та запобігання їхнім небажаним наслідкам Указом Президента України від 26 серпня 2021 року № 477/2021 було введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про стратегію кібербезпеки України». Вагомим кроком, спрямованим на боротьбу з кіберзлочинністю, стало й підписання Україною Другого додаткового протоколу до Конвенції про кіберзлочинність 30 листопада 2022 року, що спрямований на посилення співпраці та розкриття електронних доказів між державами.

Кримінальний кодекс України містить самостійний розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», статті якого передбачають відповідальність за вчинення протиправних дій. Крім того, з метою імплементації положень Ланцаротської конвенції 2021 року Кримінальний кодекс (КК) України доповнено ст. 156-1, 301-1, 302-1, у яких встановлено відповідальність за вчинення будь-яких дій сексуального характеру щодо дітей, зокрема з використанням інформаційних комп'ютерних технологій.

Згідно зі статистичними даними Офісу Генерального прокурора, серед кримінальних правопорушень, передбачених ст. 361–363-1 розділу XVI КК України, спостерігається тенденція щодо збільшення їх кількості. Якщо впродовж

2013 року обліковано 595 кримінальних правопорушень (до суду з обвинувальним актом направлено 256), то вже 2019 року їх було 2204 (1259), 2020-го – 2498 (1484), 2021-го – 3310 (1947), 2022-го – 3415 (2435). Істотне збільшення кількості кримінальних правопорушень зазначеної категорії спричинено стрімким розширенням сфери застосування інформаційних комп'ютерних технологій.

Унаслідок активізації кримінальних правопорушень цієї групи змінилися і показники судової статистики щодо засуджених осіб. Згідно з даними Державної судової адміністрації України, 2013 року за ст. 361–363-1 КК України засуджено 49 осіб, 2019-го – 50, 2020-го – 56, 2021-го – 76, 2022-го – 74 особи.

Аналіз наведених статистичних даних дає підстави стверджувати про низьку ефективність розслідування та розкриття кримінальних правопорушень, передбачених розділом XVI КК України. Зазначене спричинено недостатнім рівнем знань і практичних навичок у суб'єктів розслідування в процесі розслідування досліджуваної категорії кримінальних правопорушень.

Слід ураховувати, що дана статистична інформація не цілком відображає ситуацію щодо вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій в Україні, оскільки обмежується лише розділом XVI КК України, оскільки залишає поза увагою інші кримінальні правопорушення, що можуть вчиняти з використанням інформаційних комп'ютерних технологій.

Проблемні аспекти розслідування кримінальних правопорушень зазначеної категорії висвітлено в працях вчених-криміналістів: Н. М. Ахтирської, П. Д. Біленчука, А. С. Білоусова, В. М. Бутузова, В. О. Голубєва, В. Г. Гончаренка, М. В. Гуцалюка, І. В. Європіної, В. А. Журавля, Є. Д. Лук'янчикова, Б. Є. Лук'янчикова, О. В. Манжая, А. І. Марущака, О. І. Мотляха, Л. П. Паламарчук, О. А. Самойленко, В. Г. Хахановського та ін.

Теоретичне підґрунтя цього наукового дослідження становлять праці українських та іноземних учених: В. П. Бахіна, В. К. Весельського, А. Ф. Волобуєва, Г. Гросса, В. І. Галагана, В. Г. Гончаренко, В. О. Гринюка, В. А. Динту, М. В. Карчевського, Н. І. Клименко, О. Н. Колесниченка,

О. Ю. Костюченко, В. О. Коновалової, І. І. Когутича, О. П. Кучинської, В. К. Лисиченка, Г. А. Матусовського, І. Ю. Мірошнікова, М. А. Погорецького, М. В. Салтевського, Д. Б. Сергєєвої, В. В. Тіщенка, Ю. М. Чорноус, В. М. Шевчука, В. Ю. Шепітька, М. Є. Шумила, М. Г. Щербаковського та ін.

Попри вагомі напрацювання дослідників у цій сфері, більшість теоретичних і практичних питань розслідування кримінальних правопорушень, що вчиняють з використанням інформаційних технологій, залишається невирішеними. Розвиток криміналістичних знань не відповідає темпам поширення інформаційних технологій у суспільстві, а отже, постає потреба напрацювання сучасних рекомендацій щодо розслідування таких кримінальних правопорушень.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано на кафедрі кримінального процесу та криміналістики в межах планів наукової роботи Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка в межах планів науково-дослідних робіт юридичного факультету за напрямом «Доктрина права в правовій системі: теоретичні та практичні аспекти».

Тему дисертації «Розслідування злочинів, що вчиняються з використанням інформаційних технологій (кіберзлочинів)» затверджено рішенням Вченої ради юридичного факультету Київського національного університету імені Тараса Шевченка 28 листопада 2019 року (протокол №5). Тему дисертації уточнено рішенням Вченої ради Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка 28 лютого 2023 року (протокол № 14) на «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій».

Мета і завдання дослідження. Мета роботи полягає в комплексному дослідженні особливостей розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, у контексті аналізу положень криміналістичної науки, норм національного законодавства й міжнародного досвіду, а також різних наукових підходів і практики їх застосування.

Поставлена мета зумовлює необхідність виконання таких *завдань*:

– окреслити генезу виникнення та стан наукових досліджень криміналістичних проблем розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– запропонувати криміналістичну класифікацію кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– висвітлити міжнародно-правові засади й іноземний досвід розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– визначити елементний склад криміналістичної характеристики досліджуваної категорії кримінальних правопорушень;

– окреслити способи вчинення зазначених кримінальних правопорушень і сліди їх вчинення;

– дослідити обстановку вчинення та надати характеристику особи злочинця в кримінальних правопорушеннях, вчинених з використанням інформаційних комп'ютерних технологій;

– виокремити слідчі ситуації, що можуть виникати під час розслідування цієї категорії кримінальних правопорушень;

– висловити пропозиції щодо удосконалення формування слідчих версій та планування розслідування кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій;

– схарактеризувати тактичні особливості проведення окремих слідчих (розшукових) дій;

– визначити особливості використання спеціальних знань під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Об'єкт дослідження – правовідносини, що виникають між суб'єктами, які проводять досудове розслідування, слідчим суддею та іншими учасниками

кримінального провадження (підозрюваними, свідками, потерпілими, експертами, спеціалістами та іншими).

Предмет дослідження – розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Методи дослідження. Методологічну основу дисертаційного дослідження становлять загальнонаукові та спеціальні методи наукового пізнання. Зокрема, *історико-правовий* метод застосовано для аналізу виникнення такого криміногенного явища, як «комп'ютерний злочин», розвитку міжнародного й національного законодавства окремих країн щодо боротьби із цими протиправними діяннями, а також дослідження наукових праць вітчизняних учених за цією тематикою; *соціологічний та статистичний* методи використано під час проведення опитування прокурорів і здійснення аналізу отриманих даних, а також під час узагальнення судової практики; *системно-структурний* – для формування криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, слідчих ситуацій та версій розслідування; метод *моделювання* – для розроблення криміналістичних рекомендацій щодо планування розслідування, проведення окремих слідчих (розшукових) дій та негласних слідчих (розшукових) дій, а також призначення відповідних експертиз під час розслідування зазначених кримінальних правопорушень; *догматичний* метод застосовано для визначення і тлумачення понять, що сприяло уточненню понятійного апарату роботи.

Емпіричну базу дослідження становлять результати опитування 200 прокурорів, які здійснюють організацію та процесуальне керівництво досудовим розслідуванням і підтримують публічне обвинувачення в суді, статистичні дані Офісу Генерального прокурора (Генеральної прокуратури України) та Державної судової адміністрації України, матеріали вітчизняної та міжнародної слідчої та судової практики.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим в Україні дослідженням, в якому на підставі аналізу наукових підходів вітчизняних та зарубіжних вчених, слідчої та судової практики, визначено

теоретичні та практичні особливості проведення розслідування в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій. З-поміж найважливіших положень, що становлять наукову новизну, слід виокремити такі:

вперше:

– запропоновано класифікацію наукових досліджень вчених-криміналістів Незалежної України щодо розслідувань «комп'ютерних злочинів», «кіберзлочинів», «злочинів у кіберпросторі» тощо;

– обґрунтовано доцільність використання терміну «інформаційні комп'ютерні технології» серед інших суміжних термінів;

– розроблено криміналістичну класифікацію кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– запропоновано в процесі планування, висунення версій та проведення допиту потерпілого та підозрюваного під час розслідування кримінальних правопорушень, що вчиняють з використанням інформаційних комп'ютерних технологій, використовувати можливості штучної нейронної мережі (ШНМ) та штучного інтелекту;

– аргументовано поділ на чотири етапи (вихідний, початковий, наступний, завершальний) проведення розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– конкретизовано слідчі ситуації, що можуть виникати на кожному з етапів розслідування зазначеної категорії кримінальних правопорушень;

– запропоновані відповідні зміни та уточнення положень Кримінального процесуального кодексу України, що стосуються тематики дослідження (додаток 1).

удосконалено:

– елементний склад криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– визначення форм електронної інформації, що може знаходитися у засобах інформаційних комп'ютерних технологій;

– конкретизацію ознак особи кіберзлочинця;

– рекомендації щодо встановлення психологічного контакту між слідчим і допитуваною особою;

– наукові та практичні рекомендації щодо проведення огляду місця події, обшуку й допиту в зазначених кримінальних правопорушеннях;

набуло подальшого розвитку:

– визначення способів вчинення кримінальних правопорушень даного виду кримінальних правопорушень;

– теоретичне формування обстановки кримінальних правопорушень зазначеної категорії;

– визначення електронних доказів у кримінальному провадженні;

– положення, що стосуються участі спеціаліста під час розслідування кримінальних правопорушень досліджуваної категорії;

– тактичні рекомендації щодо призначення та проведення судових експертиз під час розслідування цієї категорії кримінальних правопорушень.

Практичне значення одержаних результатів полягає в тому, що сформульовані в дисертації висновки, рекомендації, положення та пропозиції може бути використано в:

– практичній діяльності – безпосередньо слідчими, дізнавачами, прокурорами з метою підвищення ефективності розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій (акт Національної поліції України від 07.04.2023 р.; акт Верховного Суду № 216/0/158-23 від 03. 05. 2023 р.; акт Тренінгового центру прокурорів України від 26.04.2023 р.);

– науково-дослідній діяльності – для подальших наукових досліджень методики розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій;

– освітньому процесі – під час викладання курсу криміналістики в закладах вищої освіти юридичного профілю, для підготовки підручників, навчальних і методичних посібників (акт факультету правничих наук Національного університету «Києво-Могилянська академія» від 19.04.2023 р.; акт кафедри кримінального права та правоохоронної діяльності юридичного факультету Запорізького національного університету від 01.05.2023 р.).

Особистий внесок здобувача. Усі сформульовані в дисертації висновки та положення обґрунтовано на підставі власних досліджень. Нові наукові результати отримані дисертантом особисто. У співавторстві опубліковано одну наукову статтю «Криміналістична характеристика: особа кіберзлочинця» (*Юридичний науковий електронний журнал.* 2019. № 1. С. 171–175). Особистий внесок здобувача полягає у визначенні ознак особи кіберзлочинця. Дисертація є самостійним науковим дослідженням автора.

Апробація результатів дисертації. Основні висновки, положення, пропозиції дисертаційного дослідження обговорювалися на засіданнях кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка, а також були оприлюднені на науково-практичних конференція та круглих столах, серед яких: Круглий стіл «Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці» (Харків, 12 грудня 2019 рік); Всеукраїнська науково-практична конференція «Актуальні питання кримінального права, кримінології та судочинства», присвяченої 165-річниці з дня народження професора Л.С. Білогриць-Котляревського (Київ, 15 травня 2020 рік); Всеукраїнська науково-практична конференція «Кримінальний процес та криміналістика: сучасний стан та перспективи» (Харків, 26 листопада 2020 рік); II-га міжнародна науково-практична інтернет-конференція «Актуальні питання судової експертології, криміналістики та кримінального процесу» (Київ, 19 листопада 2020 рік); Міжнародна науково-практична конференції «Донецький юридичний інститут МВС України: освітні традиції, перевірені часом» до 60-річчя заснування закладу освіти (Маріуполь, 28 квітня 2021 рік); Міжнародна науково-

практична конференція «Актуальні питання розвитку юридичної науки та практики» (Київ, 12 травня 2022 рік); Міжнародний науково-практичний круглий стіл «Використання цифрової інформації в розслідуванні кримінальних правопорушень» (Харків, 12 грудня 2022 рік).

Структура та обсяг дисертації. Дисертація містить анотації, вступ, три розділи, що охоплюють 10 підрозділів, висновки, список використаних джерел (323 джерел на 32 сторінках) і 4 додатків (на 18 сторінках). Загальний обсяг дисертації становить 257 сторінок, з яких основного тексту – 189 сторінки.

РОЗДІЛ 1
МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

1.1. Генеза виникнення та стан наукових криміналістичних досліджень проблем розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Засоби інформаційних технологій стали невід'ємною частиною повсякденного життя людей. Використання їх спрощує виконання побутових справ, відкриває нові можливості для роботи, дає змогу вдосконалювати та пришвидшувати вже наявні процеси життєдіяльності. Проте, теперішні інформаційні технології, які ми маємо у сучасному вигляді пройшли тривалий шлях розвитку та вдосконалення.

Аналізуючи історію розвитку інформаційних технологій за видами інструментарію технологій, науковці виокремлюють декілька етапів їх становлення:

1) «ручний» (з давніх часів до другої половини XIX ст.), який вирізняється ручною обробкою інформації (за допомогою пера й рахівниць), а зв'язок відбувався шляхом пересилання листів і пакетів;

2) механічний (з кінця XIX ст.), що ознаменувався винайденням друкарської машинки й телефону, вдосконаленням системи поштового зв'язку;

3) електричний (з 1940-х років XX ст. до 1960 років XX ст.) – розроблення перших електронно-обчислювальних машин (ЕОМ) і створення електричних писальних машинок, копіювальних технічних пристроїв тощо;

4) електронний (з початку 70-х років XX ст.) – створення на базі ЕОМ автоматизованих систем управління та інформаційно-пошукових систем, що оснащені широким спектром базових і програмних комплексів;

5) комп'ютерний етап (із середини 80-х рр. XX ст.) — «комп'ютерна» («нова») технологія, головним обладнанням якої є персональний комп'ютер [82].

Саме з виникненням і розвитком персональних комп'ютерів та комп'ютерних систем більшість учених-криміналістів пов'язують появу нового виду кримінальних правопорушень – «комп'ютерних злочинів».

Перший «комп'ютерний злочин» учинено задовго до того, коли персональний комп'ютер почав з'являтися в кожній оселі.

Один із перших задукоментованих випадків, пов'язаних зі злочинним використанням комп'ютера, стався 1966 року в штаті Міннеаполіс (США). Програміст М. А. Беннет, маючи доступ до комп'ютерної системи Національного міського банку Міннеаполіса, написав код, який змінив програмне забезпечення так, що у звітах не відображалося перевищення кредитного ліміту на його особистому рахунку. У зв'язку з виходом з ладу комп'ютерної системи, банк повернувся до ручної обробки й виявив невідповідності на рахунку Беннета. Згодом ФБР провело розслідування, а Беннет отримав умовний строк у січні 1967 року. Цю справу в історії вважають першою, що пов'язана зі злочинним використанням комп'ютера [287].

Фундатором дослідження «комп'ютерних злочинів» став американець Д. Б. Паркер. У своїй книзі «Crime by Computer» (1976) учений сформулював визначення поняття «комп'ютерне зловживання» (*computer abuse*), яке потлумачив як інцидент, учинений умисно, унаслідок якого жертва зазнала або могла зазнати збитків, а виконавець отримав або міг отримати вигоду, використовуючи комп'ютер [278, с. 25].

Першою країною, що здійснила законодавче закріплення кримінальної відповідальності стосовно певних видів «комп'ютерних злочинів», є Швеція. Зокрема, у травні 1973 року прийнято закон «Про дані», що передбачав кримінальну відповідальність за неправомірну зміну, знищення або надання неправильної інформації умисно чи з необережності, що міститься в автоматизованій системі, особою, яка розпоряджається цією інформацією.

Відповідальність за вчинення таких дій – штраф чи позбавлення волі строком до одного року [316].

Водночас зазначений нормативно-правовий акт стосувався здебільшого захисту персональних даних фізичних осіб, які розміщені в автоматизованій системі (базах даних), а відповідальність стосувалася тільки осіб, які працюють з такою автоматизованою системою.

Протягом 1980–1990 років використання персональних комп'ютерів інтенсивно поширювалося на всіх континентах, що своєю чергою спричинило стрімкий розвиток «комп'ютерної злочинності». Тому в різних країнах нагальною стала необхідність криміналізації «комп'ютерних злочинів».

Однією з перших закріпила спеціальні норми про «комп'ютерні злочини» Федеративна Республіка Німеччина (ФРН). У травні 1986 року внесено зміни в КК ФРН, згідно з якими закріплено кримінальну відповідальність за комп'ютерне шахрайство (§263a); незаконне отримання відомостей, які можуть бути відтворені або передані електронним або магнітним шляхом (§ 202a); комп'ютерний саботаж (§ 303b) [267].

У жовтні того самого року в США прийнято федеральний закон «Про комп'ютерне шахрайство та зловживання», головна мета якого полягає в захисті секретної, фінансової та кредитної інформації, що розміщена в комп'ютерах уряду чи фінансових установ. Цей нормативний акт вніс низку поправок у 18-й звід законів США, главу 41, § 1030, а саме криміналізував такі дії: крадіжку майна за допомогою комп'ютера, що здійснюють у формі обману; змінення, пошкодження або знищення даних, що належать іншим особам, і незаконний продаж паролів [323].

Слід зауважити, що положення §1030 ще доповнювали 1988, 1989, 1990, 1994, 1996, 2001, 2002, 2008 та 2020 року [263].

1990 року прийнято закон про неправомірне використання комп'ютерів у Великій Британії [274]. Також 1994 року набув чинності КК Франції, у якому містився окремий розділ «Порушення в роботі автоматизованої системі обробки даних» [272].

Не є винятком й Україна, у законодавстві якої відповідальність за вчинення «комп'ютерних злочинів» було передбачено 1994 року. Зокрема, КК України 1960 року [120] встановлював відповідальність за «комп'ютерні злочини» лише в ст. 198-1 «Порушення роботи автоматизованих систем». Натомість у новому КК України 2001 року [119] вперше передбачено окремий розділ XVI.

Перший «комп'ютерний злочин» на території України зафіксовано 1990 року. Злочинець склав програму для ЕОМ, що здійснювала перерахунок комсомольських внесків робітників одного з промислових підприємств м. Луганська на розрахунковий рахунок районного комітету комсомолу, за якого відрахування відповідних грошових сум здійснювалося із заробітної плати не тільки членів комсомолу, а й решти робітників підприємства [34].

Попри те, що в Україні в кінці XX ст. «комп'ютерна злочинність» не була таким масовим явищем, як нині (протягом 1997–2001 років зареєстровано 52 посягання, що належали до «комп'ютерних злочинів» [2]), українські вчені різних галузей права зосереджували увагу як на теоретичних, так і на практичних аспектах цього криміногенного явища.

Оскільки загальноприйнятого визначення поняття цього виду кримінальних правопорушень не сформульовано, термін «комп'ютерні злочини» став узагальнювальним, його використовували в науковій літературі та практичній діяльності. Необхідно зазначити, що науковцями використовуються різні поняття: «злочини у сфері комп'ютерної інформації», «інформаційні злочини», «злочини у сфері ЕОМ», «злочини у сфері комп'ютерних технологій», «кіберзлочини» тощо.

Вважаємо за доцільне наукові дослідження українських учених-криміналістів, що стосуються проблемних питань розслідування «комп'ютерних злочинів», об'єднати в декілька груп за часовими межами.

Першу групу становлять дослідження українських учених із часу проголошення незалежності України до початку XXI ст. (1991–2000). Протягом цього періоду формується загальне уявлення та методика розслідування цього нового виду кримінальних правопорушень – «комп'ютерних злочинів».

Друга група – наукові дослідження щодо методики розслідування «комп'ютерних злочинів» періоду з 2001-го до 2014 року. Необхідність проведення наукових досліджень була зумовлена стрімким розвитком і запровадженням інформаційних технологій у всіх сферах суспільного життя, що своєю чергою спричинило істотне збільшення кількості таких кримінальних правопорушень. Також у цей період відбувається ратифікація Україною Конвенції Ради Європи про кіберзлочинність [99], а КК 2001 року [119] містить самостійний розділ про зазначені кримінальні правопорушення.

Третя група охоплює дослідження, які проводили з 2014 року й донині. Необхідність активізації здійснення криміналістичних досліджень цієї групи кримінальних правопорушень зумовлена насамперед військовою агресією рф проти України, зокрема і з використанням кіберпростору. Крім того, упродовж цього періоду прийнято чимало нормативних документів, спрямованих на запобігання кримінальним правопорушенням цієї категорії, серед яких: Закон України «Про основні засади забезпечення кібербезпеки в Україні» [193], Указ Президента України про введення в дію рішення Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» [197] тощо.

Розглядаючи першу групу наукових досліджень, слід зауважити, що одними з перших серед українських науковців сформулювали власне визначення поняття «комп'ютерна злочинність» П. Д. Біленчук і М. А. Зубань 1994 року. На думку зазначених дослідників, це суспільно небезпечна діяльність (чи бездіяльність), яку здійснюють з використанням інформаційних технологій з метою спричинення збитків державі, підприємствам, а також правам осіб [21].

Вагомий внесок у розвиток методики розслідування «комп'ютерних злочинів» робить П. Д. Біленчук – автор понад 600 праць, значна частина з яких стосується дослідження цього протиправного діяння. Цей вчений ще 1991 року акцентував на значущості наукового вивчення такого криміногенного явища, як «комп'ютерні злочини» [17].

Слід також виокремити роботу А. Ф. Волобуєва «Проблеми розслідування «комп'ютерних» злочинів (1996), у якій «комп'ютерний злочин» потлумачено як

окремий вид (групу) злочинів, у яких предметом посягання є специфічні ознаки комп'ютера або окремі елементи комп'ютерних систем, а об'єктом, відповідно, суспільні відносини з володіння, використання комп'ютерної техніки [44].

Науковий інтерес стосовно методики розслідування «комп'ютерних злочинів» у кінці XX ст. становлять праці В. О. Голубєва, а саме: «Комп'ютерні злочини в банківській діяльності» [50], «Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту» (1998) (у співавторстві з О. М. Юрченком) [55]; «Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації та її попередження» (1998) (у співавторстві з М. С. Вертузаєвим, О. І. Котляревським, О. М. Юрченком) [16]; «Правові проблеми захисту інформаційних технологій» [56]; «Теоретично-правові проблеми боротьби з комп'ютерною злочинністю» (1998) [52] тощо.

Значний науковий внесок у розслідування «комп'ютерних злочинів» зробили вчені: М. С. Вертузаєв «Комп'ютерна злочинність в Україні: міфи та реальність» (1997) [31]; В. Д. Гавловський та В. С. Цимбалюк «Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій» (1998) [45]; А. Ф. Волобуєв «Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки» (1998) [43], «Використання спеціальних знань при розслідуванні розкрадань з використанням комп'ютерної техніки» (1998) [42]; М. В. Салтевський «Основи методики розслідування злочинів, скоєних з використанням ЕОМ» (2000) [215]; О. М. Моісеєв «Залучення спеціаліста до розслідування комп'ютерних злочинів» (2000) [137] тощо.

Початок XXI століття ознаменувався другою групою наукових досліджень – проведенням низки ґрунтових дисертаційних робіт щодо розслідувань «комп'ютерних злочинів».

Слід виокремити кримінально-правове дисертаційне дослідження Д. С. Азарова «Кримінальна відповідальність за злочини у сфері комп'ютерної інформації» (2002) [2]. Попри те, що ця робота не стосується криміналістичної методики розслідування кримінальних правопорушень зазначеної категорії, однак у ній увагу зосереджено на кримінально-правовому аналізі «комп'ютерних

злочинів», що згодом дало підґрунтя для визначення понятійного апарату таких протиправних посягань.

Крім того, науковець сформулював поняття «злочини у сфері комп'ютерної інформації», згідно з яким це умисні суспільно небезпечні дії, що посягають на відносини щодо здійснення інформаційної діяльності стосовно комп'ютерної інформації, предметом і знаряддям вчинення яких є така інформація в різних її виявах (відомості, дані, комп'ютерні програми тощо) [2, с. 182].

Важливе значення для подальшого вдосконалення методики розслідування «комп'ютерних злочинів» мали й інші дисертаційні дослідження українських вчених-криміналістів.

Зокрема, 2004 року перше вітчизняне криміналістичне дисертаційне дослідження, що стосується розслідування «комп'ютерних злочинів», здійснила Л. П. Паламарчук («Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»). Учена розробила науково обґрунтовані рекомендації щодо криміналістичного забезпечення розслідування незаконного втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, розглянула особливості початкового етапу розслідування та проведення окремих слідчих (розшукових) дій, а також напрями підвищення ефективності виявлення та розслідування зазначених кримінальних правопорушень [164].

Зауважимо і про дисертаційне дослідження О. І. Мотляха «Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій» (2005), у якому науковець здійснив поглиблений аналіз наявних напрацювань українських та іноземних учених у сфері розслідування кримінальних правопорушень, пов'язаних з інформаційними технологіями [138].

Новизна наукового дослідження Л. В. Борисової «Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження» (2007) полягала у формулюванні авторського визначення поняття «транснаціональний комп'ютерний злочин», теоретичному обґрунтуванні поділу комп'ютерних злочинів за професійною ознакою, а також удосконаленню слідчих ситуацій

початкового етапу розслідування на базі вітчизняного й іноземного досвіду проведення окремих слідчих дій [25].

У роботі Д. В. Пашнєва «Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій» (2007) увагу спрямовано на методи й засоби виявлення, фіксації, вилучення та дослідження слідів злочинів, вчинених із застосуванням комп'ютерних технологій [166].

Дослідниця О. А. Самойленко «Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій» (2007) уперше проаналізувала механізм викрадень майна, вчинених із використанням комп'ютерних технологій, а також удосконалила концепцію використання спеціальних комп'ютерно-технічних знань під час розслідування зазначених кримінальних правопорушень [219].

Вагомий внесок у розроблення теоретичних і практичних рекомендацій з підготовки та проведення окремих слідчих (розшукових) дій під час розслідування «комп'ютерних злочинів» зробив А. С. Білоусов у дослідженні «Криміналістичний аналіз об'єктів комп'ютерних злочинів» (2008) [24].

Деякі проблемні питання розслідування кримінальних правопорушень з використанням інформаційних технологій проаналізовано в роботі В. Д. Поливанюка «Особливості розслідування злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій» (2008). Здійснено узагальнення нормативно-правових актів, що регулюють банківську діяльність і регламентують діяльність інформаційних технологій, досліджено механізм і способи вчинення кримінальних правопорушень у банківській діяльності України з використанням інформаційних технологій [170].

Виважене дослідження стосовно проблемних питань розслідування зазначених кримінальних правопорушень здійснила І. В. Європіна в роботі «Криміналістичне забезпечення протидії комп'ютерній злочинності» (2011). Учена розробила комплексні теоретичні положення криміналістичного забезпечення протидії комп'ютерній злочинності, зокрема щодо методики розслідування цих злочинів [72].

Доцільність використання поняття «злочини, вчинені з використанням інформаційних технологій» замість «комп'ютерні злочини» розглянуто в дисертаційному дослідженні Н. С. Козак «Криміналістичні прийоми, способи і засоби виявлення та розслідування комп'ютерних злочинів» (2011). Також у цій праці комплексно розглянуто способи й тактико-криміналістичні прийоми виявлення та розслідування таких протиправних діянь [94].

Деякі питання, що частково стосуються розслідування «комп'ютерних злочинів», науковці вивчали в інших криміналістичних дисертаційних дослідженнях (В. І. Пазиніч «Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України» (2009) [163]; Т. В. Михальчук «Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів» (2009) [136]; А. І. Анапольска «Розслідування шахрайств, пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків» (2011) [4]; А. В. Крижевський «Криміналістична характеристика шахрайств у сфері мобільного зв'язку» (2012) [107] тощо).

На монографічному рівні основні аспекти методики розслідування «комп'ютерних злочинів» у період з 2001-го до 2014 року висвітлили вчені-криміналісти.

Слід зауважити про колективну монографію «Інформаційна безпека: проблеми боротьби зі злочинами у сфері використанням комп'ютерних технологій» (2001 рік, за редакцією Р. А. Калюжного), у якій увагу зосереджено на проблемних питаннях методики виявлення та розслідування кримінальних правопорушень, вчинюваних у сфері використання комп'ютерних технологій, методиці виявлення та розслідування розповсюдження шкідливих комп'ютерних програм і технічних засобів [53].

У роботі «Розслідування комп'ютерних злочинів» (2003) В. О. Голубєв розглянув кримінально-правову та криміналістичну характеристику «комп'ютерних злочинів», а також тактичні особливості проведення окремих слідчих (розшукових) дій під час їх розслідування. Зауважимо, що вчений ототожнює поняття «комп'ютерний злочин» і «кіберзлочин» [51].

У монографії «Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій» (2009) О. А. Самойленко на підставі іноземної та вітчизняної слідчої практики розглянула проблемні питання криміналістичної характеристики таких протиправних діянь та особливості їх розслідування [219].

Основні питання криміналістичної характеристики й методики розслідування «комп'ютерних злочинів» висвітлено в навчальних і науково-практичних посібниках:

– «Криміналістика» (підручник, 2001 рік, за загальною редакцією П. Д. Біленчука), у главі «Основи методики розслідування злочинів у галузі інформаційних технологій» якої висвітлено поняття і загальну характеристику злочинів, що вчинені з використанням сучасних інформаційних технологій, а також здійснено криміналістичну характеристику зазначених протиправних діянь [111];

– «Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій» (навчальний посібник, 2002 рік, за загальною редакцією Р. А. Калюжного), у розділі 4 якого здійснено кримінолого-криміналістичну характеристику «комп'ютерних злочинів». Розділи 5 і 6 присвячено особливостям методики виявлення та розслідування «комп'ютерних злочинів», а розділ 11 висвітлює особливості проведення слідчих дій на початковому й подальшому етапах розслідування зазначених кримінальних правопорушень [54];

– «Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій» (науково-практичний посібник, 2004 рік, за загальною редакцією професора Я. Ю. Кондратьєва), у якому розглянуто проблемні питання боротьби зі злочинами у сфері використанням ЕОМ (комп'ютерів), а також проаналізовано іноземний досвід боротьби із зазначеними кримінальними правопорушеннями [40];

– «Криміналістична тактика і методика розслідування окремих видів злочинів» (навчальний посібник, 2007 рік), що містить розділ «Особливості методики розслідування злочинів у сфері високих технологій», присвячений класифікації та криміналістичній характеристиці злочинів у сфері високих

технологій, а також визначено правові засади й особливості методики розслідування цих злочинів [18];

– «Керівництво з розслідування злочинів» (науково-практичний посібник, 2009 рік, за редакцією В. Ю. Шепітька). Розділ «Розслідування злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» розглянуто криміналістичну характеристику, типові слідчі ситуації та особливості тактики проведення окремих слідчих (розшукових) дій у зазначених кримінальних правопорушеннях [86];

– «Розслідування комп'ютерних злочинів» (навчально-практичний посібник, 2010), у якому вчені М. Г. Щербаковський та Д. В. Пашнєв спрямували увагу на криміналістичну характеристику комп'ютерних злочинів, особливості використання спеціальних знань під час розслідування зазначеної категорії кримінальних правопорушень, міжнародній взаємодії у боротьбі з комп'ютерними кримінальними правопорушеннями [255].

Аналіз перерахованих досліджень став вагомим теоретичним підґрунтям для вдосконалення сучасної методики розслідування кримінальних правопорушень, що вчиняють з використанням інформаційних комп'ютерних технологій.

Підсумовуючи результати розгляду цього періоду, слід зазначити, що в юридичній літературі початку XXI ст. поступово поняття «комп'ютерна злочинність» стали витісняти поняття «злочини у сфері ЕОМ», «інформаційний злочин», «кіберзлочин», «злочини, що вчинені у кіберпросторі», «злочин у сфері інформаційних технологій» тощо. З цього приводу слушно зазначає П. Д. Біленчук, що у зв'язку з розвитком комп'ютерних технологій відбувається і трансформація понятійного апарату.

Зазначене супроводжується такими факторами:

1) прийняттям Конвенції про кіберзлочинність [99], яка запроваджує нове поняття «кіберзлочин», однак не пропонує його визначення;

2) розвитком і вдосконаленням комп'ютерних пристроїв (смартфонів, планшетів тощо), що зумовило зміну поняття «комп'ютерний злочин», оскільки

такі кримінальні правопорушення почали вчиняти не тільки з використанням персонального комп'ютера.

Проаналізуймо третю групу наукових праць. Дисертаційне дослідження «Розслідування шахрайств, учинених із використанням мережі Інтернет» здійснив 2014 року С. В. Самойлов. Учений запропонував класифікацію способів вчинення шахрайств, учинених із використанням мережі Інтернет, а також розглянув процес слідоутворення як невід'ємну частину цих кримінальних правопорушень [221].

Праця Б. Б. Теплицького «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (2021) є першим комплексним дослідженням із цієї тематики. У роботі проаналізовано іноземний досвід технічного забезпечення протидії кіберзлочинам, на підставі чого сформовано пропозиції щодо розвитку правового регулювання вітчизняного науково-технічного забезпечення кібербезпеки. Увагу спрямовано на використання чинника раптовості під час проведення обшуку та оптимізацію переліку питань для операторів ЕОМ, програмістів, відповідальних осіб за інформаційну безпеку, адміністраторів і співробітників, які здійснюють технічне обслуговування обчислювальної техніки [234].

Виокремимо роботу Т. В. Коршикової «Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки», у якій здійснено криміналістичну характеристику розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки, що охоплює: предмет і способи, слідову картину й обстановку, особу злочинця і особу потерпілого. Увагу зосереджено на основних напрямах розслідування таких протиправних діянь, що надають можливість встановити IP-адреси електронно-обчислювальної техніки, їх місцезнаходження та винних осіб [105].

Слід виокремити також праці вітчизняних учених-криміналістів, серед яких: О. А. Самойленко «Основи методики розслідування злочинів, вчинених у кіберпросторі» (2020), у якій у контексті специфіки кіберпростору як обстановки вчинення кримінального правопорушення досліджено криміналістичну

класифікацію кримінальних правопорушень, вчинених у кіберпросторі, розглянуто їх криміналістичну характеристику, організацію розслідування та використання спеціальних знань у розслідуванні зазначених кримінальних правопорушень [217].

Питання методики розслідування кримінальних правопорушень цієї категорії також висвітлено в окремих розділах навчальних і науково-практичних посібників:

– «Актуальні проблеми розслідування кіберзлочинів» (2018) Н. М. Ахтирської. У навчальному посібнику розглянуто основні напрями розвитку інформаційних технологій, проаналізовано міжнародне законодавство й міжнародні зобов'язання України щодо боротьби з кіберзлочинністю, а також дослідження електронних доказів під час розслідування кіберзлочинів [12];

– «Протидія злочинам у сфері використання інформаційних технологій» (2019 рік, за редакцією М. В. Карчевського), де здійснено криміналістичну характеристику злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також особливості початкового етапу розслідування, типові слідчі ситуації та версії, проведення окремих слідчих (розшукових) дій у зазначених кримінальних правопорушеннях [202];

– «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» (2019 рік, авторський колектив: Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов та ін.). У науково-практичному посібнику увагу спрямовано на кримінально-правову характеристику кримінальних правопорушень, передбачених розділом XVI КК України, а також взаємодію слідчого та спеціаліста в кримінальних провадженнях зазначеної категорії кримінальних правопорушень [122].

Також, окремі питання розслідування даних протиправних діянь досліджувалися і нами [140-158].

Підсумовуючи, зауважимо, що засоби інформаційних технологій постійно змінюються та вдосконалюються, і це зумовлює появу нових видів кримінальних правопорушень, які вчиняють з використанням інформаційних комп'ютерних

технологій. Своєю чергою наукова спільнота має здійснювати ретельне дослідження зазначених протиправних діянь і розробляти комплексні сучасні методики розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій.

1.2. Криміналістична класифікація кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Останніми роками види кіберзагроз постійно змінюються. Якщо в минулому столітті «комп'ютерні злочинці» вчиняли свої дії заради того, щоб «розважитися», то нині такі дії становлять істотну загрозу для суспільства, оскільки наслідки від їхніх протиправних дій можуть бути фатальними. Це своєю чергою пов'язано з удосконаленням інформаційних технологій, які є рушієм не тільки світового прогресу, а й злочинної діяльності, що надає можливість злочинцям використовувати здобутки сучасного цифрового суспільства зі злочинною метою. Тому вагомий науковий інтерес, з криміналістичної точки зору, становлять інформаційні технології.

Стисло схарактеризуємо поняття «інформація» і «технологія».

Термін «інформація» походить від латинського *informatio*, що означає роз'яснення, відомості, виклади [78, с. 15].

Закон України «Про інформацію» тлумачить інформацію як будь-які відомості (або дані), що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [189].

Технологією вважають сукупність відомостей та знань про послідовність певних виробничих операцій у процесі виробництва чого-небудь; сукупність способів обробки чи переробки матеріалів, виготовлення виробів, проведення різних виробничих операцій тощо [29, с. 1245].

Перша згадка про «інформаційні технології» з'явилася в журналі «Harvard Business Review» 1958 року. Попри те, що ця стаття була присвячена проблемам

менеджменту в майбутньому, її автори Г. Дж. Левіт (H. J. Leavitt) і Т. Л. Фішер (T. L. Whisher) розповідають про технологію, що цілком змінить середній та великий бізнес. Оскільки єдиної установленої назви цій технології на той час не було, дослідники сформулювали поняття «інформаційна технологія» [291].

Вітчизняним автором цього поняття вважають В.М. Глушкова. Учений тлумачив поняття «інформаційні технології» як значну кількість процесів, що пов'язані насамперед з обробкою інформації [161].

У науковій літературі є різні підходи до визначення поняття «інформаційні технології», серед яких: науковий, суспільно-економічний, операційний, антропологічний, педагогічний [81, с. 9–11].

Згідно із Законом України «Про національну програму інформатизації», інформаційними технологіями вважають сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, розосередження даних, швидкий пошук інформації, доступ до джерел інформації незалежно від місця їх розташування [190].

Водночас Державний стандарт ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення» поняття «інформаційні технології» визначає як технологічний процес, предметом перероблення й результатом якого є інформація.

Досліджуючи вітчизняну наукову літературу та нормативно-правові акти України, зауважимо про використання схожих понять: «сучасні інформаційні технології», «інформаційно-комунікаційні технології», «інформаційно-телекомунікаційні технології» тощо.

Наприклад, у ст. 156-1, 301-1, 301-2 КК України [119] застосовано поняття «з використанням інформаційно-телекомунікаційних систем або технологій». Однак законодавець не пропонує тлумачення цього терміна.

З цього приводу доречно зазначає К. В. Юдкова, що саме через відсутність єдиної системи термінологічного апарату виникають ситуації, коли нормативно-правові акти не відповідають складності й багатоаспектності тих реальних процесів і явищ, поява та існування яких має істотний вплив на розвиток суспільства [261, с. 63–67].

Переважна більшість науковців [5; 201, с. 267; 236, с. 356] тлумачить поняття «інформаційні технології» як загальний термін, що використовують для посилань на всі технології, пов'язані зі створенням, обробкою, зберіганням, використанням, пересиланням і керуванням інформацією в різних її видах.

У межах нашого дослідження будемо розглядати лише ті інформаційні технології, що працюють з інформацією в цифровому вигляді в комп'ютері, де є поєднання програмних засобів (software) та обраного комплексу апаратних засобів (hardware).

Вважаємо за доцільне використовувати термін «інформаційні комп'ютерні технології», аби акцентувати, що під час вчинення зазначених кримінальних правопорушень знаряддям є комп'ютер (смартфон, планшет, ноутбук тощо).

Згідно з визначенням Великого тлумачного словника української мови, комп'ютер – це електронна обчислювальна машина [29, с. 446].

Відповідно до дефініції, яку пропонує Оксфордський словник, комп'ютером слід вважати електронну машину, що може зберігати, систематизувати та знаходити інформацію, виконувати процеси з числами й даними, а також керувати іншими машинами [301].

Тобто комп'ютер є складним технічним пристроєм, що містить апаратні та програмні засоби. Апаратні – це різні пристрої, механізми й елементи (центральний процесор, відеокарта, вінчестер, мікроконтролер, мишка тощо); програмні – програмне забезпечення (операційна система (Windows, Linux тощо), драйвери, файлові менеджери тощо).

Загалом комп'ютер за використанням можна класифікувати на:

– інтернет речей (вбудовані комп'ютери), що є в мікрохвильових печах, пральних машинах, принтерах, автомобілях, літаках, кораблях, розумних колонках, годинниках і будинках тощо;

– персональні мобільні пристрої (мобільні телефони, планшети тощо);

– настільні комп'ютери (нетбуки, ноутбуки, персональні комп'ютери тощо);

– сервери, суперкомп'ютери, комп'ютерні кластери.

Саме з виникненням і розвитком персональних комп'ютерів починає з'являтися таке криміногенне явище, як «комп'ютерний злочин» *(computer crime)*. Надалі це визначення трансформувалося в поняття кіберзлочин. Однак у юридичній літературі не сформовано єдиного підходу стосовно того, який термін необхідно застосовувати: «кіберзлочин», «комп'ютерний злочин», «інформаційний злочин», «злочини у сфері інформаційних технологій» тощо.

З цього приводу слушно зазначають вітчизняні науковці, що визначення нової групи кримінальних правопорушень завжди слід здійснювати на підставі ознак, що характеризують об'єкт посягання. З кримінально-правової позиції, вважає М. В. Карчевський, доречніше використовувати термін «кримінальні правопорушення у сфері використання інформаційних технологій», що охоплюють ст. 361–363-1 КК України (розділ XVI КК України) [202, с. 19–20]. Натомість з криміналістичної позиції інформаційні комп'ютерні технології є предметом, знаряддям або засобом вчинення кримінального правопорушення, що має значення для методики розслідування кримінальних правопорушень [85, с. 36]. Тому під час проведення криміналістичних досліджень слід використовувати поняття «комп'ютерний злочин» або «кіберзлочин» [202, с. 20].

Термін «кіберзлочин» є сполученням слів «кібернетика» – наука про загальні закономірності процесів керування та зв'язку в організованих системах (машини, живі організми, суспільні формування тощо), головною частиною кібернетики є теорія інформації, яка вивчає процес передачі інформації та різні способи її кодифікації [228, с. 158], і «злочин».

Оксфордський тлумачний словник префікс *cyber* визначає як компонент складного слова, що стосується інформаційних технологій, мережі Інтернет, віртуальної реальності. Схоже визначення пропонує і Кембриджський словник. Отже, *cybercrime* – це злочинність, пов'язана з використанням комп'ютерно-інформаційних технологій. Водночас термін *computer crime* переважно стосується кримінальних правопорушень, що вчиняють проти комп'ютерів або комп'ютерних даних [203, с. 41–42].

Ми поділяємо думку іноземних науковців, що в кінці XX ст. слово «кібер» *(cyber)* стали активно використовувати в літературі як синонім майже всіх понять, що пов'язані з комп'ютерами й Інтернетом (наприклад, кіберпростір, кібершопінг, кіберсерфінг тощо) [302, с. 380–381].

Слід зазначити, що термін «кіберзлочин» уперше застосували іноземні науковці *Sussman* та *Heuston* 1995 року [317, с. 477].

Це поняття стали активно використовувати після підписання державами – членами Ради Європи й іншими державами 2001 року Конвенції про кіберзлочинність, яка ратифікована Україною 7 вересня 2005 року [99].

Своєю чергою українські науковці по-різному трактують поняття «кіберзлочин».

Зокрема, М. А. Погорецький та В. П. Шеломенцев розглядають поняття «кіберзлочин» у широкому та вузькому значеннях. У широкому значенні кіберзлочини – це кримінальні посягання, що відбуваються в кіберпросторі, об'єктом посягання яких є суспільні відносини в різних сферах життєдіяльності людини, пов'язані з використанням ресурсів кіберпростору. У вузькому значенні кіберзлочини слід трактувати як кримінальні посягання з використанням кіберпростору на певні процеси, що пов'язані з використанням комп'ютерних систем [169, с. 92].

Цілком слушним видається визначення, запропоноване Н. М. Ахтирською, яка кіберзлочином вважає кримінальні правопорушення, що вчиняють з використанням комп'ютерної техніки (комп'ютерів, пристроїв й іншого обладнання), комп'ютерних систем і мереж з порушенням встановленого законом порядку інформаційної безпеки, незалежно від предмета посягання та сфери застосування [12, с. 12].

Також учена цілком доречно виокремлює особливості вчинення кіберзлочинів (характерні ознаки), до яких належать: віртуальний простір вчинення (кіберпростір), наслідки можуть бути як віртуальні, так і реальні (матеріальні й моральні), віддаленість місця настання наслідків від місця безпосереднього вчинення протиправних дій, транснаціональний характер

злочинних дій, ускладнена процедура ідентифікації особи, цифровий (комп'ютерний) характер слідчої інформації, шкідливий програмний продукт як засіб вчинення кримінального правопорушення, диференційована мета (залежно від суб'єкта та ситуації), різний предмет посягання (інформація, власність, мораль, безпека тощо), значні розміри завданої шкоди [12, с. 14].

Кіберпростором слід вважати інформаційний (віртуальний) простір, який виникає (існує) за допомогою інформаційних комп'ютерних технологій. Кіберпростір розглядають як: 1) локальне середовище (коли інформаційно-комп'ютерну технологію не під'єднано до мережі); 2) локальну мережу; 3) глобальну мережу передачі даних (Інтернет), коли інформаційно-комп'ютерні технології підключено до цих мереж [129, с. 216–217].

У національному законодавстві визначення поняття «кіберзлочин» міститься в Законі України «Про основні засади забезпечення кібербезпеки України» [193], де в п. 8 ч. 1 ст. 1 зазначено, що кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнане злочином міжнародними договорами України.

Слід зауважити, що в цьому Законі після терміна «кіберзлочин» у дужках зазначено «комп'ютерний злочин». Цей Закон було прийнято відповідно до зауважень науково-експертного та юридичного управлінь Апарату Верховної Ради України, які не заперечують можливості впровадження нової термінології в національне правове поле. Проте її слід уводити комплексно й узгоджувати з чинним законодавством. Зокрема, акцентовано на необхідності встановлення співвідношення між поняттями «комп'ютерні злочини» і «кіберзлочини». Також поняття «кіберзлочин» має бути узгоджено з термінологією КК України, що має окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а також з іншими законодавчими актами, у яких використано термін «комп'ютерний злочин» [194].

Отже, можна дійти висновку, що, використовуючи конструкцію «кіберзлочин (комп'ютерний злочин)», законодавець з метою уникнення колізії під час застосування на національному рівні цих термінів узгоджує їх. Однак це не означає, що за змістом такі поняття тотожні [140, с. 54].

Не можна оминути увагою висловлені в науковій літературі думки вчених стосовно використання поняття «кіберправопорушення» [15; 133; 235]. Зокрема, Р. В. Бараненко зауважує, що з появою інституту кримінальних проступків у національному кримінальному законодавстві термін «кіберзлочин» і «комп'ютерний злочин» мають втратити свою актуальність. Науковець пропонує замість цих понять використовувати термін «кіберправопорушення» і внести відповідні термінологічні зміни в національне законодавство України [15, с. 88].

На нашу думку, використання запропонованого поняття «кіберправопорушення» є широким за змістом і може охоплювати діяння, що належать до адміністративних правопорушень. Тому для того, щоб акцентувати увагу саме на кіберправопорушеннях як кримінально караних діяннях, необхідно використовувати термін «кримінальні кіберправопорушення», що охоплює кіберзлочини, а також кримінальні кіберпроступки (згідно з положеннями КК України).

Однак не слід нехтувати й поняттям «кіберзлочин». У Конвенції про кіберзлочинність («*The Convention on Cybercrime*») використано поняття *cybercrime*, отже, термін «кіберзлочин» відповідає міжнародним стандартам, а також цей термін активно використовують у міжнародній практиці.

Українські вчені у своїх дослідженнях нерідко використовують поняття «кіберзлочин».

З цього приводу цілком слушною є думка О. А. Самойленко, яка стверджує, що, використовуючи дефініцію «кіберзлочин», вітчизняні науковці звужують зміст кримінального правопорушення, вчиненого в кіберпросторі, оскільки класифікують кіберзлочини на підставі позицій визначеної в Конвенції або криміналістично значущої ознаки – способу вчинення суто «комп'ютерного

злочину», що спричиняє неповноту розроблених методик розслідування [217, с. 58].

Необхідно зауважити, що методика розслідування окремих кримінальних правопорушень (або криміналістична методика) – це система наукових положень і рекомендацій щодо організації та здійснення розслідування та запобігання окремим видам кримінальних правопорушень. У структурі криміналістичної методики розрізняють дві частини – загальні положення та окремі методики. Остання своєю чергою слугує комплексом порад типізованого характеру, що є найефективнішим під час розслідування певного виду (роду) кримінального правопорушення. Об'єктом дослідження криміналістичної методики є різні кримінальні правопорушення. Саме для ефективного пізнання цього об'єкта та створення відповідних рекомендацій розробляють криміналістичну класифікацію кримінальних правопорушень [114, с. 3–4].

Доречно стверджує В. О. Пчеліна, що криміналістична класифікація кримінальних правопорушень є методом пізнання, який полягає в систематизації кримінальних правопорушень за криміналістично значущими ознаками відповідно до законів логіки задля вдосконалення теоретичних основ і розроблення нових криміналістичних методик з метою задоволення потреб слідчої практики [204, с. 308].

У криміналістичній літературі немає єдиного підходу стосовно того, які критерії використовувати під час розгляду криміналістичної класифікації: кримінально-правові, криміналістичні чи змішані (кримінально-правові та криміналістичні).

З огляду на сучасні дослідження, більшість вітчизняних учених-криміналістів схиляються до думки, що для криміналістичної класифікації кримінальних правопорушень слід застосовувати саме кримінально-правові та криміналістичні критерії [59, с. 37–38; 204; 244, с. 102–103; 260, с. 344].

Кримінально-правовий критерій визначає нормативну суть класифікації, передбаченої законом, а криміналістичний враховує чинники, пов'язані зі специфікою виявлення та розкриття різних видів кримінальних правопорушень

залежно від особливостей предмета посягання, обстановки приготування, вчинення та приховування, механізму і способів, типології особи злочинця, мети й мотивації злочинних дій тощо [116, с. 143].

Розробляючи криміналістичну класифікацію кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, на нашу думку, слід застосовувати як кримінально-правові, так і криміналістичні критерії.

Розглядаючи криміналістичну класифікацію кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, доцільно застосовувати кримінально-правові критерії класифікації, запропоновані Г. А. Матусовським, на прикладі криміналістичної класифікації економічних кримінальних правопорушень як систему їхніх груп і видів, передбачених відповідними нормами КК України, що розподілені за сферами суспільних відносин [132, с. 42–43].

За кримінально-правовими критеріями зазначені кримінальні правопорушення можна поділяти на такі групи:

1) злочини у сфері основ національної безпеки України, що вчиняються з використанням інформаційних комп'ютерних технологій: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109); посягання на територіальну цілісність і недоторканність України (ст. 110); фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110-2); державна зрада (ст. 111); колабораційна діяльність (ч. 1, 3, 6, ст. 111-1); пособництво державі-агресору (ст. 111-2); диверсія (ст. 113); шпигунство (ст. 114); несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114-2);

2) кримінальні правопорушення у сфері охорони життя та здоров'я, що вчиняються з використанням інформаційних комп'ютерних технологій: доведення до самогубства (ст. 120); домашнє насильство (ст. 126-1); погроза вбивством (ст. 129); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132); незаконне розголошення лікарської таємниці (ст. 145);

3) кримінальні правопорушення у сфері волі, честі та гідності особи, що вчиняються з використанням інформаційних комп'ютерних технологій: вербування людини з метою експлуатації (ст. 149);

4) кримінальні правопорушення у сфері статевої свободи чи статевої недоторканості, що вчинені з використанням інформаційних комп'ютерних технологій: розбещення неповнолітніх (ст. 156); домагання дитини для сексуальних цілей (ст. 156-1);

5) кримінальні правопорушення у сфері виборчих, трудових та інших особистих прав і свобод людини й громадянина, що вчиняються з використанням інформаційних комп'ютерних технологій, насамперед передбачені: ст. 157; ч. 1 ст. 158; ст. 158-1; ст. 159–161; ст. 163, 168, 174, 176, 182–184;

6) кримінальні правопорушення у сфері власності, що вчиняються з використанням інформаційних комп'ютерних технологій: ст. 185; ч. 1, 2, 4 ст. 189, 190–192, 195, 198;

7) кримінальні правопорушення у сфері господарської діяльності, що вчиняються з використанням інформаційних комп'ютерних технологій: ст. 200, 201-2, 203-2, 206, 209, 222-1, 229, 231, 232;

8) кримінальні правопорушення у сфері громадської безпеки, що вчиняються з використанням інформаційних комп'ютерних технологій, передусім: терористичний акт (ст. 258); втягнення у вчинення терористичного акту (ст. 258-1); публічні заклики до вчинення терористичного акту (ст. 258-2); створення терористичної групи чи терористичної організації (ст. 258-3); сприяння вчиненню терористичного акту (ст. 258-4); фінансування тероризму (ст. 258-5), а також завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи

пошкодження об’єктів власності (ст. 259); незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (у частині збуту) (ст. 263); погроза вчинити викрадання або використати радіоактивні матеріали (ст. 266);

9) кримінальні правопорушення у сфері громадського порядку та моральності, що вчиняються з використанням інформаційних комп’ютерних технологій, зокрема: заклики до вчинення дій, що загрожують громадському порядку (ст. 295); виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300); а також ст. 301, 301-1, 301-2, 303, 304;

10) кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, що вчиняються з використанням інформаційних комп’ютерних технологій, передбачені ст. 306, 307, 311–313, 315, 323 та 324;

11) кримінальні правопорушення у сфері охорони державної таємниці, що вчиняються з використанням інформаційних комп’ютерних технологій: розголошення державної таємниці (ст. 328); передача або збирання відомостей, що становлять службову інформацію, зібрану в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330);

12) кримінальні правопорушення у сфері авторитету органів державної влади, органів місцевого самоврядування, об’єднань громадян і журналістів, що вчиняються з використанням інформаційних комп’ютерних технологій: погроза щодо працівника правоохоронного органу (ст. 345); погроза щодо журналіста (ст. 345-1); погроза щодо державного чи громадського діяча (ст. 346); погроза щодо службової особи чи громадянина, який виконує громадський обов’язок (ст. 350); незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359);

13) кримінальні правопорушення у сфері правосуддя, що вчиняються з використанням інформаційних комп’ютерних технологій, а саме: втручання в діяльність судових органів (ст. 376); незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя (ст. 376-1);

погроза щодо судді, народного засідателя чи присяжного (ст. 377); розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381); розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387); погроза щодо захисника чи представника особи (ст. 398);

14) кримінальні правопорушення у сфері військової служби, що вчиняються з використанням інформаційних комп'ютерних технологій: погроза щодо начальника (ст. 405), а також ст. 410, 422, 435-1;

15) кримінальні правопорушення у сфері безпеки людства, міжнародного порядку та миру, що вчиняються з використанням інформаційних комп'ютерних технологій, а саме: пропаганда війни (ст. 436); виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436-1); виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436-2).

З приводу кримінальних правопорушень, передбачених розділом XVI КК України, слушно зазначає О. А. Самойленко, що такі кримінальні правопорушення є особливими, через те, що можуть поєднуватися з іншими кримінальними правопорушеннями [217, с. 66].

Оскільки з криміналістичної позиції доцільно використовувати термін «кримінальні кіберправопорушення», на нашу думку, у криміналістичних дослідженнях можна також уживати замість «кримінальні правопорушення, що вчиняються з використанням комп'ютерно-інформаційних технологій», поняття «кримінальні кіберправопорушення» чи «кіберзлочини». Наприклад, кримінальні кіберправопорушення у сфері громадської безпеки; кримінальні кіберправопорушення у сфері власності; кіберзлочини проти основ національної безпеки (якщо це тільки злочини, передбачені КК України).

З огляду на це, у нашому дисертаційному дослідженні поняття «кримінальні кіберправопорушення» використано як синонім до кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

У межах криміналістичної класифікації кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, ураховуючи відмітні ознаки даних протиправних діянь (вчиняють у кіберпросторі, мають транснаціональний характер тощо), можна виокремити такі криміналістичні критерії: особа злочинця, мотив і мета, особа потерпілого, наслідки тощо.

Класифікація кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій за особою злочинця, має враховувати такі особливості: кількість осіб, вік, місце роботи, зв'язок із жертвою, наявність в особи відповідних навичок і вмінь поводитися з комп'ютерною технікою.

Залежно від складності вчинення зазначених протиправних діянь їх можуть вчиняти *одноосібно* або *групою осіб*. Наприклад, шпіонаж чи диверсія, що вчиняються з використанням інформаційних комп'ютерних технологій, потребують застосування вмінь і навичок ширшого кола людей, натомість домашнє насильство здебільшого вчиняють одноосібно.

За віком розмежовують малолітніх, неповнолітніх і повнолітніх. Слід зазначити, що цей критерій має здебільшого кримінальний, кримінологічний та кримінально-процесуальний характер.

За місцем роботи можна виокремити тих осіб, які безпосередньо працюють у сфері, що дає змогу застосовувати вміння та навички в злочинній діяльності (програмісти, фахівці у сфері кібербезпеки, IT-спеціалісти), і тих, хто працює у сферах, не пов'язаних з інформаційними технологіями.

За зв'язком «злочинець–жертва»: 1) тих, які безпосередньо знають потерпілого; 2) тих, які не знали потерпілого; 3) тих, хто обрав жертву з певних джерел (медіа, баз даних тощо);

Наявність в особи відповідних *навичок і вмінь* передбачає, що особа могла набути такі навички самостійно, у зв'язку із професійною діяльністю або здобула їх у процесі навчання у відповідному закладі освіти.

Класифікуючи кримінальні кіберправопорушення за *мотивом*, О. А. Самойленко залежно від мотиву пропонує виокремлювати: 1) корисливий

мотив, що пов'язаний з фінансово-економічною сферою відносин; 2) соціально-економічний мотив, що пов'язаний із соціальною сферою відносин суб'єктів; 3) антидержавно-політичний мотив, пов'язаний з державно-політичною сферою; 4) ідейний мотив, пов'язаний зі світоглядною сферою життя [217, с. 64–66].

Потерпілих осіб поділяють: 1) за віком: малолітні, неповнолітні, повнолітні; 2) за статусом: фізичні особи, юридичні особи, держава.

Наслідки вчинення можна поділити на: 1) матеріальні: фізичні та майнові; 2) нематеріальні: неперсоніфіковані (політичні, управлінські, морально-психологічні, культурно-історичні, соціально-безпекові); персоніфіковані (честь, гідність); комбіновані [118, с. 107–108].

Слід зазначити, що наведена криміналістична класифікація кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, не є вичерпною.

Своєю чергою кожен із запропонованих кримінально-правових і криміналістичних критеріїв криміналістичної класифікації може слугувати подальшим окремим дослідженням, що сприятиме розробленню нових методик розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Отже, дослідження криміналістичної класифікації зазначених кримінальних правопорушень має важливе науково-теоретичне та практичне значення, що виявляється у формуванні криміналістичних основ для подальшого дослідження та розроблення методики розслідування, що стануть рекомендаціями для ефективного проведення розслідування таких протиправних діянь.

1.3. Міжнародно-правові засади та зарубіжний досвід розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Вивчення іноземного досвіду розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, має

важливу практичну роль для ефективного проведення досудового розслідування, встановлення винних осіб і притягнення їх до кримінальної відповідальності.

Оскільки кіберзлочинність має транснаціональний характер (тобто злочинець може перебувати в одній країні, а вчиняти свої злочинні дії в іншій), необхідно тісно співпрацювати з іншими державами, а також досліджувати й використовувати їх ефективний досвід у боротьбі із цими протиправними виявами.

Важливими міжнародними нормативними актами у сфері боротьби та протидії кримінальним правопорушенням, зокрема й кримінальним кіберправопорушенням, є: 1) Європейська конвенція про взаємну допомогу у кримінальних справах (Страсбург, 20 квітня 1959 року) [71]; 2) Декларація ООН про злочинність і суспільну небезпеку (12 грудня 1996 року) [62]; 3) Конвенція ООН проти транснаціональної організованої злочинності (Палермо, 12 грудня 2000 року) [98]; 4) Конвенція про кіберзлочинність (Будапешт, 23 листопада 2001 року) [99].

Вагомим кроком міжнародної спільноти в боротьбі з кіберзлочинністю стало підписання членами Ради Європи й іншими державами 2001 року Конвенції про кіберзлочинність [99], яка ратифікована Україною 2005 року [196]. Згодом, 2006 року, підписано Додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [67].

Слід зазначити, що в Конвенції про кіберзлочинність [99] виокремлено чотири групи таких протиправних діянь.

Першу групу кіберзлочинів становлять правопорушення проти конфіденційності, доступності й цілісності комп'ютерних даних і систем: 1) незаконний доступ – доступ до комп'ютерної системи без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою (ст. 2); 2) нелегальне перехоплення – протиправне перехоплення технічними засобами комп'ютерних даних (ст. 3); 3) втручання в дані – навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації (ст. 4); 4) втручання в систему – перешкоджання функціонуванню комп'ютерної системи

шляхом введення, передачі, пошкодження, знищення, погіршення, зміни або приховування комп'ютерних даних (ст. 5); 5) зловживання пристроями – навмисне без права на це їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином (ст. 6).

До другої групи належать правопорушення, пов'язані з комп'ютерними даними: 1) підробка, пов'язана з комп'ютерними даними (ст. 7); 2) шахрайство з використанням комп'ютерних даних (ст. 8).

До третьої групи належать правопорушення, що стосуються змісту: 1) дії, пов'язані з дитячою порнографією, – вироблення, пропонування або надання, розповсюдження або передача, здобуття, володіння (ст. 9);

Четверту групу формують правопорушення щодо порушення авторських і суміжних прав (ст. 10).

Також згідно з Додатковим протоколом додано ще одну групу – акти расизму та ксенофобії, вчинені з використанням комп'ютерних мереж (ст. 3) [67].

З плином часу постала необхідність покращити міжнародне співробітництво між державами у сфері надання електронних доказів. Тому 2021 року Комітет міністрів Ради Європи прийняв Другий додатковий протокол до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів [310].

Міжнародне співробітництво необхідно тлумачити як сукупність міжнародно-правових принципів і норм, які встановлюють порядок взаємодії держав, компетентних органів, посадових осіб, громадян й осіб без громадянства під час кримінального провадження шляхом надання міжнародної правової допомоги, а також відносин з міжнародними інституціями [13, с. 20].

У Другому додатковому протоколі [310] зазначено, що поштовхом для його створення слугувало:

– зростання рівня кіберзлочинності у сфері інформаційно-комунікаційних технологій та інтернеті, що ставить під загрозу демократію, верховенство права та права людини;

– збільшення кількості жертв кіберзлочинів;

– необхідність держави нести відповідальність за захист осіб не тільки офлайн, а й онлайн, зокрема шляхом здійснення ефективного досудового розслідування та судового розгляду;

– докази кримінального правопорушення зберігаються в електронній формі в комп'ютерних системах, які знаходяться в юрисдикції іноземних держав.

Характеризуючи Другий додатковий протокол, Н. М. Ахтирська слушно акцентує на його певних особливостях, а також вплине на процес розслідування. Насамперед: 1) відбувається розширення міжнародного співробітництва та збору електронних доказів у кримінальному провадженні, що своєю чергою значно розширить можливості використання способів співробітництва не тільки конвенційних кіберзлочинів, а й інших кримінальних правопорушень; 2) не може бути відмовою в міжнародному співробітництві у разі відсутності такого складу кримінального правопорушення в законодавстві запитуваної держави або у зв'язку з іншим термінологічним визначенням чи віднесення до іншої категорії тяжкості; 3) розширюються можливості отримання інформації від постачальників послуг, що перебувають на території іншої держави [14].

У цьому Протоколі [310] розглянуто можливість отримання показань у режимі відеоконференції (ст. 11) та створення спільних слідчих груп для спільного розслідування (ст. 12).

Зокрема, у разі необхідності проведення допиту в режимі відеоконференції, запитуюча і запитувана Сторони проводять консультації для вирішення питань, що можуть виникнути у зв'язку з виконанням запиту, а саме: яка зі Сторін головує; особи, які повинні бути присутні; порядок проведення допиту; яка зі Сторін буде надавати переклад тощо.

Процедура й умови, що регулюють роботу спільних слідчих груп, повинні враховувати функції, тривалість і періоди подовження, організацію, умови отримання, передачі й використання інформації чи доказів, умови конфіденційності та умови участі Сторін у проведенні слідчих дій тощо.

Отже, підписання та ратифікація Другого додаткового протоколу [310] до Конвенції про кіберзлочинність [99] та внесення відповідних змін у кримінальне

процесуальне законодавство є не тільки необхідним кроком нашої держави для здійснення ефективного міжнародного співробітництва під час розслідування кримінальних правопорушень, зокрема й кримінальних кіберправопорушень, а також покладає обов'язок на вітчизняних науковців проводити дослідження та розробляти відповідні криміналістичні рекомендації з огляду на особливості Другого додаткового протоколу.

Жодна країна не може самостійно протистояти кіберзлочинності, тому постає потреба в тісній міжнародній співпраці з іншими державами у сфері розслідування.

За даними звіту Федерального бюро розслідувань, загальна сума матеріальних збитків у Сполучених Штатах Америки від кіберзлочинності лише за 2021 рік сягає 6,9 млрд доларів, що на 64 % більше, порівняно з 2020 роком. У зазначеному звіті обліковано і значну кількість скарг – 847 376 імовірних випадків вчинення кіберзлочинів. Тому питання ефективного розслідування кіберзлочинів, що проводить кібервідділ Федерального бюро розслідувань США, є надзвичайно важливим [283].

Серед країн Європейського Союзу привертає увагу ФРН, у якій, згідно зі статистичними даними, 2021 року було зареєстровано 146 363 кіберзлочинів, а також комп'ютерного шахрайства (оскільки його обліковують окремо від кіберзлочинів) – 113 002 [303].

Розслідування кіберзлочинів у ФРН здійснюють поліцейські земель Німеччини. Якщо кіберзлочин вчинено проти федерального органу чи об'єкта або частини об'єкта критичної інфраструктури, тоді розслідування проводить Відділ кіберзлочинності Федерального управління кримінальної поліції Німеччини, відповідно до закону ФРН «Про Федеральне управління кримінальної поліції» (*Bundeskriminalamtgesetz – BKAG*) [284].

Головною функцією цього Відділу є: 1) розслідування діяльності осіб у кіберпросторі, ліквідація злочинних структур; 2) забезпечення збору, обробки й аналізу відповідної інформації для розслідування; 3) консультування керівництва Федерального управління кримінальної поліції Німеччини у сфері кримінальної політики, пов'язаної з кіберзлочинністю [279].

Облік кіберзлочинів у кожній країні здійснюють на підставі національного кримінального законодавства. З огляду на це, різняться і статистичні дані країн щодо вчинення, реєстрації, обліку кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Наприклад, порівняно з ФРН, у Франції за 2021 рік було зафіксовано 47 560 кіберзлочинів, що на 6,9 % більше, ніж 2020 року [292].

Розслідування кіберзлочинів у Франції здійснює Відділ по боротьбі з кіберзлочинами, що входить у Центральне управління судової поліції. Структурними підрозділами Відділу є: центральний офіс боротьби з кіберзлочинами, група цифрових доказів, група прогнозування та аналізу, а також офіс стратегічної координації [305]. Інші правоохоронні органи Франції також можуть проводити розслідування кіберзлочинів залежно від виду кримінального правопорушення, що вчинене з використанням комп'ютерних технологій, зокрема:

1) Національна поліція або Національна служба жандармерії – кіберзлочини проти неповнолітніх, крадіжка особистих даних, шахрайство з платіжними картками, фішинг тощо);

2) Відділ боротьби з кіберзлочинністю – хакерські атаки, шахрайство, що стосується способу оплати, телефонне й інтернет-шахрайство;

3) Головне управління внутрішньої розвідки – кримінальні правопорушення, що спрямовані проти державних установ і мереж, а також критичної інфраструктури [315].

На відміну від Франції, статистичні дані Іспанії стосовно рівня кіберзлочинності суттєво відрізняються. Зокрема, 2021 року в Іспанії було зареєстровано 305 477 кримінальних правопорушень, що належать до категорії кіберзлочинів. Порівняно з 2020 роком, показник кіберзлочинності в Іспанії зріс на 6,1 % [286].

Розслідування кіберзлочинів у цій країні здійснює Центральна бригада технологічних розслідувань, що входить до складу Групи технологічних розслідувань Головного відділення судової поліції Головного управління поліції, функціями якої є: проведення розслідувань кіберзлочинів (інтернет-шахрайства,

кібератак, розповсюдження, збут дитячої порнографії, крадіжка даних тощо), а також здійснення міжнародного співробітництва у сфері кіберзлочинності [266].

Своєю чергою в Туреччині за 2021 рік було відкрито 19 947 кримінальних проваджень, що пов'язані з кіберзлочинністю [264]. Зареєструвати кримінальне правопорушення може прокурор, а також працівники провінційних поліцейських управлінь боротьби з кіберзлочинністю або відділів жандармерії [311, с. 11]

Саме органи прокуратури Республіки Туреччина відіграють вирішальну роль у розслідуванні всіх кримінальних правопорушень, зокрема кіберзлочинів, шляхом проведення розслідування та надання вказівок правоохоронним органам щодо виконання певних процесуальних дій [311, с. 11].

За дорученням прокурора розслідування кіберзлочинів здійснює Департамент боротьби з кіберзлочинністю, що належить до Головного управління безпеки МВС Турецької Республіки. Поміж функцій цього Департаменту слід виокремити: проведення розслідувань кіберзлочинів, а також експертиз електронних пристроїв; збір необхідних доказів щодо події кіберзлочину; здійснення міжнародного співробітництва у сфері боротьби з кіберзлочинністю [312].

Привертають увагу правоохоронні органи Канади, де розслідування кіберзлочинів здійснює Королівська канадська поліція на трьох рівнях:

1) федеральному – кіберзлочини, що пов'язані з національною безпекою Канади, зокрема які стосуються критичної інфраструктури; відмивання коштів, фінансування тероризму; незаконний обіг наркотиків;

2) міжнародному – здійснює співпрацю з міжнародними партнерами щодо швидкого надання чи отримання цифрових доказів;

3) у провінціях і муніципалітетах – розслідування кіберзлочинів, у яких інтернет і комп'ютерні технології є ключовою складовою для вчинення кримінального правопорушення: сексуальна експлуатація дітей в інтернеті, місцеві та регіональні види шахрайства й кібербулінг [309].

Усвідомлюючи небезпечність кіберзагроз для держави, 2021 року Сейм Республіки Польща прийняв закон про створення «Центрального Бюро боротьби з кіберзлочинністю» [321].

Згідно зі ст. 5d закону Республіки Польща «Про поліцію» [320], це Бюро є організаційним підрозділом поліції та відповідає за виконання таких завдань:

1) виявлення, запобігання та боротьба з кримінальними правопорушеннями, що вчинені з використанням ІТ систем, інформаційно-комунікаційних систем чи мереж, а також встановлення та притягнення винних осіб до відповідальності;

2) здійснення діяльності щодо підтримки організаційних підрозділів поліції у виявленні, попередженні та припиненні кіберзлочинів [269].

Відповідно до ст. 311 КПК Польщі, розслідування проводить прокурор. Водночас прокурор може доручити поліції проведення розслідування загалом або виконання окремих дій з розслідування [322].

Для розслідування кіберзлочинів створено спеціальний орган у Сінгапурі. Це Технологічний кримінальний відділ, який належить до складу Департаменту кримінальних розслідувань і складається з трьох відділів: відділ політики щодо технологічних правопорушень, відділ розслідування технологічних правопорушень і відділ судових експертиз технологічних правопорушень [276].

Отже, інші країни гостро реагують на виклики кіберзлочинності, що засвідчує створення спеціальних структурних підрозділів у системі їхніх правоохоронних органів з розслідування або допомоги в розслідуванні цих протиправних діянь. Міжнародне співробітництво між державами має вагоме значення для ефективного розслідування кримінальних правопорушень, що вчиняються з використанням комп’ютерних інформаційних технологій.

Перш ніж перейти до вивчення іноземного досвіду розслідування кіберзлочинів, зауважимо, що поняття «досвід» визначають як сукупність знань, умінь, що здобувають протягом життя та на практиці, а також те, що було в житті, з чим доводилося зустрічатися [29, с. 242].

На нашу думку, іноземний досвід розслідування кримінальних правопорушень, що вчиняються з використанням комп’ютерних інформаційних

технологій, слід тлумачити як набуті практичні знання та вміння правоохоронних органів інших країн, що можуть бути застосовані для ефективного розслідування зазначеної категорії кримінальних правопорушень.

У сучасному світі серед здобутків іноземного досвіду виокремимо використання можливостей штучного інтелекту під час розслідування кримінальних правопорушень, зокрема кримінальних кіберправопорушень.

Теорію використання штучного інтелекту започатковано 1950 року, коли А. Тюрінг запропонував тест Тюрінга для визначення здатності комп'ютера виявляти інтелектуальну поведінку (машинний інтелект) [306].

Штучний інтелект став невід'ємною складовою суспільства. Його застосування вбачається в різних сферах життєдіяльності людини (культура, музика, медицина, інженерія, правова сфера тощо).

Наприклад, медична система Watson Health, що створена на базі штучного інтелекту, має змогу аналізувати дані пацієнта та на їх підставі встановлювати відповідний діагноз [296].

Музичний сервіс Spotify [313] створив штучний інтелект, що може шукати плагіат у піснях. Аналізуючи мелодію, ноти, текст та акорди, він здатний виокремити конкретні шматки твору й на основі цього підібрати список відповідних пісень, що могли бути першоджерелами [282].

Сформувалася тенденція поступового запровадження штучного інтелекту в правовій сфері.

У цьому контексті зазначимо про застосування судами США штучного інтелекту «COMPAS», що здатний на підставі аналізу кримінального минулого людини, її громадських зв'язків, місця роботи та проживання спрогнозувати, чи вчинить особа правопорушення в майбутньому [273].

У Китаї створено штучний інтелект «Smart Court SoS», що здатний аналізувати судові справи, рекомендувати закони й постанови, які повинен застосувати суд, складати юридичні документи, а також виправляти те, що штучний інтелект вважає людськими помилками у вироку [271].

Вбачаючи необхідність у закріпленні основних положень використання штучного інтелекту, Рада Європи наприкінці 2018 року прийняла першу Європейську етичну хартію про використання штучного інтелекту в судових системах [281].

Згідно з положеннями цієї Хартії [281], штучним інтелектом є набір наукових методів, теорій і технік, метою яких є за допомогою машини відтворити когнітивні здібності людини.

Правоохоронні органи інших країн уже використовують можливості штучного інтелекту й під час проведення розслідування кримінальних правопорушень. Зокрема, у травні 2018 року Нідерланди почали використовувати можливості штучного інтелекту під час розслідування тяжких кримінальних правопорушень. У процесі розслідування зазначених правопорушень штучний інтелект аналізує отримані дані та пропонує, які саме докази має бути використано в кримінальному провадженні, а також може вказувати на ймовірні результати ДНК-експертизи [285].

Певний досвід використання штучного інтелекту під час розслідування кримінальних правопорушень є і у правоохоронних органів Туреччини. Зокрема, з 18 травня 2022 року правоохоронні органи цієї країни почали використовувати програму «ASENA», що допомагає в розслідуванні кримінальних правопорушень, пов’язаних з розповсюдженням наркотичних засобів. Програма аналізує переміщення особи, її маршрути та дії, на підставі цього може сформувати висновок причетності особи до наркотичних кримінальних правопорушень. У чотирьох випадках з десяти програма точно наводить правоохоронні органи на торговців наркотичними засобами [318].

Необхідно зауважити, що 2 грудня 2020 року Кабінет Міністрів України схвалив Концепцію розвитку штучного інтелекту в Україні [199].

У цій Концепції визначено шляхи й способи розв’язання ключових проблем за допомогою впровадження та розвитку штучного інтелекту в таких сферах: освіті, економіці, кібербезпеці, інформаційній безпеці, обороні, публічного управління, правового регулювання та етики, а також правосудді. У сфері кібербезпеки, згідно

з Концепцією, передбачено, що штучний інтелект повинен сприяти захисту комунікаційних, інформаційних і технологічних систем, інформаційних технологій тощо. У сфері інформаційної безпеки – виявляти, запобігати та нейтралізовувати реальні й потенційні загрози поширення через медіа культу жорстокості, насилля, порнографії, спроби маніпулювати суспільною свідомістю, зокрема шляхом розповсюдження упередженої або неповної інформації тощо. У сфері правосуддя – визначати необхідні заходи ресоціалізації засуджених осіб; виносити судові рішення у справах незначної складності (за згодою сторін) тощо.

Натомість у Концепції не зазначено про впровадження та застосування штучного інтелекту в розслідування кримінальних правопорушень, зокрема щодо розслідування кримінальних кіберправопорушень.

За результатами проведеного опитування 200 прокурорів, більша частина (52,5 %) респондентів позитивно оцінює використання штучного інтелекту під час розслідування кримінальних правопорушень [162].

Слід зауважити, що впровадження та використання міжнародного досвіду щодо можливостей штучного інтелекту в процесі розслідування кримінальних кіберправопорушень в Україні дасть змогу швидко й ефективно проводити досудове розслідування, економити час слідчого в складанні процесуальних документів, планувати і висувати версії розслідування, а також аналізувати значну кількість зібраних даних за тривалий проміжок часу [156, с. 277].

Тому для реалізації міжнародного досвіду з використання можливостей штучного інтелекту в розслідуванні кримінальних правопорушень щодо кримінальних кіберправопорушень необхідно:

1) удосконалити чинне національне законодавство, зокрема щоб використання штучного інтелекту регулював відповідний Закон;

2) створити відповідні центри, що можуть постійно вдосконалювати та підтримувати штучний інтелект на належному технічному рівні;

3) підвищити рівень цифрової грамотності працівників органів досудового розслідування та прокурорів, що здійснюють розслідування та процесуальне керівництво зазначених кримінальних правопорушень [156, с. 277].

Висновки до розділу 1

Здійснений аналіз методологічних засад дослідження проблем розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, дає підстави для таких висновків:

1. Наукові дослідження українських вчених-криміналістів, що стосуються проблемних питань розслідування «комп'ютерних злочинів», доцільно поділити на декілька груп за часовими межами.

Першу групу становлять дослідження українських учених із часу проголошення незалежності України до початку XXI ст. (1991–2000). Протягом цього періоду формується загальне уявлення та методика розслідування цього нового виду кримінальних правопорушень – «комп'ютерних злочинів».

Друга група – наукові дослідження щодо методики розслідування «комп'ютерних злочинів» періоду з 2001-го до 2014 року. Необхідність проведення наукових досліджень була зумовлена стрімким розвитком і запровадженням інформаційних технологій у всіх сферах суспільного життя, що своєю чергою спричинило істотне збільшення кількості таких кримінальних правопорушень. Також у цей період відбувається ратифікація Україною Конвенції Ради Європи про кіберзлочинність [99], а КК 2001 року [119] містить самостійний розділ про зазначені кримінальні правопорушення.

Третя група охоплює дослідження, які проводили з 2014 року й донині. Необхідність активізації здійснення криміналістичних досліджень цієї групи кримінальних правопорушень зумовлена насамперед військовою агресією рф проти України, зокрема і з використанням кіберпростору. Крім того, упродовж цього періоду прийнято чимало нормативних документів, спрямованих на запобігання кримінальним правопорушенням цієї категорії.

2. У дослідженні розглянуто лише ті інформаційні технології, що працюють з інформацією в цифровому вигляді в комп'ютері й передбачають поєднання програмних засобів (software) та обраного комплексу технічних засобів (hardware).

Отже, доцільно використовувати термін «інформаційні комп'ютерні технології», акцентуючи на тому, що під час вчинення зазначених кримінальних правопорушень знаряддям є комп'ютер (телефон, планшет, ноутбук тощо).

3. Здійснюючи криміналістичну класифікацію кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, застосовують як кримінально-правові, так і криміналістичні критерії.

За кримінально-правовими критеріями кримінальні правопорушення, що вчиняються з використанням інформаційних комп'ютерних технологій, можна класифікувати на:

1) злочини у сфері основ національної безпеки України, що вчиняються з використанням інформаційних комп'ютерних технологій; 2) кримінальні правопорушення у сфері охорони життя та здоров'я, що вчиняються з використанням інформаційних комп'ютерних технологій; 3) кримінальні правопорушення у сфері волі, честі та гідності особи, що вчиняються з використанням інформаційних комп'ютерних технологій; 4) кримінальні правопорушення у сфері статевої свободи чи статевої недоторканості, що вчинені з використанням інформаційних комп'ютерних технологій; 5) кримінальні правопорушення у сфері виборчих, трудових та інших особистих прав і свобод людини й громадянина, що вчиняються з використанням інформаційних комп'ютерних технологій; 6) кримінальні правопорушення у сфері власності, що вчиняються з використанням інформаційних комп'ютерних технологій; 7) кримінальні правопорушення у сфері господарської діяльності, що вчиняються з використанням інформаційних комп'ютерних технологій; 8) кримінальні правопорушення у сфері громадської безпеки, що вчиняються з використанням інформаційних комп'ютерних технологій; 9) кримінальні правопорушення у сфері громадського порядку та моральності, що вчиняються з використанням інформаційних комп'ютерних технологій; 10) кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, що вчиняються з використанням інформаційних комп'ютерних технологій; 11) кримінальні правопорушення у сфері охорони державної таємниці, що вчиняються

з використанням інформаційних комп'ютерних технологій; 12) кримінальні правопорушення у сфері авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян і журналістів, що вчиняють з використанням інформаційних комп'ютерних технологій; 13) кримінальні правопорушення у сфері правосуддя, що вчиняються з використанням інформаційних комп'ютерних технологій; 14) кримінальні правопорушення у сфері військової служби, що вчиняються з використанням інформаційних комп'ютерних технологій; 15) кримінальні правопорушення у сфері безпеки людства, міжнародного порядку та миру, що вчиняються з використанням інформаційних комп'ютерних технологій.

У межах криміналістичної класифікації кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, ураховуючи відмітні ознаки даних протиправних діянь (вчиняють у кіберпросторі, мають транснаціональний характер тощо), можна виокремити такі криміналістичні критерії: особа злочинця, мотив і мета, особа потерпілого, наслідки тощо.

4. Іноземним досвідом розслідування кримінальних правопорушень, що вчиняються з використанням комп'ютерних інформаційних технологій, слід вважати набуті практичні знання та вміння правоохоронних органів інших країн, що можуть бути застосовані для ефективного розслідування зазначеної категорії кримінальних правопорушень.

5. Упровадження та застосування міжнародного досвіду щодо можливостей використання штучного інтелекту під час розслідування кримінальних кіберправопорушень в Україні дасть змогу швидко й ефективно проводити досудове розслідування, економити час слідчого в складанні процесуальних документів, планувати та висувати версії розслідування, а також аналізувати значну кількість зібраних даних за тривалий проміжок часу.

6. Для реалізації міжнародного досвіду з використання можливостей штучного інтелекту в розслідуванні кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, необхідно:

1) удосконалити чинне національне законодавство, зокрема щоб використання штучного інтелекту регулював відповідний Закон;

2) створити відповідні центри, що можуть постійно вдосконалювати та підтримувати штучний інтелект на належному технічному рівні;

3) підвищити рівень цифрової грамотності працівників органів досудового розслідування та прокурорів, що здійснюють розслідування та процесуальне керівництво зазначеними кримінальними правопорушеннями.

РОЗДІЛ ІІ
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

2.1. Елементний склад криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Розслідування кримінальних правопорушень є особливою діяльністю органу досудового розслідування, мета якої полягає в збиранні, перевірці й оцінці отриманих у процесі розслідування доказів, встановленні підозрюваних осіб і притягненні їх до кримінальної відповідальності.

Саме для ефективного проведення розслідування кримінальних правопорушень учені-криміналісти розробляють відповідні методики розслідування, що мають надавати сучасні науково-методичні рекомендації та слугувати відповідним орієнтиром для слідчого під час розслідування окремих категорій кримінальних правопорушень.

Необхідність розроблення методики розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, засвідчують дані опитування прокурорів, згідно з якими 82 % прокурорів вважають за доцільне подальше розроблення методик для підвищення ефективності розслідування цієї категорії кримінальних правопорушень [162].

Одним із центральних елементів методики розслідування є криміналістична характеристика кримінального правопорушення, що є результатом наукового пізнання та узагальнення типових ознак певного виду або роду кримінальних правопорушень [114, с. 11].

Оскільки серед учених-криміналістів єдиного підходу до визначення загального поняття криміналістичної характеристики кримінальних

правопорушень немає, тому в криміналістичній літературі сформульовано значну кількість різних дефініцій криміналістичної характеристики.

Одним із перших вітчизняних дослідників криміналістичної характеристики є О. Н. Колесниченко [111, с. 359]. На думку вченого, «криміналістична характеристика – це система відомостей про криміналістично значущі ознаки кримінальних правопорушень даного виду, що відображає закономірні зв'язки між ними і служить побудові і перевірці слідчих версій для вирішення основних завдань розслідування» [229, с. 30].

На наш погляд, найзмістовнішим є визначення, запропоноване М. А. Погорецьким, Д. Б. Сергєєвою та З. М. Топорецькою, які криміналістичну характеристику кримінальних правопорушень розглядають як «інформаційну модель типових ознак певного виду (групи) кримінальних правопорушень, яка відображає закономірні зв'язки між цими ознаками та дозволяє обрати необхідну методику та засоби розслідування» [210, с. 25].

Дискусійним є питання виокремлення основних елементів криміналістичної характеристики, що пов'язані між собою.

Традиційно в криміналістичній літературі визначають від чотирьох до десяти елементів криміналістичної характеристики кримінальних правопорушень. Здебільшого це: 1) предмет посягання; 2) спосіб вчинення кримінального правопорушення; 3) особа злочинця; 4) місце, час й обстановку; 5) типові сліди («слідова картина») та ін.

Розглядаючи криміналістичну характеристику кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, В. О. Голубєв слушно зауважує, що криміналістична характеристика зазначених протиправних діянь є сукупністю найбільш значущої взаємопов'язаної інформації про ознаки та властивості таких кримінальних правопорушень, що здатні слугувати підставою для висунення версій про подію кримінального правопорушення і особу кіберзлочинця, а також дає змогу правильно оцінити ситуації, що виникають у процесі розслідування [51, с. 65].

Посиленої уваги потребує встановлення кількісного та якісного складу елементів криміналістичної характеристики зазначеної категорії кримінальних правопорушень.

На підставі наукових досліджень вітчизняних вчених-криміналістів різних часів [12, с. 229; 51, с. 65; 72, с. 41; 86, с. 387–393; 112, с. 867; 134, с. 283–301; 138; 164; 202, с. 185], присвячених проблематиці розслідування «комп'ютерних злочинів», «інформаційних злочинів», «кіберзлочинів», «злочинів у сфері інформаційних технологій» тощо, можна виокремити такі притаманні цьому виду кримінальних правопорушень елементи криміналістичної характеристики: 1) об'єкт; 2) предмет злочинного посягання; 3) способи вчинення; 4) способи приховування; 5) особа злочинця; 6) особа потерпілого; 7) сліди вчинення («слідова картина»); 8) знаряддя та засоби вчинення; 9) місце, час, обстановка; 10) місце (як окремий елемент); 11) час (як окремий елемент); 12) обстановка (як окремий елемент); 13) мотив і мета (як окремий елемент і у взаємозв'язку з іншими елементами).

З огляду на викладене, на наше переконання, для кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, найбільш значущими елементами криміналістичної характеристики, які згодом буде досліджено, є спосіб вчинення, типові сліди, обстановка й особа злочинця. Зазначені елементи криміналістичної характеристики кримінальних правопорушень цієї категорії розглядає переважна більшість учених-криміналістів.

Потребує аналізу позиція О. А. Самойленко, яка розглядає наявність зв'язків між елементами, що утворюють механізм його вчинення: 1) предмет посягання та його зв'язок з мотивами вчинення кримінальних правопорушень у кіберпросторі; 2) взаємозв'язок типової особи злочинця і типових слідів; 3) типові способи/технології вчинення кримінальних правопорушень у кіберпросторі [217, с. 3].

У контексті встановлення взаємозв'язку між елементами криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, слушною є думка В. Ю. Шепітька, що

елементи криміналістичної характеристики мають кореляційні зв'язки (імовірні залежності), тобто за наявності одних ознак слідчий може припустити наявність інших [114, с. 11].

Із цього приводу В. Л. Синчук зауважує, що виявлення та використання кореляційних залежностей між елементами криміналістичної характеристики кримінальних правопорушень надає можливість шляхом індукції припустити наявність ще не відомих фактів, які мають відношення до події кримінального правопорушення. Тобто виявлення в процесі розслідування будь-якого елемента системи з певним ступенем імовірності може вказувати на наявність іншого, ще не встановленого елемента, визначати напрями й засоби його пошуку. Саме в можливості розкриття конкретного кримінального правопорушення з використанням узагальнених даних про раніше розслідувані аналогічні кримінальні правопорушення і полягає практичне інструментальне значення криміналістичної характеристики [224, с. 114–115].

Вбачається, що в кореляційному зв'язку знаходяться такі елементи криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, як спосіб вчинення і типові сліди. Залежно від обрання злочинцем способу вчинення, слідчий може зрозуміти, де необхідно шукати сліди зазначеного кримінального правопорушення. Це можна простежити на прикладі ухвалених вироків.

Згідно з вироком Києво-Святошинського районного суду Київської області від 9 листопада 2021 року, було встановлено, що ОСОБА_1, який має навички програмування, здійснив розповсюдження шкідливого програмного забезпечення, що здатне здійснювати несанкціоноване втручання в роботу комп'ютерів з метою викрадення персональних даних.

Використовуючи власний персональний комп'ютер із жорстким диском, на якому виявлено відомості про авторизацію для адміністрування облікового запису за відповідним посиланням, розповсюдив шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, використовуючи раніше створену поштову скриньку, у якій створив лист з текстом «Обучение в

использование 50$», прикріпивши архів, що містить шкідливі програмні засоби, призначені для викрадення персональних даних, і надіслав на поштову скриньку ОСОБА_2. Для цього використав серверне обладнання, що забезпечувало надання послуг хостингу на засадах анонімності за визначену плату.

Унаслідок надсилання електронного листа з поштової скриньки зі шкідливими програмними засобами на електронну поштову скриньку ОСОБА_2 ОСОБА_1 отримав пароль до його поштової скриньки та несанкціонований доступ до перегляду особистої інформації, розміщеної на ній, тобто вчинив несанкціоноване втручання в роботу персонального комп'ютера, що належить ОСОБА_2, яке призвело до витоку особистої інформації останнього та порушення встановленого порядку її маршрутизації [36].

За іншим *вироком Київського районного суду міста Полтави від 12 серпня 2022 року, після початку збройної агресії рф проти України громадянка України ОСОБА_1, перебуваючи за місцем свого проживання, використовуючи власний мобільний телефон Samsung Galaxy M11, через мережу Інтернет зі своєї сторінки в соціальній мережі умисно, протиправно та систематично здійснювала публічні заперечення здійснення збройної агресії проти України та публічні заклики до підтримки рішень та/або дій держави-агресора шляхом поширення на власній сторінці у соціальній мережі закликів, спрямованих на заперечення здійснення збройної агресії проти України та підтримки рішень і дій держави-агресора* [37].

У таких випадках способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій – це: 1) розповсюдження шкідливого програмного забезпечення та використання послуг хостингу, що надають анонімність; 2) поширення на власній сторінці в соціальній мережі закликів на заперечення збройної агресії (поширення шкідливого контенту) шляхом використанням мобільного телефону та мережі Інтернет.

Такі способи вчинення дають змогу слідчому зрозуміти, де особа залишила ймовірні сліди протиправного діяння. У цих випадках сліди було залишено в засобах інформаційних комп'ютерних технологій (персональний комп'ютер (його

апаратні та програмні засоби), мобільний телефон, комп'ютер жертви, а також сервер тощо).

Досліджуючи кореляційний взаємозв'язок між обстановкою та особою злочинця як елементами криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, проаналізуємо такі ситуації.

Згідно з вироком Смілянського міськрайонного суду Черкаської області від 29 квітня 2022 року, було встановлено, що ОСОБА_1 3 травня 2021 року в проміжок часу з 08 год 38 хв до 10 год 49 хв, перебуваючи в приміщенні магазину «Ходак», що на вул. В. Чорновола, 3, у м. Сміла Черкаської області, маючи умисел на заволодіння грошовими коштами з банківської картки (універсальна) ПАТ КБ «ПриватБанк», що належить ОСОБА_2, володіючи спеціальними навичками, застосовуючи програмні засоби, здійснив несанкціонований доступ до інформації, що зберігається та обробляється в автоматизованій системі ПАТ КБ «ПриватБанк». Видаючи себе за власника картки, увів в оману автоматизовану систему та за допомогою власного мобільного телефону не встановленої слідством марки та моделі шляхом використання мережі Інтернет прикріпив до банківського рахунку ОСОБА_2 фінансовий ліміт картки ПАТ КБ «ПриватБанк», що належала ОСОБА_2, з якої 3 травня 2021 року о 08 год 38 хв перевів грошові кошти в сумі 5000 грн на інтернет розваги, заподіявши потерпілому матеріальної шкоди на зазначену суму.

Після цього ОСОБА_1 здійснив ще низку протиправних дій:

– 3 травня 2021 року з 08 год 30 хв до 09 год 30 хв, перебуваючи в приміщенні магазину «Ходак», що на вул. В. Чорновола, 3, у м. Сміла Черкаської області, умисно заволодів грошима в сумі 20 000 грн;

– цього самого дня о 10 год 49 хв, перебуваючи в парку культури та відпочинку, що на вул. Перемоги в м. Сміла Черкаської області, за допомогою власного мобільного телефону не встановленої слідством марки та моделі шляхом використання мережі Інтернет перевів грошові кошти в сумі 5000 грн на інтернет розваги;

– 06 травня 2021 року в проміжок часу з 12 год 13 хв до 12 год 53 хв у не встановленому слідством місці, маючи доступ до рахунку ОСОБА_2, за допомогою мережі Інтернет у 9 спроб перевів грошові кошти в сумі 10 600 грн з картки ОСОБА_2 на розваги в мережі Інтернет [38].

В іншій ситуації, *згідно з вироком Суворовського районного суду міста Одеси від 16 березня 2021 року, ОСОБА_1, перебуваючи за місцем свого проживання, використовуючи комп'ютер, під'єднаний до мережі Інтернет, зареєстрував власну сторінку на вебсайті й використовував її для того, щоб розповсюдити матеріали із закликами до умисних дій, вчинених з метою зміни меж державного кордону України.*

Згодом 25 квітня 2020 року ОСОБА_1, усвідомлюючи, що зі змістом матеріалів, які були ним розповсюджені в Інтернеті, може ознайомитися необмежена кількість осіб, а також бажаючи настання шкідливих наслідків (протиправного відокремлення південної та південно-східної частин території України), перебуваючи за зазначеним вище місцем свого проживання, використовуючи комп'ютер, під'єднаний до мережі Інтернет, використовуючи браузер Chrome з активованим вбудованим сервісом для доступу до заблокованих інтернет ресурсів, авторизувавшись у соціальній мережі як користувач «ОСОБА_2», розмістив на «стіні» (публічній дошці оголошень) публікацію, яка містить зображення карти України з відокремленими південною та південно-східною частинами території України, зображеними в кольорах прапору Російської Федерації, що було доступно для загального ознайомлення всім користувачам соціальної мережі Інтернет [39].

Отже, залежно від особи злочинця, а саме його обізнаності у використанні інформаційних комп'ютерних технологій, можна визначати обстановку кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

У першому випадку для цього типу особи злочинця, який має навички та вміння використання інформаційних комп'ютерних технологій, притаманним є вчинення протиправних діянь не за місцем проживання, а з різних місць.

У другому випадку особливість таких типів особи злочинця полягає у вчиненні протиправних дій за місцем свого проживання, тобто за місцем розміщення власного комп'ютерного засобу.

На підставі викладеного можна дійти висновку, що визначення кількісної та якісної структури елементів криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, залежить від:

1) дослідження та використання українськими вченими-криміналістами структурних елементів криміналістичної характеристики у своїх працях, що дає змогу узагальнити їх використання та обрати найбільш застосовувані елементи криміналістичної характеристики;

2) аналізу криміналістичних даних про раніше вчинені кримінальні правопорушення, що вчиняються з використанням інформаційних комп'ютерних технологій, які дають змогу встановити кореляційні зв'язки між обраними елементами криміналістичної характеристики.

2.2. Спосіб і сліди кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Посилену увагу під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, необхідно спрямувати на спосіб їх вчинення.

Термін «спосіб» тлумачать як певну дію, прийом чи систему прийомів, що надає можливість зробити, виконати щось, досягти потрібного результату [29, с. 1179].

У юридичній науці спосіб вчинення кримінального правопорушення досліджують у кримінально-правовому, кримінально-процесуальному, криміналістичному напрямах, що позначається на його визначенні.

Зокрема, у кримінальному праві спосіб вчинення пов'язаний з іншими елементами об'єктивної сторони кримінального правопорушення та є

кваліфікуючою ознакою. Кримінально-процесуальне право розглядає спосіб вчинення як структурну обставину предмета доказування. У криміналістиці за допомогою встановлення способу вчинення кримінального правопорушення розшукують осіб, які його вчинили, і з'ясовують закономірності механізму слідоутворення [33, с. 27].

У криміналістичній науці спосіб вчинення кримінального правопорушення вчені почали вивчати із середини XX ст., ці дослідження не втратили своєї актуальності й нині.

Цілком слушно зауважує В. О. Коновалова, що проблема способу вчинення кримінального правопорушення як одна з ключових у криміналістиці залишається дискусійною. Це спричинено наявністю різних підходів науковців до інтерпретації понятійного апарату, зокрема до змісту понять «спосіб вчинення» і «спосіб приховування» [103, с. 7].

Наприклад, М. В. Даньшин допускає самостійне існування за певних умов способу приховування кримінального правопорушення, що не належить до структури способу його вчинення. Такою умовою є відсутність єдиного злочинного задуму, що охоплює всі стадії злочинної діяльності [61, с. 10].

Своєю чергою О. Н. Колесниченко сформулював власну криміналістичну концепцію способу вчинення кримінального правопорушення, яку пропонує визначати як спосіб дій злочинця, що виявляється в певній послідовності, поєднанні окремих дій, прийомів, застосовуваних суб'єктом. Учений запропонував розглядати окремо спосіб готування, спосіб вчинення і спосіб приховування кримінального правопорушення [229, с. 35].

Натомість С. М. Зав'ялов вважає, що спосіб вчинення кримінального правопорушення – це спосіб дій з готування, вчинення та приховання слідів кримінального правопорушення, що характеризує криміналістично значущі дані про виконавця та засоби, які він застосовує, можливості використання цих даних у розкритті й розслідуванні кримінальних правопорушень [74, с. 93–94].

Найвичерпнішим вбачається визначення, запропоноване М. А. Погорецьким, Д. Б. Сергєєвою та З. М. Топорецькою, що спосіб вчинення кримінального

правопорушення – це послідовність дій суб'єкта, спрямована на досягнення поставленої мети (певного злочинного результату), це все те, що характеризує дії злочинця в процесі підготовки (підшукання місця, підготування знарядь і засобів, необхідних для здійснення злочинної мети), вчинення та приховування слідів кримінального правопорушення [210, с. 27].

Цілком слушно стверджує В. Ю. Шепітько, що готуванням є підшукування або пристосування знарядь чи засобів, пошук співучасників, усунення перешкод, а також інше умисне створення умов для вчинення кримінального правопорушення (ст. 14 КК України). Такі підготовчі дії створюють лише умови до вчинення кримінального правопорушення. Своєю чергою приховування кримінального правопорушення є однією з форм протидії розслідуванню, що за змістом можуть поділятися на: приховування шляхом утаювання інформації, знищення інформації (зокрема слідів кримінального правопорушення), маскування та фальсифікації інформації (створення неправдивих слідів та інших речових доказів) [114, с. 12–13].

Попри несформованість єдиного підходу вчених-криміналістів до трактування способу вчинення кримінального правопорушення та враховуючи наявні позиції науковців, доходимо висновку, що для кримінальних правопорушень, які вчиняються з використанням інформаційних комп'ютерних технологій, притаманними є дії, що передбачають готування, вчинення та приховування.

Загалом спосіб вчинення кримінальних правопорушень зазначеної категорії – це сукупність послідовних дій суб'єкта (суб'єктів), що охоплюють дії з готування, вчинення та приховування, спрямовані на досягнення певного злочинного результату з використанням інформаційних комп'ютерних технологій [145, с. 121].

Слід зауважити, що спосіб вчинення відбувається в кіберпросторі, натомість дії з готування та приховування можуть вчиняти як у кіберпросторі, так і поза його межами.

У більшості вчинених кримінальних кіберправопорушень наявні дії з підготовки та приховування, оскільки їх не можуть вчиняти раптово, вони потребують необхідних технічних знань і навичок, тобто певної підготовки.

У разі використання інформаційних комп'ютерних технологій з метою вчинення кримінального правопорушення у зловмисника формується розуміння, що його буде складно встановити, оскільки він вчиняє протиправні дії віддалено, а інформаційні комп'ютерні технології дають змогу приховати себе.

У криміналістичній науковій літературі є різні думки вчених стосовно виокремлення ймовірних способів вчинення зазначеної категорії кримінальних правопорушень.

Свого часу О. І. Мотлях розглядав три види способів вчинення: 1) способи безпосереднього доступу до комп'ютерних технологій (операційної системи) та комп'ютерної інформації; 2) способи віддаленого (опосередкованого) доступу; 3) способи виготовлення, розповсюдження на технічних носіях шкідливих програм для електронно-обчислювальної машини [138, с. 44].

На думку Н. М. Ахтирської, способи вчинення кіберзлочинів слід класифікувати на підставі правової регламентації, тобто в межах статей КК України [12, с. 108–110].

Цілком слушно вчена додає, що кримінально-правовою характеристикою способів протиправних дій не слід обмежуватися, оскільки є розгалужена система способів вчинення кримінальних правопорушень цієї категорії з притаманними їм ознаками залежно від сфери вчинення: банківська (платіжні системи, зміна маршрутизації коштів, перехоплення даних карток тощо); енергетична система; сфера державного управління; оборона, правоохоронна система і правосуддя (втручання в роботу інформаційних автоматизованих систем) тощо [12, с. 110].

Достатньо складно виокремити всі способи вчинення цих кримінальних правопорушень [148, с. 238], оскільки з розвитком інформаційних комп'ютерних технологій цей вид злочинної діяльності буде стрімко змінюватися, спричиняючи виникнення нових способів. Однак, з огляду на реалії сьогодення, можна визначити

найтиповіші та найпоширеніші нині способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій:

1) використання шкідливого програмного забезпечення;

2) вчинення DoS/DDoS атак;

3) несанкціонований доступ до інформації;

4) шахрайство, вчинене з використанням інформаційних комп'ютерних технологій;

5) поширення шкідливого (протиправного) контенту (спам, погрози, створення, поширення та збут дитячої порнографії, заклики до вчинення насильства, домагання тощо);

6) порушення авторських чи суміжних прав з використанням інформаційних комп'ютерних технологій;

7) комплекс способів і використання інформаційних комп'ютерних технологій як засіб користування кіберпростором для вчинення інших кримінальних правопорушень.

Детальніше схарактеризуємо кожен з окреслених способів вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій.

До першої групи належать дії зі створення шкідливого програмного забезпечення (або вдосконалення вже наявного), придбання, збут або розповсюдження, а також його використання з метою отримання незаконного доступу до системи або даних засобів інформаційних комп'ютерних технологій.

У світі є широким є масив шкідливого програмного забезпечення: віруси, хробаки, рекламне ПЗ, «троянський кінь» (троян), макровіруси, руткіти, keylogger (кейлогери), BIOS-віруси, шпигунські програми тощо, які використовують залежно від мети злочинця [145, с. 122].

Одними з найпоширеніших шкідливих програмних засобів, стверджує М. Гудмен, є троянські програми. Вони часто маскуються під легальні компоненти програмного забезпечення та активуються для завдання удару по цілі, коли користувач завантажує комп'ютер і запускає для виконання файли в конкретному

програмному середовищі. Трояни часто створюють «чорні ходи» або «люки», що дають хакерам постійний доступ до зараженої системи [77, с. 22].

Слід зауважити, що в національному кримінальному законодавстві немає конкретного визначення шкідливого програмного забезпечення.

Згідно з рекомендаціями щодо обмеження наслідків впливу шкідливого програмного забезпечення урядової команди реагування на комп'ютерні надзвичайні події, що функціонує в складі Державної служби спеціального зв'язку та захисту інформації України, шкідливим програмним забезпеченням є програмне забезпечення, яке за умови запуску може завдати шкоди різними способами, зокрема: 1) призвести до блокування пристрою або його непридатності для використання; 2) здійснити крадіжку, шифрування, зміну чи видалення даних; 3) використати засіб інформаційно-комп'ютерних технологій для атак на інші організації; 4) здійснити майнинг криптовалюти; 5) використовувати платні послуги на основі даних, що знаходяться в засобах інформаційних комп'ютерних технологій; 6) отримати облікові дані, що дозволяється отримати доступ до використовуваних систем або служб [75].

З огляду на зазначене, можна окреслити найвагоміші криміналістичні ознаки шкідливого програмного забезпечення (шкідливої програми):

– програма здатна блокувати, шифрувати та змінювати інформацію, а також використовувати можливості засобів інформаційно-комп'ютерних технологій;

– програма діє таємно і не попереджає власника про характер своїх дій;

– для виявлення програми необхідно мати спеціальні знання, а для встановлення, що програма справді є шкідливою, необхідно провести відповідну експертизу.

Друга група – вчинення DoS/DDoS атак, які є нападом на комп'ютерну систему з наміром заблокувати цей ресурс, зробивши його не доступним для користувачів. DDoS атака – це розподілений напад, який відбувається одночасно з зі значної кількості IP-адрес [280].

Наприклад, від великої DDoS атаки постраждали парламент Бельгії, інтернет-провайдер і правоохоронні органи. Через цю атаку парламенту Бельгії довелося

перенести засідання, а поліцейські сайти Брюсселя та Антверпена були недоступними. Також недоступними на деякий час виявилися системи онлайн запису на вакцинацію від COVID-19 [298].

Здебільшого злочинці заражають засіб інформаційних комп'ютерних технологій шкідливим програмним забезпеченням, через що він стає частиною ботнету й використовується для вчинення DDoS атак [145, с. 123].

Ботнет – це комп'ютерна мережа, що складається з послідовності хостів із запущеними ботами – автономними програмами [26]. Один з найвідоміших є Bredolab, який функціонував протягом 2009–2010 років і налічував понад мільйон комп'ютерів зомбі, що здійснювали розсилання різного спаму [26].

Третя група – це здійснення несанкціонованого доступу, суть якого полягає в одержанні злочинцем доступу до об'єкта (інформації) [76, с. 12].

Злочинці використовують різні методи, щоб отримати доступ до інформації інших осіб, що знаходиться в засобах інформаційних комп'ютерних технологій. Зокрема, це дії з аналізу трафіку, самостійного добору паролів, брутфорсу тощо.

Аналіз трафіку передбачає перехоплення і подальший аналіз мережевого трафіку з метою отримання певної інформації [3].

Під час самостійного добору паролів особа добирає (чи вгадує) пароль до даних (облікового запису в соціальній мережі, електронної пошти тощо).

Наприклад, хакер з Нідерландів отримав несанкціонований доступ до аккаунта Дональда Трампа в соціальній мережі Twitter з 5-ї спроби, вгадавши пароль [241].

Брутфорс атака – злом облікового запису шляхом перебору всіх можливих комбінацій паролів.

Здебільшого злочинці намагаються отримати несанкціонований доступ до інформації, що знаходиться в засобах інформаційних комп'ютерних технологій, для подальшого розповсюдження чи збуту отриманої інформації.

Наприклад, 2020 року в мережу Інтернет було викладено базу даних, що налічує понад 300 млн ідентифікаторів користувачів Facebook: номери телефонів, імена та прізвища тощо. Будь-хто міг отримати доступ до цієї бази без паролів чи

автентифікації. Така інформація може бути використана для проведення SMS-розсилок і шахрайства [308].

До четвертої групи належить поширене в наш час інтернет-шахрайство. Це вид шахрайства з використанням мережі Інтернет і засобів інформаційних комп'ютерних технологій (комп'ютерів, телефонів, планшетів тощо) [145, с. 123].

Найпоширенішим видом інтернет-шахрайства є фішинг, мета якого полягає в отриманні конфіденційних даних особи шляхом підроблення електронних листів, оголошень або сайтів чи програмного забезпечення [259].

Зокрема, зловмисник самотужки розробив програмне забезпечення (застосунок) для смартфонів, який за своїм дизайном був ідентичним із державним застосунком «Дія» [239].

В іншому випадку ПАТ КБ «ПриватБанк» виявив небезпечний фішинговий сайт, що виманює в користувачів логіни та паролі для входу до електронного банкінгу. Цей сайт «замаскувався» під програми виплат українцям і збирав дані для викрадення грошей з рахунків [174].

Для вчинення шахрайства з використанням інформаційних комп'ютерних технологій поширеним є застосування методу соціальної інженерії – збір інформації від людини не технічними засобами (брехня, погрози, моніторинг особи в соціальній мережі тощо), а із застосуванням «психологічних хитрощів» [307, с. 9].

П'ята група кримінальних правопорушень, які вчиняються з використанням інформаційних комп'ютерних технологій, передбачає поширення шкідливого або протиправного контенту (спаму, погроз, створення, поширення та збут дитячої порнографії, заклики до вчинення насильства, домагання тощо), яке може негативно позначитися на психологічному стані особи чи осіб [145, с. 123].

Шоста група – незаконне копіювання, поширення або публікація програмного забезпечення, ігор і всього, що захищено авторським чи суміжним правом, з використанням засобів інформаційних комп'ютерних технологій та кіберпростору (поширення та публікація) [145, с. 123].

Сьомий комплекс способів охоплює дві чи більше різних груп способів вчинення, причому один з них використовується як основний, а інший – як додатковий. Наприклад, використання шкідливих програм (1) для зараження засобів інформаційних комп'ютерних технологій з подальшим використанням їх у мережі ботнетів для вчинення DDoS атак (2).

З використанням інформаційних комп'ютерних технологій переважно як засобу для виходу в кіберпростір (мережу Інтернет) можуть вчиняти низку інших кримінальних правопорушень: збут майна, одержаного злочинним шляхом, збут наркотичних засобів тощо.

Важливу роль у виявленні та розслідуванні кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, відіграють знання про способи підготовки та приховування, які допомагають слідчому зрозуміти мислення злочинця, спробувати спрогнозувати його подальші дії та запобігти їм.

На нашу думку, способами підготовки до вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій також можуть бути: 1) перегляд відповідних «гайдів» із вчинення кримінального правопорушення (наприклад, гайд зі створення шкідливого програмного забезпечення); 2) добір відповідних сервісів анонімізації; 3) вивчення жертви за її діяльністю в соціальних мережах; 4) створення фейкових облікових записів; 5) пошук співучасників (однодумців) у мережі Інтернет; 6) використання даних інших геолокацій.

З приводу способів приховування доречно зазначає О. І. Мотлях, що способи приховування кримінальних правопорушень, пов'язаних з інформаційними комп'ютерними технологіями, мають певну відмінність від традиційних. Зокрема, злочинці легковажно ставляться до способів приховування злочинної діяльності, мотивуючи це таким: 1) власні практичні знання та здібності в керуванні інформаційними комп'ютерними технологіями вважають досконалішими за знання фахівців правоохоронних органів у цій сфері; 2) переконані, що залишені ними сліди мають тимчасовий характер або їх взагалі немає; 3) вважають низькою

ймовірність виявлення доказів, що аргументовано б доводили їх винуватість [138, с. 47–48].

До типових способів приховування кримінальних кіберправопорушень можна віднести:

– перекручення чи знищення інформації;

– використання програм, що ускладнюють виявлення неправомірного доступу;

– мінімізація обсягу інформації для учасників кримінального правопорушення щодо справжньої його мети;

– використання викрадених паролів і логінів;

– упровадження замаскованих шкідливих програм (типу «троянський кінь»);

– використання фальсифікованої поштової електронної або IP-адреси;

– використання анонімних серверів;

– використання програм, що ускладнюють виявлення неправомірного доступу [112, с. 870; 134, с. 294].

На нашу думку, такі переліки є обґрунтованими, проте вони не є вичерпними, їх можна доповнити іншими способами, зокрема: зміна справжнього місця геолокації, використання «заражених» засобів інформаційних комп'ютерних технологій тощо.

Безперечно, інтенсивний розвиток інформаційних комп'ютерних технологій змушує зловмисників підлаштовуватися та вигадувати нові способи незаконного використання інформаційних комп'ютерних технологій у своїх злочинних намірах. Тому знання про типові способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій сприяє ефективнішій організації та проведенню розслідування. Насамперед, розуміння способу вчинення дає змогу слідчому визначитися щодо конкретних напрямів пошуку слідів протиправного діяння [145, с. 123].

Дані про спосіб вчинення, слушно зауважує В. Ю. Шепітько, дають змогу повністю встановити сліди, їх локалізацію та особливості механізму слідоутворення, оскільки в процесі злочинного діяння використання злочинцем

певного способу вчинення означає залишення характерного комплексу слідів [114, с. 13].

Водночас М. В. Салтевський зазначає, що сліди кримінального правопорушення – це результат відображення минулого, поданого в сьогоденні, результат взаємодії об'єктів неживої та живої природи, що опинилися у сфері злочинної діяльності [214, с. 86, 89].

У криміналістичній літературі є різні думки вчених стосовно трактування слідів кримінального правопорушення як елементу криміналістичної характеристики, а також щодо використання відповідного поняття: «слідова обстановка», «слідовий вібавід», «слідова картина» кримінального правопорушення. Деякі науковці виокремлюють поняття «слідова обстановка» кримінального правопорушення, розуміючи його як час, місце, обставини, обстановку вчинення кримінального правопорушення. «Слідова обстановка» концентрує проблематику ідеальних і матеріальних слідів. М. І. Скригонюк пропонує використовувати поняття «слідовий вібавід», обґрунтовуючи це тим, що слово «вібавід» утворюється як абревіатура трьох слів-компонентів: ві – відображення, ба – бачення, від – відтворення [227, с. 250].

Водночас поняття «слідова картина» кримінального правопорушення ввів у криміналістичну термінологію М. В. Салтевський, розглядаючи обстановку в широкому її значенні як елемент криміналістичної характеристики, що становить абстрактну модель ознак кримінального правопорушення, які відображаються в матеріальному середовищі внаслідок його вчинення [212, с. 14, 17–18].

Проте, на наше переконання, слід розглядати окремо обстановку та сліди як елементи криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, оскільки в кримінальних правопорушеннях зазначеної категорії вагомим криміналістичним елементом є також обстановка їх вчинення.

Традиційно в криміналістичній літературі прийнято поділяти сліди на матеріальні та ідеальні. Ідеальні сліди – це відображення події або її елементу в пам'яті людини, уявний образ сприйнятого, характер якого залежить від стану

органів чуття особи, її пам'яті, рівня інтелекту тощо. Матеріальні сліди – це відображення механізму події та її результатів на об'єктах матеріального світу [113, с. 138].

У межах базового визначення розглядають і сліди кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. Матеріальними слідами цієї категорії кримінальних правопорушень необхідно вважати [112, с. 876–877]:

– сліди-відображення зовнішнього фізичного впливу на інформаційні комп'ютерні технології (сліди рук, ніг, знарядь злому тощо);

– сліди-речовини у вигляді витратних матеріалів (тонерів, фарб, різних мастил, що використовують у комп'ютерних системах, їх мережах і периферійних пристроях);

– сліди-предмети – змінні диски та стрічки, пристрої дистанційного зняття інформації, роздруківки на паперових носіях і документи на електронних носіях, кабелі та роз'єми, пристрої фізичного знищення комп'ютерів, їх мереж.

Своєю чергою ідеальні сліди залишаються в пам'яті людини, яка сприймала дії злочинця або наслідки його втручання в інформаційну систему. Нерідко такі сліди мають вирішальне значення, оскільки є єдиними й відіграють важливу роль у діагностичних дослідженнях, дають змогу встановити причиновий зв'язок між подією і наслідками, на цій підставі з'ясувати динаміку подій, що відбулися [126, с. 470–471].

Однак у криміналістичній науці тривають дискусії стосовно того, чи доцільно виокремлювати третій вид слідів, що знаходяться в засобах інформаційних комп'ютерних технологій у цифровому вигляді. Деякі науковці доводять, що такі сліди є виключно матеріальними слідами, а інші вважають їх окремим видом слідів. Для їх позначення використовують різні поняття: «електронні цифрові сліди», «інформаційні сліди», «електронні сліди», «комп'ютерні сліди» тощо.

Зокрема, у науковій літературі запропоновано такі визначення [1, с. 173; 24, с. 88–89; 51, с. 108–109; 166, с. 60]:

– «комп'ютерні сліди» – матеріальні сліди, що утворюються в кіберпросторі або віртуальному просторі (Д. В. Пашнєв);

– «електронні цифрові сліди» – матеріальні невидимі сліди, які фіксують за допомогою електронних пристроїв, вони містять відомості чи дані, зафіксовані на матеріальних носіях (Г. В. Авдєєва та С. В. Стороженко);

– «інформаційні сліди» – нетрадиційні сліди, що утворюються внаслідок впливу на комп'ютерну інформацію (В. О. Голубєв);

– «віртуальні сліди» – сліди, що виникають унаслідок впливу на інформаційні процеси (А. С. Білоусов).

На нашу думку, уваги потребує позиція Н. М. Ахтирської, яка використовує поняття «електронний слід» і зазначає, що електронна інформація не належить у чистому вигляді ні до матеріальних слідів, ні до ідеальних. Як матеріальний слід електронна інформація зберігається в пам'яті машини й може бути вилучена звідти, а принцип дії комп'ютера має схожість з принципом діяльності мозку людини, хоча й відрізняється від нього тим, що складається не з нейронів, а з електронних схем. Також електронній інформації притаманні певні ознаки «ідеального» сліду: вона невидима, не сприймається ні за допомогою людських органів (зору, слуху), ані за допомогою спеціальних засобів посилення сприйняття (збільшувальні пристрої, спеціальні порошки тощо) [12, с. 136–137].

Специфічні властивості електронних слідів такі: 1) відсутність нерозривного зв'язку з матеріальним носієм; 2) можливість миттєвого перенесення в просторі; 3) можливість знищення чи зміни інформації будь-якого обсягу за стислі проміжки часу; 4) ідентичність оригіналу інформації, що має електронну форму, і всіх його копій (незалежно від виду носія інформації) [1, с. 171].

Загалом електронні сліди можуть знаходитися: 1) у комп'ютерах (персональні комп'ютери, ноутбуки, нетбуки, ультрабуки, планшети, телефони тощо); 2) на пристроях зберігання даних (жорсткі та твердотільні накопичувачі, компакт-диски, стрічкові диски, карти пам'яті, USB-пристрої для зберігання даних, периферійні пристрої (сканер, факс, принтер тощо), цифрових камерах й аудіо-, відеокамерах, камерах відеоспостереження, портативних медіаплеєрах, гральних

приставках); 3) комп'ютерній мережі (локальна мережа та глобальна мережа, маршрутизатори тощо) [63].

Залежно від осіб електронні сліди можуть знаходитися: 1) на засобах інформаційних комп'ютерних технологій потерпілого; 2) в інтернет-провайдера, послугами якого користувався потерпілий; 3) на засобах інформаційних комп'ютерних технологій злочинця; 4) в інтернет-провайдера, послугами якого користувався підозрюваний; 5) в іншому місці кіберпростору [35, с. 8].

Слідами в засобах інформаційно-комп'ютерних технологій потерпілого є зміни в оперативному запам'ятовувальному пристрої, конфігурації, позаштатних режимів роботи [217, с. 126, 128] й окремих програмних продуктах [1, с. 172].

Інтернет-провайдери сліди зберігають у вигляді спеціальних файлів реєстрації – так званих Log-файлах, що є спеціальними файлами реєстрації події, у якому накопичується зібрана статистична чи службова інформація про події в системі (програмі) у хронологічному порядку. Такі Log-файли використовують для аналізу подій, виявлення помилок, збоїв, зведення статистичних даних, звітувань, відстеження дій підозрілих користувачів, вузлів тощо [161, с. 8].

У більшості випадків саме ретельний аналіз і дослідження Log-файлів має надзвичайно важливе значення для ефективного проведення розслідування в зазначених кримінальних правопорушеннях.

У засобах інформаційно-комп'ютерних технологій, що застосовував злочинець, сліди можуть зберігатися у вигляді змін у файловій системі, спеціальному «хакерському» програмному забезпеченні, в інформації на зйомних носіях [217, с. 126, 128].

Слід зауважити, що важливу інформацію мають і тимчасові файли. Більшість текстових редакторів і систем управління базами даних створюють тимчасові файли як побічний продукт нормальної роботи програмного забезпечення. Користувачі комп'ютерів переважно не усвідомлюють важливості створення цих файлів у зв'язку з тим, що їх знищує програма наприкінці сеансу роботи [35, с. 9].

Також криміналістично значущі сліди можна виявити й у кіберпросторі у вигляді даних електронного листування, за допомогою яких можна встановити

дату й час, адресу відправника тощо; даних на різних сайтах (Facebook, Twitter, Instagram тощо), які залишають електронні сліди у вигляді повідомлень, пошукових запитів, фотознімків тощо [1, с. 172].

Водночас під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, не слід нехтувати матеріальними слідами, що залишені на засобах інформаційних комп'ютерних технологій, та ідеальними слідами.

Відмітна ознака слідів у зазначених протиправних діяннях полягає в тому, що вони можуть залишатися не тільки в кіберпросторі, а й поза його межами.

Отже, залежно від обрання злочинцем відповідного способу вчинення кримінального правопорушення, вчиненого з використанням інформаційних комп'ютерних технологій, можна розуміти, де залишаються сліди їх вчинення. Однак характер залишених електронних слідів залежить від низки факторів, зокрема: виду операційної системи злочинця та потерпілого, особливостей засобів інформаційних комп'ютерних технологій та їх програмного забезпечення тощо.

Тому в цих категоріях кримінальних правопорушень, залежно від способу їх вчинення, головним для органу досудового розслідування завжди буде розуміння, де саме знаходяться ймовірні типові сліди вчинення, щоб їх вилучити в належний спосіб, не знищивши чи пошкодивши доказову інформацію.

Оскільки засоби інформаційних комп'ютерних технологій постійно змінюються та вдосконалюються, це може спричинювати зміну та розміщення електронних слідів вчинення зазначених кримінальних правопорушень, тому обов'язково необхідно під час проведення слідчих (розшукових) дій у зазначених кримінальних правопорушеннях залучати спеціаліста.

З огляду на характер електронних слідів, не можемо оминути дискусії вітчизняних науковців з приводу використання їх як електронних доказів у кримінальному провадженні [10; 18, с. 451; 35, с. 5; 245, с. 16; 294; 304, с. 261; 314; 319, с. 283].

Хоча в КПК України не міститься визначення «електронних доказів», проте його використовують у Кодексі адміністративного судочинства України,

Господарському процесуальному та Цивільному процесуальному кодексах України.

У науковій літературі обґрунтовують думку про необхідність внесення обов'язкових положень у КПК України, що будуть визначати особливості «електронних доказів» у кримінальному провадженні.

Слід зауважити, що імплементація такої категорії, як «електронні докази», у кримінальне процесуальне законодавство України має відбуватися комплексно, з обов'язковим урахуванням досвіду іноземних країн.

У цьому контексті О. Ю. Костюченко й Н. М. Ахтирська слушно пропонують на законодавчому рівні визначити поняття електронних доказів, їх види, способи збирання, оцінку та використання на рівні спеціального закону (наприклад, Закону України «Про електронні докази») [10, с. 198].

Створення такого спеціального закону дасть змогу систематизувати національне процесуальне законодавство щодо питань збору та використання електронних доказів як єдиного правового механізму.

Не маючи за мету розгляд думок вчених стосовно визначення дефініції електронних доказів, вважаємо слушною думку, що електронними доказами є доказова інформація, що зберігається в електронному (цифровому) вигляді [268, с. 7].

З криміналістичної позиції головне – визначити, яка саме доказова інформація може бути електронним доказом, як вона створюється, фіксується та використовується, а також на яких саме джерелах (засобах) вона може знаходитися.

Тому, на нашу думку, важливим є чітке процесуальне визначення, які саме засоби інформаційних комп'ютерних технологій чи носії інформації можуть бути джерелами електронних доказів, а також у якій формі в них може зберігатися електронна інформація.

З огляду на національне законодавство [175; 176; 178; 179; 188], особливості засобів інформаційних комп'ютерних технологій, формою електронної інформації, що міститься на засобі інформаційних комп'ютерних технологій, а також може бути використана як електронний доказ у кримінальних правопорушеннях, що

вчиняються з використанням інформаційних комп'ютерних технологій, може бути: 1) файл; 2) електронний документ; 3) вебсайт; 4) вебсторінка; 5) електронна печатка й електронний підпис (зокрема вдосконалені); 6) інформаційна (автоматизована) система й інформаційно-комунікаційна система; 7) база даних (компіляція даних); 8) аудіовізуальні та музичні твори, відеограми (відео), фонограма, фото; 9) комп'ютерні програми; 10) віртуальний актив.

Отже, питання електронних доказів у національному кримінальному провадженні залишається дискусійним. Імплементація «електронних доказів» у кримінальне процесуальне законодавство України потребує окремого дослідження та законодавчого врегулювання.

2.3. Обстановка й особа, яка вчинила кримінальне правопорушення з використанням інформаційних комп'ютерних технологій

Обстановку кримінального правопорушення вивчають різні юридичні науки. Кримінальне право розглядає обстановку як елемент кримінально-правової характеристики кримінальних правопорушень; кримінологія – з позицій запобігання злочинності; кримінальне процесуальне право – у межах предмета доказування. Криміналістична наука розглядає обстановку як елемент криміналістичної характеристики, що вивчає середовище, у якому вчиняють кримінальне правопорушення [141, с. 360].

Обстановка в зазначених протиправних діяннях має вагоме науково-практичне значення для ефективного проведення розслідування кримінальних кіберправопорушень, хоча деякі вчені-криміналісти у своїх дослідженнях, що стосуються розслідування окреслених кримінальних правопорушень, не зосереджують увагу на цьому криміналістичному елементі [112; 134; 217].

Розглядаючи поняття обстановки кримінального правопорушення, цілком слушно зауважує В. А. Динту, слід розрізняти поняття «обстановка вчинення кримінального правопорушення» та «обстановка кримінального правопорушення» як частину й ціле, оскільки обстановка кримінального правопорушення включає

обстановку, у якій готувалося, вчинялося та приховувалося кримінальне правопорушення. Отже, поняття «обстановка вчинення кримінального правопорушення» за змістом є вужчим, ніж поняття «обстановка кримінального правопорушення», і є складовою останнього [64, с. 8].

Аналізуючи включення певних елементів у зміст обстановки, їх обсяг і вплив, вважає В. М. Шевчук, будуть різними залежно від кримінального правопорушення, оскільки для одних істотне значення мають кліматичні умови, для інших – виробничі чинники, географічне розташування місця вчинення кримінального правопорушення тощо. Основним критерієм характеристики обстановки вчинення кримінального правопорушення мають бути обставини, що позначаються на перебігу кримінального правопорушення та які враховує злочинець для його успішного вчинення [253, с. 966–967].

Обґрунтованою є думка В. А. Динту, «що структуру обстановки кримінального правопорушення становлять матеріальне, мікросоціальне та морально-психологічне середовища, що у своїй сукупності являють собою систему взаємопов’язаних і взаємообумовлених елементів» [64, с. 8].

Своєю чергою особливістю кримінальних правопорушень, вчинених з використанням інформаційних комп’ютерних технологій, є вчинення їх у кіберпросторі, що необхідно враховувати під час дослідження їх обстановки.

Тому доцільно розглядати комбіновану обстановку зазначених кримінальних правопорушень, до структури якої належать кіберпростір й об’єктивна матеріальна обстановка, оскільки для вчинення цієї категорії кримінальних правопорушень злочинець використовує об’єкти реального світу, поєднуючи їх з елементами кіберпростору [65, с. 73].

Убачається, що в структурі обстановки зазначених кримінальних правопорушень, з огляду на їх особливості, слід виокремлювати: 1) кіберпростір, що характеризується місцем, часом, віртуальною взаємодією учасників кримінального правопорушення; 2) матеріальне середовище – ділянка території, сукупність різних предметів, поведінка учасників події, психологічні взаємовідносини.

Під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, важливе значення має інформація про ймовірне місце та час його вчинення. Для слідчого значущим є встановлення місця вчинення кримінального правопорушення, що допомагає встановити місцезнаходження можливих доказів і коло осіб, причетних до його вчинення. Час вчинення дає змогу визначити, у якій саме послідовності здійснювали злочинні дії та яка їх тривалість [141, с. 360].

Ураховуючи специфіку вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, можна виокремити місця їх вчинення: фізичне середовище (ділянка місцевості) та кіберпростір (електронне середовище), де розміщені:

– інформаційні комп'ютерні технології (носії інформації), що зазнали злочинного впливу, і точки їхнього доступу до певних мереж;

– інформаційні комп'ютерні технології, які злочинець використовував, і точки їх доступу до певних мереж;

– мережеві вузли каналів зв'язку, з використанням яких відбувався обмін інформацією між засобами інформаційно-комп'ютерних технологій злочинця та потерпілого [27, с. 72–73].

Загалом кіберпростір як місце обстановки зазначених кримінальних правопорушень можна розглядати як: 1) середовище, у якому телекомунікаційна мережа, комп'ютерна система чи інші елементи можуть бути використані як знаряддя досягнення протиправної мети (наприклад, порушення нормального функціонування цього середовища, заволодіння об'єктами інтелектуальної власності, матеріальними цінностями, платіжними засобами; 2) специфічна обстановка, яка зазнала змін унаслідок правопорушення, що можуть бути джерелами доказів у кримінальному провадженні [220, с. 181].

Розглядаючи вибір фізичного середовища злочинцем, ми поділяємо думку О. І. Мотляха, що злочинці переважно обирають такі місця: 1) адміністративні та службові приміщення; 2) власні й орендовані житлові приміщення (офіси,

квартири, кімнати); 3) приміщення комунальної власності або ж споріднені з ними [138, с. 64].

Необхідно зазначити, що суттєва особливість цих протиправних діянь полягає в тому, що для них немає просторового обмеження, тож вчинення кримінального правопорушення може виходити за межі однієї держави. Кримінальне правопорушення вчиняють в одній державі, а негативні наслідки настають в іншій. Такі кримінальні правопорушення стають транснаціональними. Тобто головною ознакою їх є наявність іноземного елемента в криміналістичній характеристиці та кримінально-процесуальних відносинах під час його розслідування [112, с. 873–874].

Слушно зазначають П. Д. Біленчук, А. В. Кофанов, О. Л. Кобилянський та Є. П. Паніотов, що для визначення кримінального правопорушення як транснаціонального необхідно зауважити про таке:

– громадянство злочинця, оскільки для кожної держави вчинене кримінальне правопорушення є транснаціональним, якщо воно вчинене іноземцем (і не тільки ним);

– професіоналізм транснаціональної злочинності розглядають як високий рівень володіння злочинною майстерністю, постійне зайняття злочинною діяльності з метою отримання доходів;

– динаміку кримінального правопорушення, оскільки особи, що вчиняють транснаціональні кримінальні правопорушення, можуть пересуватися з однієї країни до іншої та не мати постійного місця проживання [23, с. 11].

У деяких випадках така динаміка є основою для вчинення зазначених кримінальних правопорушень. Наприклад, навмисне використання часових меж злочинцем, коли він учиняє протиправні дії, перебуваючи в одній країні, де денний час доби, а потерпілий – в іншій країні, де нічний час доби.

Зокрема, 16 березня 2020 року в нічний час Міністерство охорони здоров’я і соціальних служб США зазнало кібератаки, імовірно вчиненої іноземцями, метою яких було підірвати відповідь відомства на пандемію коронавірусу [139].

В Україні в ніч із 13-го на 14 січня 2022 року вчинено кібератаку на державні інформаційні ресурси, що була спрямована на завдання шкоди інфраструктурі державних електронних ресурсів [41].

Тому для кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, важливим є дослідження і встановлення часу його вчинення.

Досліджуючи криміналістичну структуру часу, М. В. Салтевський та В. М. Мєшков стверджували, що в її складі є: момент часу, фактор часу та часове відношення. Момент часу в криміналістичному розумінні – точка відліку, що фіксує початок, закінчення або розвиток процесів і явищ, наприклад, початок кримінального діяння. Фактор часу – часова характеристика тривалості події чи явища: швидкість руху в просторі, швидкість розвитку та протікання певних процесів. Часове відношення – характеристика певного ряду події чи явищ, їх послідовність і хронологічність виникнення, розвитку та закінчення (яка подія відбулася першою, яка послідовність дій злочинця тощо) [213, с. 31–32].

З огляду на зазначене, можна стверджувати, що моментом часу кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, є початок злочинних дій у кіберпросторі. Фактором часу слугує тривалість певної протиправної події, наприклад, час тривалості DDoS атаки або час знаходження шкідливої програми в засобах інформаційно-комп'ютерних технологій. Часовим відношенням можна вважати початок виходу злочинцем у кіберпростір і вчинення протиправних дій, наприклад, відкриття певного сайту та розміщення на ньому матеріалів, що пропагують культ насильства.

Слід зауважити, що встановлення часу вчинення кримінального правопорушення зазначеної категорії не становить істотних проблем, оскільки операційна система засобу інформаційно-комп'ютерних технологій детально фіксує кожну операцію (створення чи видалення файлу тощо).

Проте є випадки, коли час вчинення зазначеного кримінального правопорушення встановити неможливо. Це може бути зумовлено технічними причинами, зокрема, коли під час перезавантаження засобу інформаційно-

комп’ютерних технологій цілком або частково обнуляються чи стираються дані тощо. У таких випадках час вчинення необхідно встановлювати за допомогою спеціаліста або шляхом проведення судової комп’ютерно-технічної експертизи. Крім того, час вчинення кримінальних правопорушень, вчинених з використанням інформаційних комп’ютерних технологій, можна встановити проведенням слідчих (розшукових) дій [141, с. 361–361].

Виокремимо характерні особливості часу вчинення кримінальних правопорушень з використанням інформаційних комп’ютерних технологій:

1) час вчинення та час настання злочинних наслідків може суттєво відрізнятися у зв’язку з місцеперебуванням злочинця та потерпілого;

2) потерпілий не завжди здатен помітити вчасно наслідки вчинення зазначених протиправних діянь, тому може подовжитися часове відношення між вчиненням і викриттям кримінального правопорушення;

3) час вчинення дає змогу відтворити фізичний та віртуальний алгоритми дій між злочинцями, а також їх фізичну та віртуальну взаємодію;

4) розуміння моменту часу, фактору часу та часового відношення нададуть можливість слідчому зрозуміти обстановку зазначених протиправних діянь.

Слід зазначити, що віртуальною взаємодією учасників кримінальних правопорушень, вчинених з використанням інформаційних комп’ютерних технологій, слід вважати їх спільні дії в кіберпросторі. Наприклад, особи домовилися вчинити певні протиправні дії у відповідний день і час, використовуючи для цього допоміжні програми, у яких узгоджують свої дії (Telegram, Viber, Discord тощо). Реальною взаємодією учасників, що вчиняють зазначені категорії кримінальних правопорушень, вважають їх контакт у фізичному середовищі [141, с. 361–362].

Отже, розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій, у більшості випадків розпочинається зі сприйняття і дослідження обстановки. З’ясування обстановки зазначеного кримінального правопорушення допомагає слідчому сформулювати

слідчі версії, а також встановити суб'єкта (суб'єктів) його вчинення (особу злочинця) [141, с. 361–362].

Важливу роль у структурі криміналістичної характеристики зазначених кримінальних правопорушень відіграє особа злочинця (особа кіберзлочинця), яку досліджують різні юридичні науки.

Кримінологія вивчає особу злочинця з позицій профілактики кримінальних правопорушень; кримінальне право – з погляду кваліфікації кримінальних правопорушень; кримінальний процес – для встановлення віку особи та проведення відповідних процесуальних дій; психологічна наука своєю чергою вивчає поведінку таких осіб. Криміналістична наука вивчає особу злочинця з позицій розслідування кримінальних правопорушень [142, с. 204].

Засновником вчення про особу злочинця в криміналістичному аспекті вважають австрійського вченого Г. Гросса, який у своїх працях досліджував «знання людей» і стверджував, що важливою умовою «точної» діяльності слідчого є ґрунтовне знання людини як головного матеріалу слідства [47, с. 44]. На прикладі злочинців-ромів науковець здійснив аналіз їх характерних властивостей: уміння шпигувати, відсутність прагнення до влади й відчуття сорому, лінь, любов до життя тощо. Дослідження Г. Гросса стали науковим підґрунтям для вивчення особи злочинця.

На переконання А. В. Старушевича, вчення про особу злочинця пройшло певні історичні періоди становлення:

– період становлення криміналістичних знань (кінець XIX – початок XX ст.). Вивчали такі риси особи злочинця, як біологічні (риси зовнішності, папілярні візерунки, різні сліди відображення тощо) і психологічні особливості особи;

– період становлення криміналістики (1918–1930). Питання дослідження особи злочинця розглядали в працях вітчизняних й іноземних криміналістів;

– період із 40-х до 70-х років XX століття. Положення, що стосуються соматичних властивостей особи, стали основою для розділів криміналістичної техніки, їх почали враховувати під час розроблення тактики окремих слідчих дій, наприклад, тактики огляду місця події, тактики пред'явлення для впізнання тощо.

Психологічні особливості особи враховували під час розроблення питань криміналістичної тактики: побудови версій, тактики допиту, тактики очної ставки, для розв'язання організаційних проблем тощо;

– період із 70-х років XX ст. і донині, коли дані про особу злочинця долучено як органічний елемент у зміст різних окремих криміналістичних теорій; почалося формування криміналістичного вчення про особу злочинця як самостійну окрему криміналістичну теорію [231, с. 22–23].

Слід зауважити, що у вітчизняній криміналістичній літературі вивчення особи «комп'ютерного злочинця» починається в 90-х роках минулого століття. Зокрема, вагомий науковий внесок у дослідження «комп'ютерного злочинця» зробив П. Д. Біленчук у працях «Криміналістична характеристика портрета комп'ютерного злочинця» (1994) [19, с. 260–262] і «Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти» (у співавторстві з М. А. Зубань) [21, с. 15–17]. Надалі 1997 року з'являється перше в Україні окреме криміналістичне дослідження «Портрет комп'ютерного злочинця», у якому розглянуто поняття, характеристика та класифікація комп'ютерних злочинців [22].

Одним із перших вітчизняних науковців, хто започаткував використання поняття «кіберзлочинець», можна вважати В. О. Голубєва, який у своєму дослідженні «Розслідування комп'ютерних злочинів» використав цей термін, проте не висвітлив його [51, с. 4–5].

Аналізуючи дефініцію поняття «особа злочинця», слід зауважити, що в криміналістичній літературі є різні підходи до його визначення.

Обґрунтованою видається думка В. Ю. Шепітька, який зазначає, що особа злочинця – це поняття, що виражає сутність особи, яка вчинила кримінальне правопорушення, й охоплює дані демографічного характеру, деякі моральні властивості, а також психологічні особливості [114, с. 15–16].

Щодо загальних криміналістичних ознак особи злочинця прийнятною є думка В. М. Шевчука, який виокремлює: 1) біологічні: стать, вік, фізичні дані, зріст, вага, особливі прикмети тощо; 2) психологічні: світогляд, переконання, знання,

навички, емоції, почуття, темперамент тощо; 3) соціальні: соціальне становище, освіта, національність, сімейний стан, професія тощо [253, с. 978].

Залежно від виду вчиненого кримінального правопорушення вчені-криміналісти виокремлюють типові ознаки особи, що його вчинила (особи злочинця).

Слушно зазначають П. Д. Біленчук, Д. П. Біленчук та О. І. Котляревський про те, що потрібно вивчати «професійні» звички злочинців, які виявляються переважно в певних способах і прийомах вчинення кримінальних правопорушень, характерному «почерку» злочинця, які залишаються на місці вчинення кримінальних правопорушень, оскільки результати кожної злочинної діяльності містять сліди людини, яка їх залишила. Саме виявлення на місці вчинення кримінального правопорушення речових доказів дає змогу визначити деякі особисті соціально-психологічні ознаки злочинця, його досвід, професію, соціальні знання, стать, вік, особливості взаємодії з потерпілим [20, с. 367].

Слід зауважити, що в криміналістичному аспекті особа сучасного кіберзлочинця має індивідуальну специфіку, обумовлену наявністю в таких осіб спеціальних знань і навичок з використання інформаційних комп'ютерних технологій для досягнення злочинного наміру, а отже, за певними притаманними ознаками, властивими більшості з них, можна виявляти цю категорію кіберзлочинців [142, с. 203].

У криміналістичній літературі поділ кіберзлочинців відбувається залежно від рівня професійної підготовки та соціального становища. В узагальненому вигляді може йтися про такі види кіберзлочинців [12, с. 98–101; 112, с. 875; 134, с. 297–299]:

– хакерів – особи, які можуть здійснювати різні маніпуляції з програмним кодом;

– шпигунів, які вчиняють незаконне проникнення до інформаційних систем з метою одержання інформації, що можна буде використана з політичною, військовою, економічною метою;

– терористів – зламують програми для створення ефекту небезпеки, що може бути використана для політичного впливу;

– корисливих злочинців – особи, які проникають в інформаційні системи задля одержання особистої немайнової та майнової вигоди;

– вандалів (шкідники, комп'ютерні маніяки) – особи, які зламують інформаційні системи для одержання задоволення від завданої шкоди;

– психічно хворих – особи, які страждають на новий вид психічних розладів: інформаційні хвороби або комп'ютерні фобії;

– піратів – особи, які порушують авторське право, створюючи незаконні копії програм та інформаційних даних;

– вірус-мейкерів – створюють шкідливі програмні забезпечення для збуту чи розповсюдження;

– кардерів – викрадають кошти з банківських рахунків (кредитних карток);

– іноземних розвідувальних спецслужб, що використовують кібероснащення як один із засобів здійснення своєї шпигунської діяльності (одержання доступу до державних таємниць і конфіденційної інформації іншої держави тощо).

Проте в криміналістичній науці головним постає питання, який комплекс значущих криміналістичних ознак, що вказують на особу кіберзлочинця, необхідно виокремлювати, оскільки серед науковців не сформовано єдиного підходу щодо цього питання [83, с. 76; 147; 217, с. 115].

На нашу думку, типовими ознаками, що характеризують особу кіберзлочинця, можуть бути такі: 1) загальні (вік, освіта, професія); 2) психологічні (темперамент, характер, інтереси та схильності, мотиви і стиль поведінки, певні психічні відхилення); 3) спеціальні («професійні звички» та «почерк» кіберзлочинця) [142, с. 207]. Розглянемо детальніше кожну з них.

Загальні ознаки особи кіберзлочинця є початковим орієнтиром для органу досудового розслідування. Освіта і професія кіберзлочинця дають змогу слідчому з'ясувати, якими спеціальними знаннями може володіти особа (знання програмування, розуміння роботи обладнання тощо). Вік має здебільшого процесуальне значення, однак є допоміжною ознакою, оскільки можна визначити

коло осіб і висунути версії стосовно мотиву вчинення зазначених протиправних діянь [142, с. 207].

Натомість психологічні ознаки особи кіберзлочинця допоможуть слідчому під час проведення певних процесуальних дій. Знання темпераменту, характеру, інтересів і схильностей дають змогу встановити психологічний контакт між слідчим та кіберзлочинцем під час допиту. Знаючи мотив і стиль поведінки, можна висувати версії стосовно мети вчинення кримінального правопорушення та прогнозувати подальші дії особи. Певні психічні відхилення надають можливість зрозуміти поведінку особи кіберзлочинця в соціумі, оскільки дають оцінку певним його діям [142, с. 207].

Слід зауважити, що залежно від типу темпераменту особи кіберзлочинця (сангвінік, холерик, флегматик, меланхолік) може йтися про обрання відповідної тактики проведення допиту слідчим.

Спеціальні ознаки, притаманні конкретній особі кіберзлочинця, допомагають слідчому в ідентифікації особи за її діями та залишеними слідами. Одним із таких ідентифікаторів є звичка – певний спосіб дії, життя, манера поведінки або висловлювання, схильність до чогось, що стали звичними, постійними для кого-небудь [29, с. 352].

Більшість осіб, що поширюють шкідливий контент, вчиняють такі дії в домашній обстановці й переважно в одній манері подання інформації.

«Професійною звичкою» особи кіберзлочинця слід вважати певний спосіб дії, життя, манери поведінки, висловлювання тощо, який сформувався в особи під час професійної діяльності та має відображення у формі залишених слідів [142, с. 208].

Прикладом «професійної звички» кіберзлочинця може бути використання:

– певної марки техніки (Apple, Acer, Asus тощо), якою особа звикла послуговуватися;

– конкретної операційної системи (Linux, Windows тощо);

– програм, якими особа користувалася протягом тривалого часу й віддає перевагу саме їм (браузери: Google Chrome, Mozilla Firefox, Safari, TOR тощо);

– програм (Python, JavaScript, C# тощо);

– конкретних пошукових сервісів (Google, Bing, Yahoo) чи поштових служб (Gmail, Ukrnet) [142, с. 208].

Певну інформацію про «професійні звички» особи кіберзлочинця слідчому також можна отримати з аналізу його файлів, використавши сервіси VirusTotal або Hybrid Analysis, що допоможуть встановити тип файлу, мову програмування, місце, час і дату створення тощо.

На відміну від «професійної звички», «почерк» кіберзлочинця – це характерна дія, яку особа свідомо вчиняє, розуміючи, що цим вона виокремлює себе серед інших. Зокрема, це: вибір псевдоніма, конкретної фотокартки (аватарки), стиль залишення та написання повідомлень тощо. Варто зазначити, що вибір псевдоніма чи аватарки засвідчує певні вподобання певних осіб [142, с. 208].

Наприклад, американський хакер А. Ламо послуговувався комп'ютерами загального користування та завжди мав псевдонім «Homeless hacker» («бездомний хакер») [123].

Хакерська організація «Анонімус» використовує фотокартку костюма зі знаком питання замість голови, що символізує анонімність і вказує на відсутність чітко вираженого лідера [6].

Отримати певну інформацію можна із залишеного повідомлення кіберзлочинця. Зокрема, вчинивши масштабну кібератаку на урядові сайти України в ніч із 13-го на 14 січня 2022 року, хакери залишили повідомлення трьома мовами – українською, російською та польською про нібито масовий злив персональних даних [243]. Це повідомлення дало змогу висунути певні слідчі версії щодо ймовірних осіб вчинення зазначеного протиправного діяння

Слід зауважити, що більшість учених-криміналістів не зосереджують належної уваги на дослідженні особи неповнолітнього кіберзлочинця [51; 138; 202; 217].

Водночас аналіз відомостей про кількість зареєстрованих кримінальних правопорушень за розділом XVI КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та

комп'ютерних мереж і мереж електрозв'язку» [181] засвідчує, що 2019 року з 2204 облікованих кримінальних правопорушень 9 вчинили неповнолітні особи або за їх участю, 2020 року з 2498 кримінальних правопорушень 51 – неповнолітні особи, 2021 року з 3310 – 13, 2022 року з 3415 – 6.

Статистичні дані не цілком відображають реальну кількість вчинених кримінальних правопорушень з використанням інформаційних комп'ютерних технологій неповнолітніми особами, оскільки обмежені лише розділом XVI КК України [119].

Неповнолітні особи отримують спеціальні знання та навички з використання інформаційних комп'ютерних технологій, переглядаючи відеоґайди (стислі відеоматеріали інформаційного змісту), що знаходяться у відкритому доступі, які своєю чергою сприяють виникненню в них бажання реалізувати отримані знання та вміння в реальному житті, зокрема і до вчинення протиправних діянь.

Особа неповнолітнього злочинця вирізняється незавершеністю психічного та фізичного розвитку, що виявляється в бажанні самоствердитися та самовиразитися, почутті «дорослого» й амбіційності, тому потребує особливого ставлення до його діянь та особливого спілкування [165, с. 216].

З огляду на зазначене, можна виокремити основні мотиви вчинення таких протиправних діянь неповнолітніми кіберзлочинцями.

Вчинення протиправних дій для розваги. Шкідливий програмний засіб «Silex», що, ймовірно, був створений 14-річним іранським хакером «заради розваги», упродовж кількох годин вивів з ладу кілька тисяч різних засобів інформаційно-комп'ютерних технологій [262].

Вчинення протиправних дій для отримання прибутку. Наприклад, кіберполіція України 2020 року викрила 16-річного жителя Донеччини, який, маючи відповідні знання та навички у сфері програмування, самостійно створив шкідливий програмний засіб (вірус), що міг викрадати інформацію. Цю шкідливу програму особа продавала в месенджерах за 300 грн [87].

Вчинення протиправних дій, щоб самоствердитися чи самовиразитися. Лондонська поліція 2022 року виявила хлопця віком 17 років, який входив до

складу хакерського угруповання, що брало участь у взломі компаній «Rockstar Games» та «Uber». Неповнолітній виклав у мережу викрадений архів з відеофайлами та вихідним кодом комп'ютерної гри «GTA 6», на розробку якої витратили 2 млрд доларів. Також він атакував систему компанії «Uber», отримавши доступ до листування та електронних адрес. Неповнолітнього злочинця вдалося викрити через використання ідентичних методів злому [242].

Отже, особу неповнолітнього кіберзлочинця слід вивчати детальніше.

На нашу думку, дослідження, пов'язані з особою неповнолітнього кіберзлочинця, необхідно здійснювати в межах зазначеної криміналістичної класифікації кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій (наприклад: «Розслідування кримінальних правопорушень у сфері власності, вчинених з використанням інформаційних комп'ютерних технологій неповнолітніми особами» тощо).

Зауважимо, що слідчому сприятиме виокремлення всіх наявних ознак особи кіберзлочинця в електронну базу осіб, які вчинили кримінальні правопорушення з використанням інформаційних комп'ютерних технологій. До електронної бази слід відносити такі відомості: вік, освіта, професія, встановлені психологічні ознаки, а також «професійні (злочинні) звички» і «почерк кіберзлочинця». Електронна база буде слугувати ідентифікатором для слідчого, а також допоможе виокремити відмітні ознаки кіберзлочинців.

Отже, у криміналістичній характеристиці кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, особою сучасного кіберзлочинця слід вважати систему загальних, психологічних і спеціальних ознак (даних) такої особи, що сприяють її ефективному пошуку та викриттю. З'ясування під час досудового розслідування важливих криміналістичних даних про особу кіберзлочинця є одним з основних факторів у розслідуванні кримінальних правопорушень, що вчиняються з використанням інформаційних технологій, які надають можливість слідчому говорити про обстановку зазначених кримінальних правопорушень, характерні сліди та висунення відповідних версій.

Висновки до розділу 2

Здійснене дослідження криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, дає підстави для таких висновків:

1. Найбільш значущими елементами криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, є: спосіб вчинення, типові сліди, обстановка та особа злочинця. Зазначені елементи криміналістичної характеристики цих кримінальних правопорушень знаходяться в кореляційному зв'язку (імовірних залежностях): спосіб вчинення – зі слідами вчинення, обстановка – з особою злочинця.

2. Особливість визначення елементів криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, полягає в: а) дослідженні та використанні вітчизняними вченими-криміналістами структурних елементів криміналістичної характеристики у своїх працях, що дає змогу узагальнити їх використання та обрати найбільш застосовувані елементи криміналістичної характеристики; б) аналізі криміналістичних даних про раніше вчинені кримінальні правопорушення зазначеної категорії, що дають змогу встановити кореляційні зв'язки між обраними елементами криміналістичної характеристики

3. Способом вчинення окреслених кримінальних правопорушень слід вважати сукупність послідовних дій суб'єкта (суб'єктів), що охоплюють дії з готування, вчинення та приховування, які спрямовані на досягнення певного злочинного результату з використанням інформаційних комп'ютерних технологій.

4. У більшості кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, наявні дії з підготовки та приховування, оскільки їх не можуть вчиняти раптово, вони потребують необхідних технічних знань і навичок, тобто певної підготовки.

Під час використання інформаційних комп'ютерних технологій з метою вчинення кримінального правопорушення в зловмисника формується розуміння, що його буде складно встановити, оскільки він вчиняє протиправні дії віддалено, а засіб інформаційних комп'ютерних технологій дозволяє приховати себе.

5. Достатньо складно виокремити всі способи вчинення цих кримінальних правопорушень, тому що з розвитком інформаційних комп'ютерних технологій цей вид злочинної діяльності буде стрімко змінюватися, спричиняючи виникнення нових способів. Однак, з огляду на реалії сьогодення, може йтися про найтиповіші та найпоширеніші нині способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій: 1) використання шкідливого програмного забезпечення; 2) вчинення DoS/DDoS атак; 3) несанкціонований доступ до інформації; 4) шахрайство, вчинене з використанням інформаційних комп'ютерних технологій; 5) поширення шкідливого (протиправного) контенту (спам, погрози, створення, поширення та збут дитячої порнографії, заклики до вчинення насильства, домагання тощо); 6) порушення авторських чи суміжних прав з використанням інформаційних комп'ютерних технологій; 7) комплекс способів і використання інформаційних комп'ютерних технологій як засобу користування кіберпростором для вчинення інших кримінальних правопорушень.

6. Надзвичайно важливу роль у виявленні та розслідуванні кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, відіграють знання про способи підготовки та приховування, що допомагають слідчому зрозуміти мислення злочинця, прогнозувати його подальші дії та запобігати їм.

7. Залежно від обраного злочинцем відповідного способу вчинення кримінального правопорушення з використанням інформаційних комп'ютерних технологій можна розуміти, де залишаються сліди його вчинення. Характер залишених електронних слідів залежить від таких факторів: виду операційної системи злочинця та потерпілого, особливостей засобів інформаційних комп'ютерних технологій та їх програмного забезпечення тощо. Однак під час

розслідування кримінальних правопорушень цієї категорії не слід нехтувати матеріальними й ідеальними слідами.

Засоби інформаційних комп'ютерних технологій постійно змінюються та вдосконалюються, це може спричиняти зміну та розміщення електронних слідів, тому обов'язково необхідно під час проведення слідчих (розшукових) дій залучати спеціаліста.

8. У структурі обстановки як елементу криміналістичної характеристики зазначених протиправних діянь слід виокремлювати: 1) кіберпростір, що характеризується місцем, часом, віртуальною взаємодією учасників кримінального правопорушення; 2) матеріальне середовище – ділянка території, сукупність різних предметів, поведінка учасників події, психологічні взаємовідносини.

9. Криміналістичну структуру часу кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, утворюють: момент часу, фактор часу та часове відношення. Момент часу є початок злочинних дій у кіберпросторі. Фактором часу слугує тривалість певної протиправної події. Часовим відношенням можна вважати початок виходу злочинця в кіберпростір та вчинення протиправних дій.

10. Визначено характерні особливості часу вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій : 1) час вчинення і час настання злочинних наслідків може суттєво відрізнятися у зв'язку з місцеперебуванням злочинця і потерпілого; 2) потерпілий не завжди може помітити вчасно наслідки вчинення зазначених протиправних діянь, унаслідок чого може подовжитися часове відношення між вчиненням і викриттям кримінального правопорушення; 3) час вчинення дає змогу відтворити фізичний та віртуальний алгоритми дій між злочинцями, а також їх фізичну та віртуальну взаємодію; 4) розуміння моменту часу, фактору часу та часового відношення дозволять слідчому зрозуміти обстановку зазначених протиправних діянь.

11. Віртуальною взаємодією учасників кримінальних правопорушень, вчинених із використанням інформаційних комп'ютерних технологій, слід вважати

їхні спільні дії в кіберпросторі. Реальною взаємодією учасників є їх контакт у фізичному середовищі.

12. Досліджено, що у вітчизняній криміналістичній літературі вивчення особи «комп'ютерного злочинця» розпочалося в 90-х роках минулого століття. Вагомий науковий внесок у дослідження «комп'ютерного злочинця» зробив П. Д. Біленчук у працях «Криміналістична характеристика портрета комп'ютерного злочинця» (1994), «Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти». 1997 року з'являється перше в Україні криміналістичне дослідження «Портрет комп'ютерного злочинця», у якому розглянуто поняття, характеристику та класифікацію комп'ютерних злочинців.

Одним із перших вітчизняних науковців, хто започаткував використання поняття «кіберзлочинець», можна вважати В. О. Голубєва, який у своєму дослідженні «Розслідування комп'ютерних злочинів» використав цей термін, проте не висвітлив його.

13. Типовими ознаками, що характеризують особу кіберзлочинця, є: 1) загальні (вік, освіта, професія); 2) психологічні (темперамент, характер, інтереси та схильності, мотиви і стиль поведінки, певні психічні відхилення); 3) спеціальні («професійні звички» та «почерк» кіберзлочинця).

14. Увагу зосереджено на особі неповнолітнього кіберзлочинця, зокрема розглянуто такі мотиви вчинення ними зазначених протиправних діянь: вчинення протиправних дій для розваги; вчинення протиправних дій для отримання прибутку; вчинення протиправних дій, щоб самоствердитися або самовиразитися.

15. Запропоновано виокремити всі наявні ознаки особи кіберзлочинця в електронну базу осіб, які вчинили кримінальні правопорушення з використанням інформаційних комп'ютерних технологій. До електронної бази слід відносити такі відомості: вік, освіта, професія, встановлені психологічні ознаки, а також «професійні (злочинні) звички» та «почерк кіберзлочинця».

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

3.1. Слідчі ситуації розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Проведення розслідування конкретного кримінального правопорушення потребує певного проміжку часу, має початок і завершення. Однак серед науковців не сформувався єдиний підхід стосовно того, на які етапи слід поділяти процес розслідування. Дискусії з цього питання розгорнулися у зв'язку з прийняттям 2012 року КПК України [121], що привернуло увагу вчених-криміналістів до періодизації (етапізації) розслідування кримінальних правопорушень [73].

На переконання О. А Самойленко, періодизація процесу розслідування має передбачати два етапи: початковий і наступний [217, с. 207–208].

Іншу позицію обстоює Ю. М. Чорноус, яка розглядає три етапи – початковий, наступний та заключний [110, с. 306].

На наш погляд, такою, що в цілком охоплює процес розслідування кримінальних правопорушень, вчинених з використанням інформаційних комп'ютерних технологій, є періодизація, запропонована В. А. Журавлем. Учений виокремлює такі етапи досудового розслідування:

1) вихідний;

2) початковий;

3) наступний;

4) завершальний [73, с. 141–142].

Першим етапом розслідування є *вихідний*, що триває до моменту внесення відомостей до ЄРДР [73, с. 142]. Відомостями про вчинення ймовірного

кримінального правопорушення, слушно зазначає Н. М. Ахтирська, є інформація, що може надходити:

– від фізичних осіб (заявників, потерпілих), юридичних осіб і медіа;

– за результатами аналізу медіа;

– від правоохоронних органів і внаслідок самостійного виявлення з будь-якого джерела обставин, зокрема й мережі Інтернет;

– під час розслідування інших кримінальних правопорушень;

– унаслідок надходження інформації на запит від запитуваної держави;

– у результаті добровільного надання інформації іноземною державою без надсилання запиту;

– на підставі інформації, що надходить міжнародними каналами Інтерполу, Європолу;

– як результат звернення правоохоронних органів до громадян з повідомленням про вчинення певного кримінального правопорушення та проханням повідомити щодо цього відому інформацію [12, с. 149].

Важливим на цьому етапі є саме момент внесення відомостей про кримінальне правопорушення до ЄРДР, оскільки він має певні процесуальні особливості. Згідно з правовою позицією Касаційного кримінального суду у складі Верховного суду, викладеною в постанові від 30 вересня 2021 року, підставою початку досудового розслідування є лише ті заяви та повідомлення, з яких вбачаються вагомі обставини, що можуть свідчити про вчинення кримінального правопорушення. Анонімну заяву як підставу для відкриття кримінального провадження не реєструють, вона лише є підставою для перевірки інформації, що в ній викладена, після чого відомості до ЄРДР може бути внесено за рапортом працівника поліції, який встановив наявність ознак кримінального правопорушення в заяві чи повідомленні. Водночас після прийняття заяви чи повідомлення про кримінальне правопорушення, слідчий, прокурор, з огляду на їх зміст, має перевірити ці дані, що можуть свідчити про вчинення кримінального правопорушення, за наслідками чого приймає рішення про початок досудового розслідування шляхом внесення відповідних відомостей до ЄРДР [172].

Слід зауважити, що в невідкладних випадках до внесення відомостей до ЄРДР може бути проведено огляд місця події (відомості вносять невідкладно в ЄРДР після його завершення).

Крім цього, згідно з ч. 3 ст. 214 КПК України, для з'ясування обставин вчинення кримінального проступку, до внесення відомостей до ЄРДР, можуть здійснювати: відбір пояснення, проведення медичного освідування, отримання висновку спеціаліста, зняття показань технічних приладів і технічних засобів, вилучення знарядь і засобів вчинення кримінального правопорушення, речей та документів, що є безпосереднім предметом кримінального проступку або які виявлені під час затримання особи, особистого огляду або огляду речей.

Відповідно до положень ст. 60, 214 КПК України, суб'єктами на вихідному етапі є: слідчий, дізнавач, прокурор, заявник та ін.

З огляду на викладене, цілком обґрунтовано виокремлювати вихідний етап у кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій.

Другий етап розслідування – *початковий*, що розпочинається з моменту внесення відомостей до ЄРДР і закінчується оголошенням особі підозри у вчиненні кримінального правопорушення [73].

На цьому етапі виконують такі завдання: 1) встановлення наявності чи відсутності події кримінального правопорушення (час, місце, спосіб, обстановка та інші обставини вчинення кримінального правопорушення); 2) встановлення складу кримінального правопорушення; 3) встановлення фактичних даних, що вказують на конкретну особу, яка могла вчинити кримінальне правопорушення; 4) застосування певних заходів забезпечення кримінального провадження (виклик слідчим, дізнавачем, прокурором; накладення грошового стягнення тощо) [217, с. 207–208].

Слушно стверджує В. А. Журавель, що початковий етап досудового розслідування, його межі, характер тактичних завдань також залежать від обставин відкриття кримінального провадження, зокрема: 1) провадження відкрито за фактом виявлення події, коли ще не встановлено особу, причетну до його вчинення

(підозрюваного); 2) провадження відкрито щодо конкретної особи, зокрема на підставі її затримання в порядку ст. 207, 208 КПК України [73, с. 143].

Поділяючи таке твердження, вбачаємо, що з процесуальної позиції повідомлення про підозру здійснюють у випадках, передбачених ст. 276 КПК України, а саме: 1) затримання особи на місці вчинення кримінального правопорушення чи безпосередньо після його вчинення; 2) обрання до особи запобіжного заходу; 3) наявності достатніх доказів для підозри особи у вчиненні кримінального правопорушення. Порядок повідомлення особі про підозру визначено в ст. 278 КПК України [121].

Підсумовуючи, можна дійти висновку, що оскільки закінчення початкового етапу залежить від оголошення особі повідомлення про підозру в спосіб, передбачений КПК, це позначається на тривалості цього етапу, а також на обсягу проведення необхідних слідчих (розшукових) дій цього й наступного етапів.

Варто зазначити, що на даному етапі виникають права й обов'язки потерпілої особи, з моменту подання нею заяви про вчинення кримінального правопорушення або заяви про залучення її до провадження як потерпілого [258, с. 21].

Після вручення письмового повідомлення про підозру розпочинається *наступний етап* розслідування.

З огляду на особливості щодо відкриття кримінального провадження та повідомлення особі про підозру, про що зазначено в попередньому етапі, продовжують проводити певний обсяг слідчих (розшукових) дій, спрямованих на збирання доказів.

Головним для слідчого на цьому етапі є доведення причетності особи, якій повідомлено про підозру, до вчиненого кримінального правопорушення та підтвердження обґрунтованості повідомлення про підозру [73, с. 143].

Завданнями цього етапу є встановлення:

– злочинної діяльності в повному обсязі;

– характеру й тяжкості обвинувачення щодо кожного суб'єкта кримінального правопорушення (зміна повідомлення про підозру);

– характеристики особи, яку підозрюють у вчиненні кримінального правопорушення;

– інших обставин, що можуть бути враховані під час вирішення питання про укладення угоди про визнання винуватості тощо [217, с. 208].

Цей етап триває з моменту повідомлення про підозру до прийняття рішення про завершення розслідування в порядку ст. 283 КПК України.

На *завершальному етапі* розслідування здійснюють аналіз та оцінку зібраних під час досудового розслідування доказів. На їх підставі встановлюють наявність чи відсутність фактів й обставин, що можуть мати значення для прийняття рішення в кримінальному провадженні.

Надалі, відповідно до положень ст. 283 КПК України [121], прокурор зобов'язаний у найкоротший строк після повідомлення особі про підозру здійснити одну з таких дій:

1) закрити кримінальне провадження;

2) звернутися до суду з клопотанням про звільнення особи від кримінальної відповідальності;

3) звернутися до суду з обвинувальним актом, клопотанням про застосування примусових заходів медичного чи виховного характеру.

Отже, поділ процесу розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, на чотири етапи позначається насамперед на формуванні слідчих ситуацій, що забезпечує ефективність проведення досудового розслідування зазначеної категорії кримінальних правопорушень.

Слідчі ситуації мають особливе теоретичне та практичне значення під час розслідування кримінальних кіберправопорушень.

У криміналістичній літературі є чимало підходів до визначення, складу та видів слідчих ситуацій [30; 32; 152, с. 814–822].

З цього приводу слушно зазначає О. І. Мотлях, що погляди науковців збігаються в тому, що роль слідчих ситуацій слугує розробленню ефективної організації розслідування та її методики [138, с. 84].

Аналізуючи криміналістичні дослідження щодо визначення поняття слідчих ситуацій, В. П. Бахін стверджує, що це сукупність даних про подію кримінального правопорушення та обставини, що характеризують обстановку на конкретному етапі розслідування [229, с. 19].

Слід зазначити, що для вирішення слідчої ситуації, яка склалася на конкретному етапі розслідування, визначають її тактичне завдання.

Зокрема, тактичним завданням слід вважати перелік завдань, притаманних конкретному етапу розслідування, що формується на підставі предмета доказування з огляду на слідчі ситуації [205, с. 158], для вирішення яких проводять відповідну процесуальну дію.

Учені пропонують таку класифікацію слідчих ситуацій:

1. За часом виникнення в процесі розслідування:

– вихідні (виникають до моменту внесення відомостей до ЄРДР);

– початкові (виникають на початку кримінального провадження);

– наступні (притаманні наступному етапу кримінального провадження);

– заключні (виникають на заключному етапі кримінального провадження під час оцінки його результатів).

2. За відносинами між учасниками:

– конфліктні (якщо між учасниками складаються відносини протидії чи їх інтереси не збігаються);

– безконфліктні (повний або частковий збіг інтересів учасників);

3. За відношенням до досягнення мети розслідування:

– сприятливі (наявність достатньої інформації);

– несприятливі (відсутність достатньої інформації, необхідність прийняття додаткових тактичних рішень, збирання інформації).

4. За ступенем спільності:

– типові (притаманні переважній більшості кримінальних правопорушень);

– специфічні (складаються за особливого збігу обставин) [110, с. 307].

У більшості вітчизняних досліджень, що стосувалися розслідування кримінальних правопорушень, які вчиняють з використанням інформаційних

комп'ютерних технологій, акцентують саме на слідчих ситуаціях початкового етапу розслідування, натомість інші етапи розслідування залишаються поза увагою.

Розглянемо типові слідчі ситуації чотирьох етапів розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Типові слідчі ситуації, що можуть виникати на вихідному етапі розслідування зазначених кримінальних правопорушень, на наш погляд, можна класифікувати на:

1. Ситуації, коли є заява потерпілого чи повідомлення особи про вчинене кримінальне правопорушення.

2. Ситуації, коли було виявлено з інших джерел обставини, що можуть свідчити про вчинення кримінального правопорушення.

Ситуація 1 за відношенням до досягнення мети може бути сприятливою або несприятливою. Сприятливою є ситуація, коли особа, яка звертається із заявою, повідомленням про вчинене кримінальне правопорушення, надає додаткову інформацію про обставини, особу злочинця, докази вчинення кримінального правопорушення, а також іншу інформацію, що буде слугувати підставою для внесення відомостей до ЄРДР і початку досудового розслідування. Також сприятливою є ситуація, коли особа звернулася із «каяттям».

Несприятливою є ситуація, коли немає відомостей про особу злочинця та недостатньо даних про обставини вчинення кримінального правопорушення.

У *ситуації 2* перелік інших джерел, з яких виявлено обставини, що можуть свідчити про вчинення кримінального правопорушення, міститься в додатку 7 до Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, затвердженого наказом Офісу Генерального прокурора 30 червня 2020 року № 298, довідник 1 [187].

Тактичними завданнями в заданих ситуаціях можуть бути: 1) прийняття та реєстрація заяви, повідомлення, а також інші джерела, з яких виявлені обставини, що можуть свідчити про вчинене кримінальне правопорушення; 2) перевірка

достатності даних, що можуть засвідчувати вчинення кримінального правопорушення; 3) визначення зі спеціалістом щодо отримання висновку (у кримінальних проступках); 4) невідкладне внесення відповідних відомостей до ЄРДР;

У заданих ситуаціях можуть проводити такі процесуальні дії:

– огляд місця події (ч. 3 ст. 214 КПК України);

– відбір пояснень (для кримінальних проступків) (п. 1 ч. 3 ст. 214 КПК України);

– отримання висновку спеціаліста, зняття показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису (для кримінальних проступків) (п. 3 ч. 3 ст. 214 КПК України);

– вилучення знарядь і засобів, речей і документів, що є безпосереднім предметом або які виявлені під час затримання особи, особистого огляду або огляду речей (для кримінальних проступків) (п. 4 ч. 3 ст. 214 КПК України);

– опитувань осіб за їх згодою; відвідування жилих та інших приміщень за згодою їх власників або мешканців для з'ясування обставин кримінального правопорушення, що готується; збирання відомостей про протиправну діяльність осіб, щодо яких проводиться перевірка та інші необхідні заходи, що витікають з положень ст. 8 Закону України «Про оперативно-розшукову діяльність» [191];

– використання можливостей баз даних єдиної інформаційної системи Міністерства внутрішніх справ України та інших інформаційних ресурсів, а також медіа (ч. 4 розділ ІІ Інструкції) [182].

Згідно з Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» [182], матеріали оперативного підрозділу Департаменту кіберполіції Національної поліції України, його структурних підрозділів, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення чи приховування яких передбачає

використанням комп'ютерів, що направляють до слідчого підрозділу для початку досудового розслідування, мають містити:

1) письмове пояснення заявника, де зазначають відомі заявнику дані про вчинення кримінального правопорушення, відповідні додатки (роздруківки або скріншоти), а також, у певних випадках документи, що підтверджують право власності на комп'ютерну інформацію чи програмно-технічні засоби;

2) установлені ідентифікаційні дані про використані інформаційних комп'ютерних технологій, а також 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.

Розглядаючи слідчі ситуації початкового етапу розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій на підставі аналізу праць науковців [51, с. 126–127; 138, с. 93–95; 217, с. 218], вважаємо за необхідне акцентувати на тому, що основним критерієм класифікації слідчих ситуацій переважно є елементи криміналістичної характеристики (спосіб вчинення, особа злочинця, сліди).

Вбачається за доцільне під час дослідження слідчих ситуацій початкового етапу розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, використати такі вихідні дані: спосіб вчинення та особу кіберзлочинця, що комбінуються між собою та за якими буде здійснено класифікацію слідчих ситуацій.

1. Спосіб вчинення невідомий, особа кіберзлочинця невідома.

Зазначена слідча ситуація поширена в більшості вчинених кримінальних правопорушень зазначеної категорії на початковому етапі розслідування.

Першочерговими слідчими (розшуковими) діями будуть: 1) проведення огляду місця події та комп'ютерних даних; 2) допит потерпілого; 3) допит свідка.

Головною метою зазначених слідчих (розшукових) дій є встановлення способу вчинення та особи кіберзлочинця.

2. Спосіб вчинення відомий, особа кіберзлочинця невідома.

У такій ситуації важливим є пошук слідів, що залишені залежно від обраного злочинцем конкретного способу вчинення. Розуміння способу вчинення допоможуть слідчому зрозуміти характер і локалізацію слідів.

Важливим у цій слідчій ситуації є проведення комп'ютерно-технічної експертизи засобу інформаційно-комп'ютерних технологій, на якому залишені ймовірні сліди вчинення протиправного діяння.

3. Спосіб вчинення невідомий, особа кіберзлочинця відома.

Така слідча ситуація можлива, коли особа, що вчинила кримінальне правопорушення, сама з'явилася з «каяттям» чи відома з показань потерпілого. Можливі випадки, коли певна організація чи певна особа заявили публічно про вчинення конкретного протиправного діяння.

Першочерговими слідчими (розшуковими) діями будуть: 1) проведення огляду місця події та комп'ютерних даних; 2) проведення допитів; 3) проведення обшуку.

У певних випадках, коли необхідно встановити коло всіх співучасників кримінального правопорушення зазначеної категорії, можуть проводити такі негласні слідчі (розшукові) дії: 1) установлення місцезнаходження радіоелектронного засобу; 2) спостереження за особою; 3) моніторинг банківських рахунків; 4) зняття інформації з транспортних телекомунікаційних мереж; 5) зняття інформації з електронних інформаційних систем; 6) аудіо-, відеоконтроль місця.

4. Спосіб вчинення відомий, особа кіберзлочинця відома.

Ця ситуація є найсприятливішою на цьому етапі розслідування, оскільки потребує швидкого проведення необхідних слідчих (розшукових) дій для фіксації необхідних слідів.

Першочерговими слідчими (розшуковими) діями на цьому етапі є: 1) огляд місця події та комп'ютерних даних; 2) обшук; 3) проведення допитів.

Проте цей перелік слідчих ситуацій є узагальненим для кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. На нашу думку, залежно від криміналістичної класифікації зазначених протиправних діянь, може йтися про типовіші слідчі ситуації (наприклад, слідчі

ситуації розслідування злочинів проти основ національної безпеки України, що вчиняються з використанням інформаційних комп'ютерних технологій тощо).

Розглядаючи слідчі ситуації, що складаються після вручення повідомлення про підозру, наступного етапу процесу розслідування кримінальних правопорушень, вчинених з використанням інформаційних комп'ютерних технологій, слід зазначити, що вони характеризуються даними про особу підозрюваного та фактичними даними (доказами), що вказують на його винуватість.

1. Підозрюваний визнає свою вину, наявні фактичні дані вказують на його винуватість.

Така слідча ситуація є сприятливою для слідчого, оскільки немає конфліктних ситуацій між слідчим і підозрюваним. Важливою слідчою (розшуковою) дією є проведення допиту підозрюваного. Ефективне проведення допиту надасть можливість слідчому перевірити наявну вже відому інформацію та підтвердити наявні фактичні дані.

2. Підозрюваний не визнає свою вину, наявні фактичні дані вказують на його винуватість.

Ця слідча ситуація вирізняється конфліктністю між слідчим і підозрюваним. За конфліктної ситуації інтереси слідчого та підозрюваного не збігаються, наприклад, підозрюваний прагне приховати сліди кримінального правопорушення та уникнути кримінальної відповідальності. Застосування окремих тактичних прийомів допиту, зокрема, пред'явлення доказів, допоможе продемонструвати наявність необхідної інформації в слідчого про причетність підозрюваного до кримінального правопорушення.

3. Підозрюваний визнає вину, але наявні фактичні дані не вказують на його винуватість/відсутність фактів та обставин, що вказують на його вину.

У цій слідчій ситуації важливе значення має проведення допиту підозрюваного, оскільки на підставі його показань можна виявити сліди вчинення протиправних діянь. Доцільно під час допиту підозрюваного встановити з ним

психологічний контакт. У деяких випадках необхідним буде проведення повторних слідчих (розшукових) дій: обшуку, огляду тощо.

4. Підозрюваний не визнає вину, наявні фактичні дані не вказують на його винуватість/відсутність фактів та обставин, що вказують на його вину.

Така слідча ситуація є несприятливою для слідчого, оскільки немає достатньої інформації для її вирішення, а отримати її шляхом проведення «гласних» слідчих (розшукових) дій неможливо. У цьому випадку необхідним буде проведення негласних слідчих (розшукових) дій, спрямованих на встановлення додаткових відомостей про кримінальне правопорушення.

На завершальному етапі розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, можуть виникати такі слідчі ситуації:

1. Ситуація, коли на підставі зібраних під час досудового розслідування доказів потрібно закрити кримінальне провадження.

Під час проведення досудового розслідування стосовно підозрюваної особи були зібрані фактичні дані, що свідчать про: відсутність події кримінального правопорушення (п. 1 ч. 1 ст. 284 КПК України); відсутність у діянні складу кримінального правопорушення (п. 2 ч. 1 ст. 284 КПК України); недостатність доказів для доведення винуватості особи в суді й вичерпано можливості їх отримання (п. 3 ч. 1 ст. 284 КПК України).

Зауважимо, що за п. 1, 2 ч. 1 ст. 284 КПК України закриття кримінального провадження можливе без повідомлення особі про підозру у вчиненні кримінального правопорушення. У такому випадку не буде наступного етапу розслідування (третього етапу).

2. Ситуація, де на підставі зібраних під час досудового розслідування доказів підозрюваного може бути звільнено від кримінальної відповідальності.

Отримавши докази винуватості підозрюваного у вчиненні кримінального правопорушення та встановивши під час досудового розслідування підстави для звільнення від кримінальної відповідальності у випадках, передбачених законом України про кримінальну відповідальність (ст. 45–49 КК України), отримавши

згоду підозрюваного, прокурор складає клопотання про звільнення від кримінальної відповідальності та направляє клопотання до суду.

3. Ситуація, коли на підставі зібраних під час досудового розслідування доказів слід звернутися до суду з обвинувальним актом, клопотанням про застосування примусових заходів медичного або виховного характеру.

Переконавшись, що отримані під час досудового розслідування докази є достатніми для складання обвинувального акту або клопотання про застосування примусових заходів медичного чи виховного характеру, прокурор або слідчий за дорученням прокурора повідомляють підозрюваному, його захиснику, законному представнику та захиснику особи, стосовно якої передбачено застосування примусових заходів медичного чи виховного характеру, про завершення досудового розслідування та надають доступ до матеріалів досудового розслідування (ч. 1 ст. 290 КПК України).

Після завершення досудового розслідування та ознайомлення учасників кримінального провадження з його матеріалами, слідчим, дізнавачем (у кримінальних проступках) складають обвинувальний акт чи клопотання про застосування примусових заходів медичного чи виховного характеру, що затверджує прокурор.

У випадку, коли прокурор не погоджується з обвинувальним актом, клопотанням про застосування примусових заходів медичного чи виховного характеру, складеними слідчим, дізнавачем, він складає його самостійно.

До зазначеної ситуації належить і досягнення угоди про визнання винуватості між прокурором та підозрюваним, що може бути ініційоване під час досудового розслідування після повідомлення особі про підозру. Складають обвинувальний акт, який з підписаною сторонами угодою направляють до суду. Натомість таке рішення може бути прийнято і на наступному (третьому) етапі.

З огляду на викладене, слідчі ситуації вихідного, початкового, наступного та завершального етапів розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій, є одним із головних елементів методики розслідування зазначених протиправних діянь. Слідчі ситуації,

що складаються на кожному етапі розслідування, допомагають зрозуміти, який комплекс слідчих (розшукових) дій необхідно провести для їх вирішення, а також визначити напрям побудови слідчих версій та планування розслідування.

3.2. Висунення версій та планування розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Одним із напрямів проведення ефективного розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій, є висунення версій та розроблення плану його розслідування.

Взаємозв'язок між версією і плануванням розслідування досліджувала В. О. Коновалова, акцентуючи на тому, що в процесі розслідування версія тісно пов'язана з плануванням розслідування. Роль версії щодо планування є визначальною, оскільки вона є тим напрямом розслідування, що обумовлює побудову комплексу слідчих (розшукових) дій, які здійснюють для її перевірки [100, с. 25].

Насамперед розглянемо поняття «версія», що є основою планування розслідування кримінальних правопорушень, які вчиняють з використанням інформаційних комп'ютерних технологій.

Слушно зауважують науковці, що у зв'язку з діяльністю щодо розслідування кримінальних правопорушень слідчий звертається до фактів та подій минулого. Тому в цьому процесі є така формально-логічна категорія, як гіпотеза, тобто обґрунтоване припущення, що пояснює характер кримінального правопорушення або його окремих обставин. У криміналістиці таке обґрунтоване припущення називають «криміналістичною версією» [117, с. 171].

Цілком прийнятним і таким, що цілком висвітлює поняття «криміналістичної версії», є визначення, сформульоване М. В. Салтевським. На думку науковця, це ґрунтоване на зібраній інформації з розслідуваного кримінального провадження

припущення (імовірне судження) слідчого, прокурора, дізнавача про подію кримінального правопорушення та злочинця загалом або окремі факти й осіб, причинові та інші зв'язки між обставинами, що підлягають розслідуванню [214, с. 281].

Поділяємо думку Ю. М. Чорноус, що криміналістична версія повинна відповідати низці вимог:

– бути реальною та простою;

– можливою для перевірки;

– обґрунтованою встановленими фактами;

– мати відношення до широкого кола обставин, які встановлюють у процесі розслідування [109, с. 67].

У криміналістичній літературі пропонують різні класифікації криміналістичних версій. На підставі криміналістичних досліджень українських вчених-криміналістів можна виокремити такі [104, с. 132; 110, с. 311–312]:

1) за суб'єктом висування: версії слідчого, дізнавача, прокурора, співробітника оперативного підрозділу, експерта, суду;

2) за ступенем визначеності висунутих припущень: типові й конкретні. Типові версії висувають у разі недостатності вихідних даних, здебільшого на початковому етапі розслідування, а також дають загальне, орієнтовне пояснення певних даних. Під час подальшої перевірки помилкові варіанти відкидають, а підтверджену типову версію деталізують і на її основі будують конкретні версії;

3) за об'єктом пояснення фактів: загальні й окремі. Загальні версії пояснюють сутність усієї розслідуваної події, а окремі – лише певні її елементи;

4) за ступенем імовірності: малоймовірні та найбільш імовірні;

5) за часом побудови: первинні й наступні. Під час проведення досудового розслідування іноді доводиться повертатися до попередніх, тобто первинних версій;

6) за предметом доказування: обвинувальні й виправдувальні. Обвинувальна версія – пояснення вчиненого кримінального правопорушення, альтернативою якого є виправдовувальна версія (контрверсія), що припускає невинуватість особи;

7) за операціями з фактичними даними: пошукові й дослідницькі;

8) за ступенем складності внутрішньої структури: комплексні (висувають щодо декількох обставин) і прості (висувають лише за однією обставиною);

9) залежно від пошукової спрямованості: ретроспрямовані (встановлення обставин минулого) і передбачувальні (встановлення фактів у теперішньому чи очікуваному майбутньому).

Слушно зауважили І. В. Гора, А. В. Іщенка та В. А. Колесник, що особою висунення слідчих версій може бути лише суб'єкт, який проводить розслідування кримінального правопорушення, – слідчий, дізнавач, прокурор. Якщо інші учасники процесу висловлюють свої припущення, їх можуть розглядати як слідчі версії лише у випадку прийняття їх слідчим, дізнавачем, прокурором.

Висловлені припущення іншими учасниками процесу можуть розглядати як слідчі версії лише у випадку прийняття їх особою (слідчим, прокурором, дізанавачем), яка проводить розслідування [57, с. 36].

Тому, розглядаючи поняття слідчих версій кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, суб'єктом їх висунення, на нашу думку, може бути слідчий, дізнавач або прокурор.

Цілком правильно зауважує В. М. Левков, що розподіл версій можуть здійснювати за етапами розслідування. Ця класифікація зумовлена ступенем імовірності й обґрунтованості того, що версії, конструйовані на першому етапі розслідування, переважно менш імовірні, ніж на подальших етапах. Версії, висунуті на подальших етапах розслідування, є ефективнішими в тому випадку, коли під час висунення версій на початковому етапі не було допущено логічних і фактичних помилок [124, с. 6].

Поділяючи позицію науковця, розглянемо особливості висунення слідчих версій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, на кожному з визначених нами етапах розслідування.

Висунення слідчих версій під час розслідування зазначених кримінальних правопорушень розпочинається ще з вихідного етапу розслідування.

Однак процес виникнення слідчих версій проходить низку умовних етапів.

1. Аналіз і синтез даних з матеріалів, унаслідок чого відбувається певне впорядкування інформації про слідчу ситуацію, що склалася під час розслідування.

2. Звернення слідчого до знань, якими він володіє, а також життєвого і професійного досвіду, який необхідний для пояснень окремих питань у зв'язку з побудовою версії. Для цього використовують інформацію не тільки з особистого, а й з узагальненого досвіду розслідування аналогічних кримінальних проваджень, інтуїцію, дані з літературних джерел, довідників, що можуть допомогти у висуненні версій.

3. Реалізація знань і досвіду, узагальнених даних, а також оцінка конкретної слідчої ситуації, що склалася, і визначення кола можливих версій.

4. Формування слідчих версій.

5. За допомогою індукції та дедукції здійснюють конкретизацію версій [115, с. 267].

На вихідному етапі розслідування зазначених кримінальних правопорушень обставини вчинення в більшості випадків є недостатньо повно з'ясовані, бракує чітких ознак складу кримінального правопорушення.

У таких випадках О. Н. Колесніченко та Г. А. Матусовський цілком доречно зазначають про можливість висунення так званих версій кваліфікації, що є різновидом слідчої версії та мають важливе значення в ситуаціях, де ще не відображені явні ознаки кримінального правопорушення, хоча шкідливі наслідки його є очевидними (наприклад, незаконне втручання в роботу ЕОМ тощо). Версії кваліфікації важливі й на подальших етапах розслідування, коли встановлено особу, яка вчинила кримінальне правопорушення, однак не встановлено обтяжуючі обставини, мотиви й способи вчинення кримінального правопорушення [95, с. 8].

До версій вихідного етапу розслідування зазначеної категорії кримінальних правопорушень можна віднести версії, запропоновані Г. В. Щербаковою, а саме: 1) кримінальне правопорушення справді вчинене за тих обставин, що випливають із первинних матеріалів; 2) помилкова заява про кримінальне правопорушення [48, с. 403].

На нашу думку, можна говорити про висунення подальших слідчих версій вихідного етапу розслідування кримінальних правопорушень зазначеної категорії:

– вчинено кримінальний проступок;

– вчинено злочин;

– немає ознак вчинення зазначених кримінальних правопорушень.

Поділяючи таку позицію науковців [138, с. 136–137; 203, с. 489–490], вважаємо, що оскільки початковий етап характеризується наявністю недостатньої кількості інформації про вчинене кримінальне правопорушення зазначеної категорії, то для побудови слідчих версій необхідно використовувати елементи криміналістичної характеристики кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

У науковій літературі пропонують й інші версії зазначених протиправних діянь. Зокрема, Г. В. Щербакова пропонує такі види версій:

– версії про особу злочинця (ів);

– версії про місця здійснення входу до комп'ютерної системи;

– версії про обставини, за яких було вчинено кримінальне правопорушення;

– версії про розмір збитків, завданих кримінальним правопорушенням [48, с. 403].

На наш погляд, пропоновані версії є більш узагальненими та, з огляду на недостатність знань у практичних працівників, вважаємо необхідним більш деталізований підхід до висунення версій.

З огляду на це, слід розглянути перелік версій, запропонований В. В. Коваленком і В. І. Чубаєвським, що ґрунтуються на матеріалах кримінального провадження, а також пов'язані з особою злочинця та місцем знаходження знаряддя вчинення:

1) щодо співучасті злочинців висувають версії про те, що: а) відбулася змова злочинців зі співробітником підприємства, установи, організації; б) відбулася змова декількох осіб у межах підприємства, установи, організації; в) злочинець діяв одноособово;

2) щодо взаємодії злочинців версії можуть бути такі: а) комп'ютерний злочин учинений групою осіб; б) кримінальне правопорушення вчинене одноосібно;

3) якщо злочинець переховується, можна висунути версії щодо його місцезнаходження: а) у друзів, знайомих; б) у будь-кого з далеких родичів; в) за місцем постійного проживання; г) у близьких родичів; д) виїхав за кордон; е) у колег;

4) розшукові версії можна виокремити залежно від місцезнаходження знарядь учинення кримінального правопорушення, інших речових доказів: а) за місцем роботи злочинця; б) за місцем проживання злочинця; в) у родичів, друзів, знайомих, партнерів по бізнесу; г) у гаражі, на складі, в інших підсобних і службових приміщеннях [202, с. 157].

У криміналістичній літературі використовують поняття «розшукові версії». З цього приводу слушно зауважує В. О. Коновалова, що розшукові версії – це припущення під час здійснення розшуку особи: про місцеперебування осіб, які вчинили кримінальне правопорушення, іншу доказову інформацію тощо. Такі версії вирізняються високою ймовірністю невизначеності, оскільки під час їх формування не завжди є достатньо інформації [100, с. 64].

Отже, проаналізувавши погляди вітчизняних вчених щодо слідчих версій, пропонуємо слідчі версії початкового етапу розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. Розглянемо можливі слідчі версії, ураховуючи обстановку (місце та час вчинення), а також сліди вчинення.

1. Версії, що стосуються місцезнаходження злочинця:

– злочинець перебуває в одній країні з потерпілим: за місцем проживання в друзів, знайомих, родичів тощо;

– злочинець перебуває в іншій країні;

– злочинець перебуває в одній країні, використовує засоби інформаційно-комунікаційних технологій в іншій, вчиняє свої протиправні дії в країні перебування потерпілого.

2. Версії про місце використання засобів інформаційно-комп'ютерних технологій:

– знаряддя ІКТ знаходиться вдома у злочинця;

– знаряддя ІКТ знаходиться в іншому місці.

3. Версії, що стосуються часу вчинення:

– злочинець навмисно обрав відповідний час вчинення;

– злочинець не обирав час вчинення.

4. Версії, що стосуються слідів:

– злочинець навмисно приховував сліди вчинення, використовуючи різні засоби анонімізації;

– злочинець не приховував сліди вчинення, оскільки знав, що в нього буде достатньо часу, щоб зникнути;

– злочинець навмисно залишив сліди в конкретному місці, щоб пустити розслідування «хибним шляхом».

Розглядаючи слідчі версії наступного етапу розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, необхідно враховувати слідчі ситуації, що склалися на цьому етапі.

1. Підозрюваний не визнає свою вину, наявні фактичні дані вказують на його винуватість, може бути висунуто такі версії:

– підозрюваний не вчиняв зазначеного протиправного діяння, а справжній злочинець використав його засіб інформаційних комп'ютерних технологій;

– справжній злочинець навмисно вирішив заплутати слідчого, щоб пустити його «хибним шляхом».

2. Підозрюваний визнає вину, але наявні фактичні дані не вказують на його винуватість/відсутність фактів й обставин, що вказують на його вину:

– кримінальне правопорушення вчинив хтось зі знайомих підозрюваного, і він хоче взяти вину на себе;

– підозрюваний не розумів характер своїх дій та вчинків;

– правопорушення було вчинене групою осіб, і підозрюваний не бажає свідчити проти них.

3. Підозрюваний не визнає вину, наявні фактичні дані не вказують на його винуватість/відсутність фактів й обставин, що вказують на його вину:

– підозрюваний, спланувавши кримінальне правопорушення, розрахував, що фактичні дані не будуть вказувати на нього;

– підозрюваний вважає, що він ретельно знищив усі сліди свого протиправного діяння.

Переходячи до розгляду завершального етапу кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, слушно зауважує О. Н. Колесниченко, що до кінця розслідування мають залишитися лише одна версія та докази, які покладені в її обґрунтування, решта версій повинні бути виключені, а також свідчити, що слідчий дійшов правильних висновків у кримінальному провадженні [97, с. 170].

Отже, залежно від слідчих ситуацій, що складаються на цьому етапі розслідування кримінальних правопорушень зазначеної категорії, може йтися про висунення таких слідчих версій:

1. Ситуація, коли на підставі зібраних під час досудового розслідування доказів потрібно закрити кримінальне провадження.

Версія: чи всі фактичні дані вказують на необхідність закриття кримінального правопорушення.

2. Ситуація, за якої на підставі зібраних під час досудового розслідування доказів підозрюваний може бути звільнений від кримінальної відповідальності.

Версія: чи всі фактичні дані вказують на доведення невинуватості підозрюваного.

3. Ситуація, коли на підставі зібраних під час досудового розслідування доказів слід звернутися до суду з обвинувальним актом, клопотанням про застосування примусових заходів медичного або виховного характеру.

Версія: чи є достатніми зібрані докази, що вказують на доведення винуватості підозрюваного.

Своєю чергою зауважимо, що всі висунуті версії мають бути перевірені під час досудового розслідування; надмірна увага одній з версій та ігнорування інших

на практиці призводить до невстановлення особи, яка вчинила кримінальне правопорушення, або притягнення до кримінальної відповідальності невинної особи.

Перевірка версій – це діяльність, спрямована на встановлення фактичних обставин, що підтверджують чи спростовують припущення, викладені в змісті версії [110, с. 394].

Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, потребує високої організації роботи слідчого. Щоб розслідування не було безрезультатним і не нагадувало сукупність проведених слідчих (розшукових) та негласних слідчих (розшукових) дій, а дало результат, потрібно розробити загальний план розслідування та організувати проведення окремих процесуальних дій.

Акцентуючи на необхідності складання плану розслідування, Г. Гросс свого часу зазначав: «Досить складно скласти план розслідування, а ще складніше його дотримуватися. План розслідування не слід порівнювати з планом підприємства чи з плануванням дому. Такий план будується на тих даних, які має слідчий» [47, с. 18–19].

Поміж вітчизняних учених-криміналістів першим дослідив на дисертаційному рівні планування розслідування О. Н. Колесніченко (1952 року захистив кандидатську дисертацію «Планування радянського попереднього слідства») [96].

У криміналістичній науці головними завданнями планування розслідування є: 1) визначення найраціональніших шляхів розслідування кримінальних правопорушень; 2) забезпечення об'єктивності, повноти та всебічності розслідування; 3) застосування криміналістичних рекомендацій з урахуванням особливостей кожного конкретного кримінального провадження; 4) забезпечення найефективніших форм взаємодії суб'єкта розслідування з іншими органами та підрозділами, громадськістю в процесі розслідування кримінального правопорушення; 5) забезпечення досягнення мети розслідування з мінімальними

витратами людських і матеріальних ресурсів, а також економного використання робочого часу слідчого [104, с. 139–140].

Слушно зауважує Ю. М. Чорноус, що кожен вид планування є особливим. Однак наявні певні вимоги, яких слід дотримуватися під час планування. Ці вимоги є принципами планування, серед них виокремимо такі:

1) індивідуальність – кожен складений план розслідування є своєрідним і неповторним для конкретного кримінального правопорушення, що слід враховувати під час його складання;

2) динамічність – передбачає підхід до розслідування та його планування як до процесу, що розвивається;

3) реальність плану – його збалансованість за ресурсами та лімітом часу;

4) конкретність – передбачає чітке формування в плані завдань, які необхідно виконати під час розслідування, відповідних дій, строків і виконавців [110, с. 319].

На тому, що перелічені принципи обов'язково слід ураховувати під час планування розслідування, акцентує переважна більшість вітчизняних учених-криміналістів. Дискусій з цього приводу в криміналістичній літературі немає.

Твердження М. В. Салтевського, що планування є обов'язковою умовою будь-якого розслідування, сумніву не викликає. Плануванням учений вважає найдоцільнішу та цілеспрямовану діяльність, яка дає змогу швидко й ефективно організувати збирання, дослідження та використання доказової інформації для розшуку і встановлення злочинця, а також інших обставин, що підлягають доказуванню [214, с. 317].

На наш погляд, у проаналізованих визначеннях науковців [126, с. 212; 110, с. 139] можна виокремити спільні риси, що стосуються планування розслідування. Зокрема, планування розслідування розглядають як творчий розумовий процес, спрямований на організацію розслідування.

Привертає увагу твердження В. О. Коновалової, що планування – це програма розслідування кримінального правопорушення, уявна чи сформульована в конкретній формі [100, с. 120]. Учена вводить поняття «програма розслідування», що є досить незвичним у контексті дослідження планування розслідування.

В українській мові термін «програма» тлумачать як наперед продуманий план діяльності, роботи тощо [29, с. 966].

Тож плануванням розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, слід розуміти наперед продуманий план дій слідчого (дізнавача, детектива) у конкретному кримінальному провадженні з розслідування зазначених протиправних діянь, що складений як слідчим (дізнавачем, детективом), так і за допомогою програмних засобів [143].

Про обов'язковість складання плану розслідування зазначено в Інструкції з організації діяльності слідчих підрозділ Національної поліції України, затвердженій наказом МВС України від 6 липня 2017 року № 570. Для того щоб забезпечити своєчасність виконання необхідних слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях, ідеться в документі, слідчий складає загальний календарний план-графік роботи в цих кримінальних провадженнях, а також плани розслідування кримінальних правопорушень [79].

Однак Інструкція стосується лише працівників слідчих підрозділів Національної поліції України, а не всіх органів, що здійснюють досудове розслідування.

Слід зауважити, що в Сінгапурі кримінально-процесуальне законодавство зобов'язує працівника поліції, який проводить розслідування, вести щоденник слідчих дій, у якому зазначено: час, коли йому надійшло розпорядження про проведення розслідування; час, коли він почав і закінчив розслідування; місця, які він відвідував, а також результат розслідування. Водночас обвинуваченому заборонено вимагати або перевіряти такий щоденник до чи під час розслідування або судового розгляду [277].

З огляду на це, необхідно закріпити в КПК України обов'язок складання плану розслідування органом досудового розслідування з подальшим долученням його до матеріалів кримінального провадження. Це буде свідченням, що в процесі

досудового розслідування перевірено всі можливі версії вчинення кримінального правопорушення, а здійснене розслідування було об'єктивним і неупередженим.

Деякі вчені-криміналісти вважають, що планування може бути усним. Інші аргументують обов'язковість складання плану в письмовій формі.

Згідно з результатами проведеного опитування прокурорів, 60 % респондентів схвалюють необхідність складання письмового плану розслідування слідчим. Лише 24 % зазначили, що письмове планування розслідування може не відбуватися. Здебільшого це прокурори, стаж роботи яких – до трьох років, тобто недостатній досвід роботи [162].

Вбачається, що планування розслідування кримінальних правопорушень, які вчиняють з використанням інформаційних комп'ютерних технологій, має відбуватися в письмовій формі. Зазначене обумовлено специфікою зазначених кримінальних правопорушень, складністю термінології, недостатністю навичок у слідчих з розслідування, необхідністю залучення спеціаліста, а також особливостями проведення слідчих (розшукових) і негласних слідчих (розшукових) дій та організаційних заходів тощо.

План розслідування може бути складено як шляхом письмового викладення слідчим його змісту, що є результатом його розумової діяльності, так і за допомогою застосування програмних засобів.

Актуальним є питання щодо застосування результатів програмування (програм) у розслідуванні кримінальних правопорушень.

Поняття програмування розслідування аналізує В. А. Журавель, зауважуючи, що програма розслідування є сукупністю приписів (криміналістичних алгоритмів) і правил рекомендаційного характеру, спрямованих на виконання комплексу тактичних завдань, охоплює кілька моделей дій слідчого, прокурора залежно від етапу розслідування, слідчої ситуації, позиції учасників кримінального провадження. Пропонує створити структурну програму дій слідчого, прокурора, що містить максимально вичерпний перелік пунктів того, які питання можуть виникати в певних ситуаціях, а також варіанти систем слідчих (розшукових) і

негласних слідчих (розшукових) дій, які доцільно застосувати задля їх реалізації [28, с. 666–667].

Своєю чергою ми пропонуємо під час планування розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, використовувати можливості штучних нейронних мереж.

Нейронні мережі – це мережі зі здатністю самостійного навчання. Їх застосовують не як технологію, інструмент або засіб, а як систему, що здатна вчитися і використовувати вивчене. Нейронні мережі влаштовані за зразком людського мозку, тобто намагаються відтворити певні аспекти влаштування нейромереж у мозку людини. Головним є те, що вони використовують дані як матеріал, на якому навчаються [238, с. 13].

Тобто штучні нейронні мережі не програмуються, а навчаються на основі покладених даних.

З наукової позиції штучна нейронна мережа – це паралельно розподілена система обробки інформації, утворена тісно пов'язаними простими обчислювальними вузлами (нейронами) (однотипними або різними), що має властивість накопичувати експериментальні знання, узагальнювати їх і робити доступними для користувача у формі, зручній для інтерпретації та прийняття рішень [211, с. 3].

Слід зауважити, що відмінність між штучною нейронною мережею (ШНМ) і штучним інтелектом полягає в тому, що ШНМ є видом машинного навчання, мета якого – частково або цілком автоматизувати рішення різних складних аналітичних задач [254].

Машинне навчання є розділом штучного інтелекту, за якого системи можуть автоматично (самостійно) навчатися та вдосконалюватися. Вони мають забезпечити незалежні методи навчання, щоб їх не потрібно було програмувати [270].

Зазначимо, що виникнення поняття «нейронна мережа» пов'язують з працею У. МакКаллоха та У. Піттса «A logical calculus of the ideas immanent in nervous

activity» (1943), у якій вчені розробили комп'ютерну модель нейронної мережі [295].

Найпоширенішими завданнями, які виконує ШНМ, є:

1. Розпізнавання образів (зображень, текстів, друкованих і рукописних, звуку, мови тощо) є тією галуззю, де найяскравіше виявляються переваги ШНМ [211, с. 9].

2. Кластеризація – розбиття множини на вхідних сигналах на класи, причому ні кількість, ні ознаки класів заздалегідь не відомі. Після навчання така мережа здатна визначити, до якого класу належить вхідний сигнал [255].

3. Прогнозування – здатність нейронної мережі до узагальнення та виокремлення прихованих залежностей між вхідними та вихідними даними. Після навчання мережа здатна передбачити майбутні значення певної послідовності на основі декількох попередніх значень або інших наявних чинників.

4. Прийняття рішень та управління. На підставі класифікації ситуацій, що надходять на вхід нейронній мережі, на виході повинна з'явитися ознака рішення, що прийняла нейронна мережа [255].

5. Виявлення тенденцій, прихованих зв'язків, аномалій, повторюваних елементів [293].

Головна перевага ШНМ полягає в тому, що вона може розв'язувати задачі в умовах невизначеності. Завдяки здатності до навчання штучна нейронна мережа дає змогу виконувати завдання з невідомими закономірностями та залежностями між вхідними й вихідними даними, що дозволяє працювати з неповними даними [293].

Можливості ШНМ активно використовують у більшості галузей людської діяльності.

Зокрема, 2018 року ШНМ AlphaZero (самостійне навчання шахам потребувало близько чотирьох годин) перемогла найсильнішу шахову програму Stockfish. Матч із тисячі партій між цією ШНМ і комп'ютерною програмою, у якому AlphaZero виграла 155, програла 6, а решту шахових партій 839 зіграли внічию [265].

Активне використання можливостей ШНМ відбувається і в медицині. Розробники Google навчили ШНМ розпізнавати за сітківкою ока захворювання серця і кровоносних судин з точністю 70 %. Мережа була навчена на 300 тис. зображень сітківки [226].

В іншому випадку дослідники з університету Дюка навчили ШНМ розпізнавати мамограми злоякісної тканини на основі восьми особливостей, з якими здебільшого працюють радіологи. Виявилося, що мережа здатна вирішувати поставлену задачу з чутливістю близько 100 % і специфічністю 59 % (порівняно з 10–20 % у радіологів) [226].

Отже, пропонуємо на базі успішних і неуспішних планів розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, навчити штучну нейронну мережу розробляти конкретний план розслідування у відповідних ситуаціях, а також аналізувати вже наявні плани розслідування на знаходження та усунення помилок [143, с. 467].

Цей план розслідування зазначених кримінальних правопорушень, що складений за допомогою ШНМ, повинен бути рекомендаційним. Будь-які правки, зміни тощо, а також прийняття рішень про проведення певних процесуальних чи тактичних дій, запропонованих у плані ШНМ, має приймати виключно слідчий [143, с. 457].

Використання можливостей ШНМ під час планування розслідування кримінальних правопорушень зазначеної категорії сприятиме:

1) підвищенню ефективності та швидкості розслідування зазначених протиправних діянь;

2) економії часу стосовно планування розслідування;

3) обранню найдоцільніших тактик і методів, які слід застосовувати в процесі досудового розслідування кримінальних правопорушень зазначеної категорії;

4) низькій імовірності того, що розслідування зайде в глухий кут;

5) забезпеченню захисту інтересів людини в кіберпросторі;

6) зниженню процесуальних і тактичних помилок;

7) дотриманню вимог розумного строку під час кримінального провадження [143, с. 457].

3.3. Особливості проведення слідчих (розшукових) дій та застосування заходів забезпечення під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Результативне проведення досудового розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, насамперед пов'язане з ефективним проведенням окремих слідчих (розшукових) і негласних слідчих (розшукових) дій, що спрямовані на перевірку слідчих версій шляхом збирання (отримання) доказів у передбаченому кримінальним процесуальним законодавством порядку, а також перевірку вже отриманих доказів для встановлення наявності чи відсутності фактів й обставин, що мають значення в конкретному кримінальному провадженні.

Кожна слідча (розшукова) дія має не тільки чітко визначені процесуальні, а й тактичні особливості її проведення, які в криміналістичній літературі називають тактичним прийомом.

Слушно зауважив В. І. Галаган, що тактичний прийом – це рекомендація про можливі альтернативні варіанти проведення процесуальних дій чи прийняття тактичних рішень. Ще до початку безпосереднього проведення слідчих (розшукових) дій слідчому необхідно вирішити певні питання, що стосуються тактичних прийомів: про час і місце, склад учасників, підготовку доказів і визначення черговості їх пред'явлення, засоби фіксації перебігу й одержаних результатів тощо [46, с. 73–74].

Для застосування тактичних прийомів під час проведення окремих слідчих (розшукових) дій у зазначених кримінальних правопорушеннях слідчому необхідно не тільки володіти певними криміналістичними вміннями та знаннями, а й розуміти специфіку таких кримінальних правопорушень і слідкувати за

сучасними криміналістичними засобами, які можна застосовувати під час проведення окремих слідчих (розшукових) дій.

Однією з першочергових слідчих (розшукових) дій, що надає можливість швидко зафіксувати сліди протиправних діянь під час розслідування кримінальних правопорушень зазначеної категорії, є проведення *огляду*.

Вітчизняні вчені-криміналісти пропонують різні визначення огляду.

Ми цілком поділяємо думку В. О. Коновалової, яка огляд тлумачить як «слідчу (розшукову) дію, що полягає в безпосередньому сприйнятті об'єктів з метою виявлення слідів кримінального правопорушення, з'ясування обставин події, а також обставин, що мають значення для кримінального провадження» [108, с. 297].

Такі міркування науковця відповідають положенням ч. 1 ст. 237 КПК України, згідно з якими огляд безпосередньо проводить прокурор або слідчий з конкретною метою – виявити та зафіксувати відомості, що стосуються обставин вчинення кримінального правопорушення.

У положеннях зазначеної статті ідеться про такі види огляду: огляд місцевості, огляд приміщення, огляд речей та документів, огляд комп'ютерних даних, огляд житла чи іншого володіння особи.

Слід зауважити, що відповідно до Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації"» від 15 березня 2022 року № 2137-IX [274] щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам введено новий вид огляду – огляд комп'ютерних даних.

Огляд комп'ютерних даних проводить слідчий, прокурор шляхом відображення в протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або в паперовій формі) [121].

Однак законодавець не пропонує визначення поняття комп'ютерних даних.

Натомість така дефініція є в Конвенції про кіберзлочинність і означає представлення фактів, інформації або концепцій у формі, що є придатною для обробки в комп'ютерній системі [99].

Слід зазначити, що єдина слідча (розшукова) дія, яку може бути проведено до внесення в ЄРДР відомостей про вчинене кримінальне правопорушення з використанням інформаційних комп'ютерних технологій, – це *огляд місця події* (ч. 3 ст. 214 КПК України), що є одним з найскладніших видів огляду.

Зауважимо, що суб'єктами, які уповноважені проводити огляд місця події до внесення відомостей до ЄРДР, згідно з чинним кримінальним процесуальним законодавством України, крім слідчого, прокурора, може бути і дізнавач, якщо це не огляд житла чи іншого володіння особи (ч. 2 ст. 237 КПК України).

Якщо потрібно проводити огляд місця події, яким може бути житло чи інше володіння особи, у такому разі необхідна добровільна згода особи чи ухвала слідчого судді, про що також було зазначено в постанові Верховного Суду колегією суддів Третьої судової палати від 6 жовтня 2021 року у справі № 756/11581/15-к [173].

Традиційно в криміналістичній літературі огляд місця події поділяють на три етапи: підготовчий, робочий та заключний.

Слушно зауважує О. В. Захарова, що такий поділ у жодному разі не порушує цілісності цієї слідчої (розшукової) дії. Він забезпечує реалізацію загальних положень тактики огляду, систематизує дії слідчого, встановлює їх послідовність, забезпечує належну якість огляду [112, с. 310].

За твердженням А. І. Кунтія [112], огляд місця події в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, сприяє з'ясуванню низки важливих питань:

– на якому об'єкті (на якому конкретно комп'ютері, у якому структурному підрозділі установи) сталася подія;

– до якого виду належить протиправне діяння, що відбулося (кваліфікація кримінального правопорушення);

– у який спосіб вчинено кримінальне правопорушення;

– які сліди чи інші докази вказують на причетність до кримінального правопорушення певної особи;

– яким є під час огляду стан засобів захисту інформації, охорони приміщень, обладнання та низка інших питань.

Поділяючи такий підхід, пропонуємо доповнити цей перелік питаннями, що потребують з'ясуванню в процесі огляду:

– де можуть зберігатися сліди вчинення таких протиправних діянь та їх локалізація;

– характер заподіяної шкоди;

– місце, час й обставини вчинення кримінального правопорушення.

Водночас зауважимо, що перелік питань не може бути вичерпним. Його слід уточнювати залежно від мети проведення огляду й обстановки вчинення кримінального правопорушення.

Першим етапом огляду місця події є підготовчий, що передбачає такі стадії: 1) до виїзду на місце події; 2) після прибуття на місце події [109, с. 74].

До виїзду для проведення огляду місця події необхідно: визначитися зі спеціалістом, який буде залучений до цієї слідчої (розшукової) дії, зі складом слідчо-оперативної групи, іншими учасниками огляду, провести їх інструктаж, проконсультуватися зі спеціалістом стосовно необхідного обладнання (засобів), що будуть використані в процесі проведення огляду, скласти план проведення огляду місця події.

У нескладних випадках, коли йдеться про один комп'ютерний засіб, що знаходиться в особи, можна обмежитися залученням тільки спеціаліста [202, с. 163].

У складних випадках, коли наявні об'єднана комп'ютерна мережа, значна кількість засобів інформаційних-комп'ютерних технологій тощо, доцільно залучати до проведення огляду місця події декількох спеціалістів у галузі інформаційних комп'ютерних технологій, які разом з криміналістом під час проведення слідчої (розшукової) дії доповнюватимуть один одного [202, с. 163].

Стосовно необхідних програмних засобів, які будуть використані під час проведення огляду, О. В. Манжай надає слушні рекомендації, що їх застосування має відповідати двом основним критеріям:

1) бути з відкритою ліцензією або перебувати на балансі правоохоронних органів, щоб можна було перевірити коректність їх роботи;

2) у разі використання відкритого програмного забезпечення необхідно відповідну копію з хеш-сумою диска долучити як додаток до протоколу [130, с. 114].

На наше переконання, необхідно постійно слідкувати за створенням і використанням сучасних програмних засобів у міжнародній практиці з розслідування зазначених протиправних діянь. Передусім це допоможе слідчому, прокурору, дізнавачу орієнтуватися в найефективніших сучасних програмних засобах, а також застосовувати їх під час проведення огляду місця події та інших слідчих (розшукових) дій.

Після прибуття на місце події постає потреба вирішити низку організаційних і технічних питань: 1) забезпечення цілісності й охорони місця проведення огляду події; 2) визначення, що буде об’єктами огляду, їх кількість, специфіка та послідовність проведення; 3) підготовка відповідного обладнання; 4) з’ясування в осіб інформації, якою вони володіють з приводу події.

Необхідно враховувати, що кримінальне процесуальне законодавство України не передбачає обов’язкової участі понятих під час проведення огляду, якщо його проводять не в житловому приміщенні. Аналізуючи окремі положення ч. 7 ст. 223 КПК України, такого висновку дійшов і Верховний Суд колегією суддів Другої судової палати Касаційного кримінального суду у своєму рішенні від 10 грудня 2020 року у справі № 473/2485/17 [171]. Однак огляд житла чи іншого володіння особи слід здійснювати за обов’язковою участю не менше ніж двох понятих незалежно від того, чи застосовують технічні засоби фіксування цієї слідчої (розшукової) дії.

Утім, якщо слідчий, прокурор, дізнавач вважатимуть за доцільне, поняті можуть бути запрошені для участі в проведенні огляду (ч. 7 ст. 223 КПК України)

На практиці переважно запрошують понятих для участі в проведенні огляду місця події з міркувань, що зазначені особи потім можуть бути допитані під час судового розгляду як свідки проведення слідчої (розшукової) дії. На наше переконання, під час розслідування кримінальних правопорушень зазначеної категорії це є тактично виправданим, оскільки своїми показаннями в суді вони сприятимуть підтвердженню зібраних (отриманих) доказів як допустимих.

Слушною є пропозиція В. О. Голубєва запрошувати понятими до огляду в кримінальних правопорушеннях зазначеної категорії осіб, які обізнані з роботою інформаційних комп'ютерних технологій [51, с. 114]. Це слугуватиме не тільки об'єктивності змісту проведення огляду, а й правильному відображенню обставин і фактів, їх належного фіксування в протоколі огляду, що буде мати важливе доказове значення в кримінальному провадженні.

Водночас кожна дія слідчого, прокурора, дізнавача чи спеціаліста повинна бути роз'яснена понятим особам, зокрема має бути роз'яснено її зміст, сутність і мету, а також у разі отримання запитань від понятих – надано відповіді, що обов'язково зазначають у протоколі [122, с. 81].

Процес робочого етапу проведення огляду місця події передбачає дві стадії: статичну та динамічну. Статична стадія полягає в дослідженні та фіксації обстановки місця події та окремих її елементів у тому вигляді, у якому вони знаходилися до початку огляду [104, с. 150].

У процесі огляду місця події на цій стадії необхідно дотримуватися таких рекомендацій [112, с. 881; 134, с. 304]: 1) сфотографувати засіб (засоби) інформаційних комп'ютерних технологій, щоб зафіксувати його (їх) стан; 2) прислухатися і придивитися до системи, щоб визначити, чи працює засіб інформаційно-комп'ютерних технологій; 3) передусім здійснити огляд засобів, що знаходяться в увімкненому стані, детально їх описати та сфотографувати; 4) використовувати в протоколі комп'ютерну термінологію.

Коли повністю здійснено статичний огляд місця події, слід переходити до наступної стадії – динамічної, що полягає у всебічному огляді окремих предметів, у разі необхідності зрушуючи їх з місця [104, с. 150].

У кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, на нашу думку, динамічна стадія пов'язана з безпосереднім обстеженням інформації, яка знаходиться в засобі (засобах) інформаційних комп'ютерних технологій.

У разі встановлення паролю на засобі інформаційно-комп'ютерних технологій за можливості слід з'ясувати пароль користувача, а також установити, чи ввімкнене шифрування диска. У випадку, коли пароль доступу встановити неможливо, необхідно доручити спеціалісту виготовити дамп (копію) оперативної пам'яті з метою відшукання паролів, що зберігаються в ній, до моменту вимкнення [216, с. 39].

Якщо є необхідність вилучити певні апаратні (технічні) пристрої, потрібно дотримуватися таких рекомендацій [122, с. 81; 202, с. 172]:

– перед від'єднанням від живлення комп'ютерної техніки необхідно завершити виконання всіх програм, що працюють на засобі інформаційно-комп'ютерних технологій, оскільки некоректний вихід з них може призвести до втрати доказової інформації або псування програмного забезпечення, що унеможливлює подальше проведення експертизи;

– промаркувати апаратні засоби перед тим, як від'єднати та вилучити;

– від'єднати всі кабелі, попередньо зафіксувавши їх положення (за допомогою фото- чи відеозйомки). Усі кабелі, що з'єднують пристрої комп'ютера, маркують з обох кінців;

– опломбувати корпус апаратного засобу, щоб унеможливити його розкриття;

– упакувати вилучені пристрої.

Слід акцентувати на тому, що за чинним кримінальним процесуальним законодавством України (абз. 3 ч. 2 ст. 168 КПК України) під час проведення огляду заборонено тимчасове вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків: 1) коли їх надання разом з інформацією необхідне для проведення експертизи; 2) якщо такі об'єкти було отримано у зв'язку із вчиненням кримінального правопорушення чи є засобом або знаряддям його вчинення;

3) якщо доступ до них обмежує особа чи необхідно долати системи логічного захисту.

У разі заборони тимчасового вилучення, необхідно за допомогою відповідних засобів виготовити копії інформації. Копіювання такої інформації здійснюють із залученням спеціаліста [121].

Технічно є три способи одержання копій електронних носіїв, що містять сліди вчинення зазначених протиправних діянь:

1) створення образу відповідного носія;

2) створення дубліката носія;

3) логічне копіювання окремих даних [130, с. 116].

У першому випадку за допомогою програмних засобів створюють відповідний образ носія, що зберігається як файл на іншому диску.

У другому випадку здійснюють копіювання даних один в один, унаслідок чого отримують точну копію носія. Такий носій можна безпечно зберігати не побоюючись, що дані може бути зіпсовано.

У третьому випадку здійснюють копіювання окремих файлів, унаслідок чого отримуємо копії, але не структуру носія. Однак, якщо на носії знаходиться прихована інформація, то вона не буде скопійована.

Кожен із зазначених випадків слід застосовувати залежно від конкретної ситуації за рекомендацією спеціаліста.

Попри заборону тимчасового вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку під час проведення огляду, законодавець прописує можливість здійснення їх тимчасового вилучення в разі, якщо вони зазначені в ухвалі суду (абз. 2 ч. 2 ст. 168 КПК України). Здебільшого це стосується випадків, коли проводять огляд житла чи іншого володіння особи за ухвалою слідчого судді.

Заключний етап огляду передбачає: 1) складання протоколу огляду місця події з долученням необхідних до нього додатків; 2) упакування об'єктів, вилучених з місця події, та вжиття заходів щодо їх збереження; 3) вжиття заходів за заявами, що надійшли від учасників огляду місця події [104, с. 152].

Протокол огляду місця події повинен відповідати вимогам, передбаченим у ст. 104 КПК України, і мати три частини: 1) вступну; 2) описову; 3) заключну.

У вступній частині зазначають: місце, час проведення огляду; особу, яка проводить огляд, усіх осіб, які присутні під час проведення огляду (прізвища, імена, по батькові, дати народження, місця проживання).

Складання описової частини протоколу огляду в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, має певну специфіку, окреслену термінологією та особливостями опису засобів інформаційно-комп'ютерних технологій. Тому під час складання протоколу огляду, на нашу думку, слід дотримуватися таких тактичних рекомендацій:

– кожен досліджуваний засіб інформаційних комп'ютерних технологій повинен бути чітко описаний в протоколі (марка, модель, заводський та інвентарний номери, технічні особливості, його місце розташування тощо);

– якщо відбувалося дослідження програмних засобів, необхідно зазначити, як вони були досліджені та в якому саме засобі інформаційно-комп'ютерних технологій;

– окремо зазначати час дослідження кожного засобу інформаційних комп'ютерних технологій;

– важливим є правильний запис усіх серійних номерів, хеш-сум, назв пристроїв тощо;

– у разі використання певних програм для дослідження засобів інформаційних комп'ютерних технологій необхідно зазначити про це;

– особливу цінність для розслідування будуть мати лог-файли (Log file), файли у яких містять інформацію про роботу засобу інформаційних комп'ютерних технологій.

Доцільно все вилучене під час огляду місця події вказувати в заключній частині протоколу, перелічивши за списком. Це полегшить надалі облік вилученого [110, с. 349].

У заключній частині протоколу зазначають про: вилучені документи й речі, виготовлені дублікати документів, а також копії інформації, зокрема комп'ютерних даних, і спосіб їх ідентифікації; спосіб ознайомлення учасників зі змістом протоколу; доповнення та зауваження учасників процесуальної дії до протоколу.

Необхідно пам'ятати, що під час виготовлення оригіналу документа в електронній формі після завершення огляду місця події спеціаліст за дорученням слідчого, дізнавача, прокурора в довільній формі складає письмове пояснення, яке разом з відображенням запису процесуальної дії приєднують як додатки до протоколу огляду місця події [184].

У разі тимчасового вилучення під час огляду електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку та іншого майна (речей, документів тощо), які є доказами кримінального правопорушення, необхідно вжити заходи щодо їх збереження. У такому випадку слід діяти відповідно до ч. 5 ст. 171 КПК України. Прокурор або слідчий за погодженням із прокурором не пізніше ніж наступного дня після вилучення майна мають звернутися до слідчого судді з клопотанням про арешт майна з метою збереження речових доказів, проведення експертного дослідження чи подолання системи логічного захисту. Сталою є практика, що перед зверненням з відповідним клопотанням до слідчого судді тимчасово вилучене майно постановою слідчого, прокурора долучають до кримінального провадження як речовий доказ і постанову долучають як додаток до клопотання. Важливо, що постановою слідчого, прокурора як речовий доказ до кримінального провадження також долучають засоби інформаційних комп'ютерних технологій, що вилучені на підставі ухвали слідчого судді про проведення огляду. Винесенню постанови передує проведення детального огляду вилученого майна, якщо під час проведення огляду місця події це не зробили.

Ще однією ефективною слідчою (розшуковою) дією в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, є *обшук*.

Відповідно до статистичних даних, 2018 року в зареєстрованих кримінальних правопорушеннях слідчі судді першої інстанції розглянули 95 524 клопотання про проведення обшуку, задоволено 72 764 клопотань; 2019 року – 94 608, задоволено – 69 712; 2020-го – 96 904, задоволено – 71 200, 2021 року – 98 657, задоволено – 72 501 [233].

Такі дані засвідчують, що обшук є однією з поширених слідчих (розшукових) дій, яку слідчі та прокурори використовують для виявлення, фіксації та вилучення доказової інформації, що має значення для з'ясування обставин вчинення кримінального правопорушення, встановлення осіб, які його вчинили.

Обшук схожий на огляд. Зазначені слідчі (розшукові) дії мають спільну мету проведення – виявлення та фіксація відомостей про обставини вчинення кримінального правопорушення.

Водночас обшуку притаманні певні процесуальні й тактичні особливості, зокрема мета обшуку є конкретнішою та передбачає також відшукання засобів чи знарядь кримінального правопорушення або майна, яке було здобуте внаслідок його вчинення, а також встановлення місцеперебування розшукуваної особи. Проведення обшуку має примусовий характер і чітко визначені процесуальні особливості.

З огляду на це й розглянемо специфіку проведення обшуку в зазначених кримінальних правопорушеннях.

Дослідивши наявні у вітчизняній криміналістичній літературі визначення обшуку [108, с. 365; 112, с. 386; 214, с. 346], можна дійти висновку, що вони суттєво не різняться. Учені-криміналісти мають спільний підхід стосовно того, що обшук – це слідча (розшукова) дія, що полягає в примусовому обстеженні приміщень, а також інших об'єктів та окремих громадян з метою виявлення та фіксації відомостей про обставини кримінального правопорушення, відшукання та вилучення знарядь або майна (речей і цінностей), яке було здобуте внаслідок його вчинення, а також установлення місцезнаходження розшукуваної особи.

Свого часу з приводу проведення обшуку Г. Гросс зауважував, що хто буде обмежуватися обшуком ящиків і скринь, ліжок, димоходів, той навряд чи що-

небудь знайде. Необхідно обшукувати всі місця без винятку, все доступне погляду, оскільки немає предметів, у яких не можна було б заховати щось, що має значення для справи (кримінального провадження) [47, с. 169].

Підставами, що передують прийняттю рішення про проведення обшуку, є наявність достатніх даних, які дають змогу вважати, що в певному місці або в певної особи знаходяться речі, документи або відомості, які можуть у них міститися і мають значення для досудового розслідування, а отримати їх у добровільному порядку шляхом витребування або за допомогою проведення інших слідчих дій неможливо, а також необхідності доступу до осіб, яких планують відшукати (п. 8 ч. 3 ст. 234 КПК України).

Процесуальними підставами проведення обшуку є ухвала слідчого судді. Отриманню такої ухвали передує звернення слідчого за погодженням з прокурором або прокурором з відповідним клопотанням, яке має бути складене з дотриманням вимог ч. 3 ст. 234 КПК України.

Однак у невідкладних випадках, передбачених ч. 3 ст. 233 КПК України, слідчий, дізнавач, прокурор мають право до постановлення ухвали слідчого судді ввійти до житла чи іншого володіння особи. Після цього необхідно невідкладно звернутися до слідчого судді з відповідним клопотанням (ч. 3 ст. 233 КПК України).

У практичній діяльності невідкладність проведення обшуку обґрунтовують у постанові, на підставі якої і проводять обшук. Нерідко постають питання, чи була необхідність терміново (невідкладно) провести обшук у конкретному провадженні та чи не було допущено порушення прав особи. На зловживанні невідкладністю проведення обшуку неодноразово акцентував Європейський суд з прав людини (ЄСПЛ) у своїх рішеннях. Зокрема, у справі «Кузьмінас проти Росії» (заява № 69810/11) [290] Суд зазначив, що ніщо не засвідчувало твердження слідчого про те, що непроведення термінового обшуку може призвести до втрати матеріалів, які стосуються розслідування. ЄСПЛ дійшов висновку, що було порушено ст. 8 (Право на повагу до приватного і сімейного життя) Конвенції про захист прав людини і основоположних свобод.

Серед тактичних особливостей проведення обшуку в кримінальних правопорушеннях, вчинених з використанням інформаційних комп'ютерних технологій, можна виокремити такі:

1) дотримання принципу раптовості під час прибуття та входження до приміщення, у якому буде проведено обшук;

2) заборона використання для пошуку тайників з магнітними носіями металошукачів або рентгенівської установки, оскільки це може призвести до знищення інформації на носіях;

3) необхідність швидко опрацювання значного обсягу виявленої інформації з метою встановлення її цінності для розслідування;

4) проведення обшуку лише на одному або декількох засобах інформаційно-комп'ютерних технологій, що належать до локальної мережі [126, с. 480].

На наш погляд, доповнити цей перелік можна такими тактичними та процесуальними особливостями:

– у клопотанні про обшук слід чітко визначити засоби інформаційно-комп'ютерних технологій, які необхідно відшукати, а до проведення обшуку ознайомитися з їх характеристикою;

– якщо під час обшуку виявлено доступ чи можливість доступу до засобів інформаційних комп'ютерних технологій, які не зазначені в ухвалі слідчого судді, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, слідчий, прокурор має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них містяться, на місці проведення обшуку. У разі їх вилучення такі речі вважають тимчасово вилученим майном (ч. 6 ст. 236 КПК України);

– у переважній більшості обшук у приміщеннях підприємств, установ, організацій необхідно розпочинати після початку робочого часу, оскільки в цей час більшість осіб перебуває на робочих місцях з увімкненими засобами інформаційних комп'ютерних технологій [299, с. 74];

– встановлення психологічного контакту з особою, у якої проводять обшук;

– спрямувати увагу на всі пристрої збереження даних (флешки, диски тощо);

– у разі необхідності провести груповий обшук.

Зауважимо, що цей перелік не є вичерпним і може бути доповнений залежно від виду розслідуваного кримінального правопорушення зазначеної категорії (до прикладу: розслідування злочинів проти основ національної безпеки України, проти власності тощо, вчинених з використанням інформаційних комп'ютерних технологій), відповідної слідчої ситуації та інших обставин. У більшості випадків під час проведення обшуку застосовують такі тактичні особливості, як і під час проведення огляду.

Ухвала слідчого судді про дозвіл на обшук житла чи іншого володіння особи надає право проникнути до житла чи іншого володіння особи лише один раз, а строк дії такої ухвали не може перевищувати одного місяця з дня її постановлення (ст. 235 КПК України).

Тому з метою забезпечення результативності проведення обшуку в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, необхідно ретельно його планувати заздалегідь. Під час планування проведення обшуку в зазначених кримінальних правопорушеннях не виключаємо можливість застосування ШІ.

Ще однією поширеною слідчою (розшуковою) дією під час розслідування кримінальних правопорушень окресленої категорії, що дає змогу отримати нові чи перевірити наявні докази, а також перевірити інформацію, отриману з інших джерел, є *допит*.

У вітчизняній криміналістичній літературі пропонують різні визначення поняття допиту. Не маючи за основну мету досліджувати їх детально, зазначимо, що ми поділяємо думку В. Ю. Шепітька, який тлумачить допит як процесуальну слідчу (розшукову) дію, що чітко передбачена кримінальними процесуальними положеннями й інформаційно-психологічним процесом спілкування осіб, а також спрямована на отримання інформації про факти, що мають значення для розслідування [114, с. 328].

Основними завданнями проведення допиту є: 1) отримання відомостей про кримінальне правопорушення; 2) перевірка вже відомих відомостей; 3) отримання

фактичних даних про спосіб вчинення та відомостей про знаряддя вчинення; 4) перевірка висунутих версій; 5) збирання відомостей про особу злочинця та його місцеперебування [112, с. 340–341].

Ефективність проведення зазначеної слідчої (розшукової) дії залежить насамперед від дотримання низки криміналістичних принципів:

1. Активність допиту – особа, яка проводить допит, є ініціатором спілкування та за допомогою процесуальних і тактичних засобів намагається отримати правдиві показання, а не просто бути реєстратором інформації.

2. Цілеспрямованість допиту – кожен допит повинен мати чітко визначену мету для одержання конкретної інформації про подію кримінального правопорушення.

3. Об'єктивність і повнота допиту – особа, яка проводить допит, не вправі на власний розсуд змінювати, скорочувати отримані показання та доповнювати їх відповідно до своїх уявлень, а також нав'язувати допитуваному ці уявлення [104, с. 172].

Необхідно зосередити увагу на своєчасності проведення допиту, про що також зауважував у своїх рішеннях ЄСПЛ. Зокрема, у рішеннях ЄСПЛ «Бєлоусов проти України» [207] і «Вергельський проти України» [208] було зазначено, що через несвоєчасність проведення допиту він був неефективним, оскільки з плином часу свідки вже не могли пригадати подробиць відповідних подій.

Тому, на нашу думку, необхідно акцентувати й на оперативності та своєчасності проведення допиту в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій.

У криміналістичній літературі пропонують різні класифікації допиту, значущість яких обумовлена як процесуальними, так і тактичними особливостями їх проведення. Розглянемо особливості допиту потерпілого та підозрюваного в зазначених категоріях кримінальних правопорушень.

У криміналістичній літературі проведення допиту має такі етапи: підготовка, проведення (робочий етап) і фіксація.

Безперечно, що однією з умов успішного проведення допиту потерпілого та підозрюваного під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій, є підготовка до його проведення.

Слушно зауважує В. Ю. Шепітько, що підготовкою до допиту слугує ретельне вивчення матеріалів кримінального провадження. Вивчення даних, що знаходяться в протоколі огляду місця події та обшуку, дає змогу виявити окремі психологічні риси особистості допитуваного: його рішучість або обачливість, сміливість і боягузливість, навички та звички, жорстокість, цинізм, схильності тощо [108, с. 334–335].

Поділяючи таку думку, зазначимо, що в процесі проведення огляду місця події чи обшуку можна встановити певні відмітні риси потерпілого й підозрюваного в зазначених кримінальних правопорушеннях. Наприклад, дослідження засобу інформаційних комп'ютерних технологій, який належить потерпілому чи підозрюваному, під час проведення огляду місця події чи обшуку надасть можливість сформувати уявну картину про особу потерпілого чи підозрюваного, встановити його вподобання, «професійні звички» і «почерк» за наявними даними в засобі (ігри, застосунки, сайти тощо). Це згодом сприятиме встановленню з допитуваною особою психологічного контакту, обранню відповідної тактики допиту й застосування тактичних прийомів під час допиту.

Загалом у криміналістичній літературі, що стосується розслідування зазначених кримінальних правопорушень, є різні рекомендації щодо підготовки до допиту [12, с. 160; 51, с. 129], серед яких виокремимо такі:

1) скласти план проведення допиту;

2) обрати місце та час проведення допиту, його послідовність стосовно інших слідчих (розшукових) дій;

3) проконсультуватися зі спеціалістами, оглянути вилучену техніку, ознайомитися з принципом її дії.

З приводу планування допиту В. О. Коновалова слушно зазначає, що наявність плану дає змогу одразу правильно та всебічно визначити коло питань, які

необхідно з’ясувати. Під час складання плану допиту необхідно керуватися обставинами, що підлягають перевірці відповідно до загального плану розслідування [102, с. 50–51].

Не виключаємо можливості під час планування допиту використовувати штучний інтелект, який слідчий, дізнавач, прокурор зможуть використовувати як під час підготовки до допиту, так і під час його проведення. Штучний інтелект буде рекомендувати, які питання необхідно ставити залежно від виду та специфіки розслідування кримінального правопорушення та спрямовувати перебіг допиту в ефективне русло.

Місце та час проведення допиту визначають з огляду на важливість відомостей, якими володіє допитувана особа, його процесуальне становище, зв’язки з іншими особами, які підлягають допиту в провадженні [53, с. 82].

Необхідно також обрати, яким способом будуть здійснювати виклик потерпілого й підозрюваного на допит, оскільки це має вагоме тактичне значення. У кримінальному процесуальному законодавстві (ст. 135 КПК України) чітко регламентовано порядок виклику. Залежно від слідчої ситуації, мети проведення допиту тощо слідчий, дізнавач, прокурор можуть обрати найраціональніший порядок здійснення виклику.

Варто наголосити, що під час розслідування зазначених кримінальних правопорушень можуть застосовуватися різні види запобіжних заходів, зокрема і такий винятковий – як тримання під вартою. При застосуванні такого запобіжного заходу, необхідно враховувати різні обставини кримінального провадження, у тому числі, як доречно зазначають науковці, звертати увагу і на стан здоров’я підозрюваної особи [288, с. 3031].

Особливо важливого значення має спілкування зі спеціалістом перед проведення допиту. Доречно залучати його і на наступних етапах проведення допиту (робочого та фіксації), оскільки у слідчого, дізнавача та прокурора існує недостатній технічний рівень знань щодо особливостей функціонування засобів інформаційних комп’ютерних технологій, їх апаратної та програмної складової [151, с. 254].

Присутність спеціаліста під час допиту надасть упевненості слідчому, дізнавачу, прокурору, оскільки вони зможуть за потреби звернутися до нього за консультацією, а також створить додатковий психологічний стимул підозрюваному, потерпілому повідомляти правдиву інформацію, оскільки вони розумітимуть, що спеціаліст володіє необхідним обсягом знань і неправдиві показання буде викрито [247, с. 136–137].

Крім того, якщо слідчий, дізнавач, прокурор почали ставити запитання, які не мають вагомого значення в кримінальному провадженні, чи допит зайшов у глухий кут, спеціаліст своєю порадою чи запитаннями до підозрюваного, потерпілого може спрямувати перебіг допиту в потрібному напрямі [151, с. 254].

Без участі спеціаліста неможливо здійснити належну фіксацію ходу та результатів допиту, оскільки саме він допомагає його фіксувати та зазначає, які технічні засоби, прилади було використано.

На нашу думку, під час підготовки до допиту в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, також необхідно [151, с. 254]:

– ураховувати наявність у потерпілого та підозрюваного досвіду роботи зі створення комп'ютерних програм певного класу;

– зважати на інформацію про потерпілого й підозрюваного, яка є в соціальних мережах, їх псевдоніми (нікнейми), коло знайомств, які фотокартки профілю використовують тощо;

– брати до уваги «професійні (злочинні) звички» та «почерк» (використання конкретної марки техніки, до яких склалася звичка користуванням, застосування конкретної операційної системи, програм, які особа використовувала протягом тривалого часу й віддає саме їм перевагу, тощо).

На робочому етапі проведення допиту застосовують тактичні прийоми, що сприяють отриманню повних і правдивих показань.

Серед основних тактичних прийомів, які можуть бути застосовані під час проведення допиту потерпілого в зазначених кримінальних правопорушеннях, є: 1) встановити психологічний контакт; 2) ретельно продумати запитання в

підготовленому порядку; 3) усунути у свідченнях неточності; 4) актуалізувати забуте в пам'яті; 5) уточнити свідчення [58, с. 125].

Більшість із зазначених тактичних прийомів може бути використано й під час допиту підозрюваної особи. Однак, зазначає В. О. Коновалова, усе залежить від ситуації, що складається під час допиту підозрюваного, – конфліктна чи безконфліктна. Вчена слушно пропонує в конфліктних ситуаціях роз'яснювати підозрюваному характер і міру його відповідальності за вчинене кримінальне правопорушення, що буде спонукати надавати правдиві показання [102, с. 91–92].

Розглянемо окремі тактичні прийоми проведення допиту потерпілого та підозрюваного в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій.

Частково поділяємо думку В. О. Коновалової та В. Ю. Шепітька, що психологічний контакт – це найсприятливіша атмосфера допиту, що позитивно позначається на взаємодії та відносинах між учасниками, певному налаштуванню на спілкування. Психологічний контакт завжди є двостороннім, його встановлення та підтримання залежать як від слідчого, дізнавача, прокурора, так і від допитуваного. Проте ініціатива має належати особам, які проводять допит [101, с. 99–100].

Водночас у зазначених кримінальних правопорушеннях під час проведення допиту підозрюваного та потерпілого є певні особливості у встановленні психологічного контакту між його учасниками [155, с. 255].

З огляду на реалії сьогодення, зокрема те, що слідчі, дізнавачі та прокурори не мають достатніх знань і навичок у технічній сфері, тому здебільшого й залучають спеціалістів для проведення допиту.

Особливість встановлення психологічного контакту полягає в тому, що він може виникати між слідчим і потерпілим/підозрюваним, з одного боку, а також між спеціалістом і потерпілим/підозрюваним – з іншого.

Нерідко складаються ситуації, що психологічний контакт налагоджується саме між спеціалістом і підозрюваним, чому сприяє розуміння ними технічної складової під час спілкування. Водночас неповне розуміння слідчим, дізнавачем,

прокурором усіх технічних нюансів, пов’язаних із використанням інформаційних комп’ютерних технологій, може дратувати підозрюваного, чим буде порушуватися атмосфера допиту та створюватися конфліктна ситуація [155, с. 255].

Тому необхідно створити атмосферу, за якої в підозрюваного й потерпілого під час допиту сформується повага до слідчого, дізнавача, прокурора. Цього може бути досягнуто завдяки:

1) ретельній підготовці до допиту в зазначених категоріях кримінальних правопорушень;

2) обговоренню заздалегідь зі спеціалістом питань, на яких буде акцентовано в процесі допиту;

3) розумінню питань, що ставитиме спеціаліст під час допиту;

4) активності й інтересу слідчого, дізнавача, прокурора у з’ясуванні всіх технічних обставин кримінального правопорушення;

5) проведенню допиту відповідно до обговореного зі спеціалістом плану [155, с. 255].

Також для встановлення психологічного контакту можуть застосовувати такі тактичні прийоми:

а) розмова з допитуваним на теми, що його цікавлять (розмова про комп’ютерні ігри, соціальні мережі, про певний розважальний контент тощо);

б) демонстрування поінформованості про обставини життя допитуваного, його потреби й інтереси (захоплення, хобі тощо);

в) створення позитивної думки в допитуваного щодо особи, яка проводить допит [112, с. 345].

Наступним тактичним прийомом є ретельна підготовка запитань у визначеному порядку. Це надасть можливість отримати більш повну інформацію від допитуваного про відомі йому факти, що мають значення для з’ясування обставин у кримінальному провадженні, а також уникнути проведення повторного допиту з одних і тих самих обставин. Залежно від мети та змісту поставлених запитань у криміналістиці їх поділяють на:

– основні (спрямовані на з’ясування головних відомостей);

– доповнювальні (спрямовані на з'ясування додаткових фактів);

– уточнювальні (ставлять у тому разі, коли допитуваний повідомив інформацію неповно);

– нагадувальні (мають на меті активізувати в пам'яті допитуваного певні асоціації);

– контрольні (спрямовані на перевірку правильності інформації) [112, с. 347].

У кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, достатньо складно перелічити всі ймовірні запитання, які можуть ставити підозрюваному чи потерпілому, оскільки необхідно враховувати особливості й види зазначених кримінальних правопорушень (про які йшлося в підрозділі 1.2), конкретні слідчі ситуації та інші обставини кримінального правопорушення.

Натомість виокремимо основні питання, які можуть ставити потерпілому та підозрюваному під час допиту в зазначених кримінальних правопорушеннях: 1) чи виявляв хто інтерес до інформації, що знаходиться в засобах інформаційних комп'ютерних технологій; 2) які дії на засобі інформаційних комп'ютерних технологій проводили до вчинення кримінального правопорушення (відкриття електронних листів, завантаження програм, відкриття сайтів тощо); 3) як було з'ясовано про вчинене кримінальне правопорушення (час, місце); 4) які дії було вчинено під час виявлення ознак кримінального правопорушення; 5) які докази можуть бути надані для підтвердження власних слів; 6) хто, на думку потерпілого, міг вчинити протиправні дії; 7) призначення засобів інформаційних комп'ютерних технологій (для службового використання, особистого користування, надання відповідних послуг тощо); 8) чи не з'являлися в приміщенні, де розміщені засоби інформаційних комп'ютерних технологій, сторонні особи, 9) хто мав доступ до засобів інформаційних комп'ютерних технологій; 10) чи відбувалося використання антивірусних програм на засобах інформаційних комп'ютерних технологій; 11) чи використовували неліцензійне програмне забезпечення; 12) якою є шкода, заподіяна вчиненим кримінальним правопорушенням, і її розмір.

Під час допиту підозрюваного насамперед необхідно з'ясувати:

– відомості про нього (анкетні дані), крім прізвища, імені та по батькові, дату народження, місце реєстрації та фактичного проживання, сімейний стан і наявність засобів зв'язку;

– яку освіту має, де її отримав, місце та час навчання;

– де, ким, на якій посаді працював і чи працює нині;

– як здобув відповідні навички роботи на засобах інформаційно-комп'ютерних технологій (навчання в освітньому закладі за відповідною спеціальністю, у зв'язку із професійною діяльністю, самонавчання тощо);

– які апаратні та програмні засоби здебільшого він використовував (марка комп'ютерної техніки, мова програмування, вид операційної системи, якими сервісами користувався тощо);

– рівень володіння засобами інформаційних технологій;

– місце, дата та час вчинення кримінального правопорушення;

– мета/мотив вчинення;

– чи попередньо планувалося вчинення протиправних дій;

– як дізнався про потерпілого/чому обрав саме його;

– до якої інформації має доступ та як її отримав;

– що надалі планував робити з інформацією, яку викрав (зокрема якщо об'єктом посягання є інформація);

– у який спосіб передавав отриману (викрадену) інформацію третім особам (якщо об'єктом посягання є інформація);

– чи може надати інформацію про використання інтернет ресурсів (паролі на сайтах, нікнейми, якими сайтами користувався тощо);

– як отримав (створив, удосконалив, придбав тощо) шкідливе програмне забезпечення та як використав чи планував його використати;

– як здійснював знищення слідів протиправного діяння та які засоби анонімізації використовував;

– які особи та як сприяли вчиненню кримінального правопорушення;

– чи має причетність до інших кримінальних правопорушень.

Обов’язково необхідно враховувати, що допит не може тривати без перерви понад дві години, а загалом – понад вісім годин на день (ч. 2 ст. 224 КПК України).

Оскільки під час розслідування кримінальних правопорушень, вчинених з використанням інформаційних комп’ютерних технологій, може виникати необхідність у допиті малолітньої чи неповнолітньої особи, акцентуємо на певних тактичних рекомендаціях, які необхідно застосовувати під час проведення допиту такої категорії осіб. Насамперед необхідно звертатися спокійним тоном, уникаючи емоцій незалежно від змісту питань, говорити повільно, формулювати стислі питання, використовувати фрази, які малолітній чи неповнолітній застосував у своїй розмові, надати можливість цілком висловитися про події, що сталися, використовувати в питаннях лише активну форму дієслова, подякувати за взаємодію [200, с. 33].

Доречно також застосовувати методику «зеленої кімнати», що полягає в проведенні допиту малолітнього чи неповнолітнього з огляду на їхні вікові та психологічні особливості та в умовах, що мінімізують або не допускають повторного травмування психіки [200, с. 42].

Такий допит малолітнього та неповнолітнього відбувається в присутності законного представника, психолога або педагога, а за необхідності – лікаря (ч. 1 ст. 226 КПК України), а також не може тривати без перерви понад одну годину, а загалом – понад дві години на день (ч. 2 ст. 226 КПК України).

Однак кримінальне процесуальне законодавство України не враховує ряд інших процесуальних особливостей стосовно допиту малолітніх чи неповнолітніх осіб. З цього приводу підтримуємо думку О.В. Капліної, О.П. Кучинської та О.М. Крукевич [289, с. 275], які зауважують про законодавче закріплення положень, що стосуються чіткого порядку залучення органом досудового розслідування педагога, психолога та лікаря, які беруть безпосередню участь у допиті малолітніх або неповнолітніх свідків. Такі зміни покращили б якість надання необхідної допомоги неповнолітнім та малолітнім свідкам та відповідали міжнародним стандартам.

Заключним етапом є фіксація проведення допиту. Основним засобом фіксації перебігу та результатів допиту є протокол допиту. Такий протокол складають згідно з вимогами, передбаченими ст. 104 КПК України. Слід зазначити, що в разі фіксації допиту за допомогою технічних засобів текст показань можуть не вносити до протоколу, якщо ніхто з учасників цієї процесуальної дії не наполягає на цьому. У такому разі в протоколі зазначають, що показання зафіксовано на носії інформації, який додають до нього (ст. 104 КПК України).

У чітко визначених випадках можуть проводити допит у режимі відеоконференції. Цими випадками є: 1) неможливість безпосередньої участі осіб за станом здоров'я або з інших поважних причин; 2) необхідність забезпечення безпеки осіб; 3) проведення допиту малолітнього або неповнолітнього свідка, потерпілого; 4) необхідність ужиття таких заходів для забезпечення оперативності досудового розслідування; 5) наявність інших підстав, визнаних слідчим, прокурором достатніми (ч. 1 ст. 232 КПК України).

Зазначений перелік не є вичерпним і може бути продовжений з огляду на специфіку розслідуваної категорії кримінальних правопорушень.

Зважаючи на висловлені в криміналістичній літературі думки щодо можливості проведення допиту під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, у режимі відеоконференції, можна виокремити такі тактичні особливості її підготовки та фіксації.

На стадії підготовки до допиту в режимі відеоконференції слід [90; 144; 250, с. 203]: 1) визначити коло осіб, яких необхідно допитати чи залучити для проведення допиту (спеціалісти, психологи, педагоги); 2) підібрати та перевірити відповідні технічні засоби (комп'ютерна техніка, перевірка наявності вільного місця на носії інформації тощо), а також забезпечити інформаційну безпеку, щоб не допустити втрату чи витік отриманої інформації; 3) визначитися з місцем проведення допиту в режимі відеоконференції; 4) повідомити всіх учасників про проведення допиту; 5) проконсультуватися зі спеціалістом й окреслити коло

значущих питань, які необхідно з'ясувати під час проведення допиту, а також їх послідовність.

Під час допиту можна використовувати спеціальні програмні засоби або загальнопоширені програми (наприклад Discord). Також можна залучити мережеві протоколи доступу: а) загальні (наприклад, взаємодія мереж Windows і UNIX, а також зв'язок в Інтернеті через мережевий протокол TCP/IP; для роботи служби телеконференцій Usenet – мережевий протокол NNTP (Network News Transfer Protocol); б) спеціально виділену лінію для правоохоронних органів [135, с. 337].

На стадії фіксації допиту в режимі відеоконференції необхідно: 1) здійснити запис відеограми на носії відеозапису; 2) створити архівну та робочу копії відеограми; 3) перевірити якість обох копій; 4) долучити робочу й архівну копії до матеріалів кримінального провадження [250, с. 203].

Слід зауважити, що ефективність проведення зазначеної слідчої (розшукової) дії залежить від справності та сучасності засобів інформаційно-комп'ютерних технологій, які застосовують, а також швидкості передання інформації [250, с. 203].

Якщо слідчий, прокурор не можуть провести допит у режимі відеоконференції, слід скористатися положеннями ч. 11 ст. 232 КПК України та провести опитування особи в режимі відео- або телефонної конференції для встановлення відомостей, які мають значення для кримінального провадження. Однак обставини, що були повідомлені особою під час опитування, не мають доказового значення, а є тільки орієнтовною інформацією для висунення версій та побудови тактики розслідування.

Здебільшого проведення допиту в режимі відеоконференції є одним з ефективних засобів збирання доказової інформації в умовах воєнного стану.

Згідно із Законом України «Про правовий режим воєнного стану» [195], воєнним станом вважають особливий правовий режим, що вводиться в Україні в разі збройної агресії.

У КПК України є розділ IX-1 «Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану», який містить положення проведення процесуальних дій в умовах воєнного стану.

У науковій літературі [237, с. 50] аргументовано зауважують, що введення в дію одного з особливих правових режимів (воєнного стану) не зумовлює автоматичного запровадження особливого режиму досудового розслідування, оскільки фактичною підставою для запровадження останнього є об'єктивна неможливість здійснення досудового розслідування у звичайному порядку.

Водночас, крім особливостей, визначених у ст. 615 КПК України, кримінальне провадження здійснюють з дотриманням загальних норм КПК України.

Однією з таких особливостей досудового розслідування є його початок. У разі відсутності технічної можливості доступу до ЄРДР рішення про початок досудового розслідування приймає слідчий, дізнавач, прокурор, про що виносить відповідну постанову, а відомості, що підлягають внесенню до ЄРДР, вносять за першої можливості. У невідкладних випадках до винесення дізнавачем, слідчим, прокурором постанови про початок досудового розслідування може бути проведено огляд місця події (постанову приймають невідкладно після завершення огляду) (п. 1 ч. 1 ст. 615 КПК України).

Ураховуючи режим воєнного стану, слідчий, дізнавач, прокурор не завжди мають можливість виїхати для проведення огляду місця події.

На наш погляд, можна виокремити такі тактичні рекомендації проведення огляду місця події в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, під час воєнного стану [144, с. 295; 237, с. 53; 248, с. 149].

По-перше, необхідно своєчасно створити слідчо-оперативну групу, визначити її кількісний і якісний склад та керівника, належно оформити це процесуально, раціонально розподілити функціональні обов'язки членів групи та створити ефективну систему обміну інформацією, підготувати необхідні технічні засоби й визначитися зі спеціалістом, який буде залучений до проведення огляду.

По-друге, перед виїздом на місце події для проведення огляду необхідно попередити військовослужбовців, які дислокуються на зазначеній території та які повинні супроводжувати слідчо-оперативну групу.

По-третє, якщо є небезпека в районі проведення огляду та неможливо його провести, тоді військові самі повинні доставити комп'ютерну техніку в найближче безпечне місце для його огляду. Однак перед цим необхідно проінструктувати військовослужбовців про порядок поводження із засобами інформаційних комп'ютерних технологій та налагодити постійний зв'язок з ними.

З огляду на істотне збільшення в умовах воєнного стану кількості виявів пропаганди, спаму, розповсюдження шкідливого програмного забезпечення в різних електронних середовищах: Instagram, Telegram, Facebook, Viber, вебсайтах тощо, постає питання щодо оперативного фіксування таких протиправних дій. Через специфіку зазначеної категорії кримінальних правопорушень не завжди постає потреба у виїзді на місце події для фіксації таких дій, оскільки їх вчиняють у кіберпросторі [144, с. 297].

Пропонуємо вдосконалити процес відеозапису екрана, створивши для слідчого операційну систему на базі Linux і додаткову програму для фіксації протиправних дій. Така програма має фіксувати всі дії слідчого з дослідження та фіксації доказової інформації, що залишена в електронному середовищі. Зокрема, програма повинна зафіксувати момент входу до операційної системи, відкриття відповідних програм фіксації, час здійснення дії, який ресурс досліджують тощо. Отримані дані відеозапису (компакт-диск, флешка) мають долучати до протоколу огляду [144, с. 297].

Одним із засобів, що допомагає отримати докази, які самостійно або в сукупності з іншими доказами можуть мати істотне значення для з'ясування обставин кримінального правопорушення, а також для встановлення осіб, які вчинили кримінальне правопорушення, є проведення *негласних слідчих (розшукових) дій*.

Процесуальні аспекти проведення негласних слідчих (розшукових) дій прописано в главі 21 КПК України. Зазначимо про деякі з них.

Негласними слідчими (розшуковими) діями є різновид слідчих (розшукових) дій, відомості про факт і методи проведення яких не підлягають розголошенню, за

винятком якщо відбулося тимчасове обмеження конституційних прав осіб під час проведення таких дій.

На нашу думку, цілком правильно висвітлює сутність негласних слідчих (розшукових) дій Д. Б. Сергєєва, яка пропонуємо визначати їх як «заходи, що складаються із сукупності пошуково-пізнавальних і посвідчувальних прийомів, відомості про факт та методи проведення яких не підлягають розголошенню, проводяться відповідним суб'єктом з метою виявлення та закріплення фактичних даних і відомостей про їх джерела для отримання доказів у кримінальному провадженні та їх перевірки» [222, с. 227–228; 223].

За кримінальним процесуальним законом негласні слідчі (розшукові) дії поділяють на дві групи. До першої належать ті, які пов'язані з втручанням у приватне спілкування (§2 глави 21): 1) аудіо-, відеоконтроль особи (ст. 260 КПК України); 2) арешт, огляд і виїмка кореспонденції (ст. 261–262); 3) зняття інформації з електронних комунікаційних мереж (ст. 263); 4) зняття інформації з електронних інформаційних систем (ст. 264 КПК України).

До другої групи належать інші негласні слідчі (розшукові) дії (§3 глави 21): 1) обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК України); 2) установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ст. 268 КПК України); 3) спостереження за місцем, річчю або особою (ст. 269 КПК України); 4) моніторинг банківських рахунків (ст. 269-1 КПК України); 5) аудіо-, відеоконтроль місця (ст. 270 КПК України); 6) контроль за вчиненням злочину (ст. 271 КПК України): а) контрольована поставка; б) контрольована та оперативна закупка; в) спеціальний слідчий експеримент; г) імітування обстановки злочину; 7) виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК України); 8) негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК України).

У більшості випадків для проведення негласних слідчих (розшукових) дій необхідна ухвала слідчого судді апеляційного суду (ст. 247 КПК України).

Необхідність проведення негласних слідчих (розшукових) дій під час досудового розслідування як у традиційних кримінальних правопорушеннях, так і тих, що вчиняються з використанням інформаційних технологій, ініціює слідчий, прокурор у разі, якщо встановлена неможливість отримати відомості про кримінальне правопорушення та особу, яка його вчинила, в інший спосіб (ч. 2 ст. 246 КПК України). Тобто законодавчо закріплено виключність цього способу збирання та перевірки доказів у кримінальному провадженні.

У разі неможливості отримати відомості про кримінальне правопорушення та особу, яка його вчинила, в інший спосіб, слідчий, прокурор в обов'язковому порядку повинні обґрунтувати це у відповідному клопотанні, з яким вони звертаються до слідчого судді (п. 7 ч. 2 ст. 248 КПК України). На цьому акцентує і ЄСПЛ. Зокрема, у рішенні «Матанович проти Хорватії» від 4 квітня 2017 року Суд зауважив, що рішення про застосування таємних заходів спостереження ґрунтувалося лише на встановленому законом вислові «розслідування не могло проводитися за допомогою інших засобів, або це було б надзвичайно складно». Проте відповідного обґрунтування щодо особливих обставин справи, а також чому слідство не могло бути проведене за допомогою застосування інших менш суворих засобів, не було (п. 112–114 рішення) [209]. Суд дійшов висновку, що було порушено ст. 8 Конвенції про захист прав людини і основоположних свобод (право на повагу до приватного і сімейного життя).

Ми поділяємо думку М. А. Погорецького, який на підставі аналізу положень статей КПК України виокремлює два види негласних слідчих (розшукових) дій:

а) які проводять виключно в кримінальному провадженні щодо тяжких або особливо тяжких злочинів: ст. 260, 261, 263, 264 (у частині дій, що проводять на підставі ухвали слідчого судді), 267, 269, 269-1, 270, 271, 272, 274 КПК України;

б) які проводять незалежно від тяжкості злочину [168, с. 56–57], а отже, їх можуть проводити в усіх без винятку кримінальних правопорушеннях: ч. 2 ст. 264, ст. 268 КПК України.

Потрібно також зазначити, що загальні засади й вимоги до організації проведення негласних слідчих (розшукових) дій, а також використання їх

результатів у кримінальному провадженні визначено в міжвідомчій Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні [192].

Законодавець дозволяє проведення негласних слідчих (розшукових) дій до винесення відповідної ухвали слідчого судді, якщо це пов'язано із врятуванням життя людей та запобіганням вчиненню тяжких чи особливо тяжких злочинів, передбачених розділами I, II, VI, VII (ст. 201 та 209), IX, XIII, XIV, XV, XVII Особливої частини КК України. У такому випадку проведення негласної слідчої (розшукової) дії розпочинається на підставі постанови прокурора або постанови слідчого, погодженої з прокурором. Проте відсутність погодження постанови слідчого прокурором свідчитиме про незаконність проведення таких дій. Після початку негласної слідчої (розшукової) дії прокурор зобов'язаний невідкладно звернутися до слідчого судді з відповідним клопотанням. У разі відмови слідчого судді в задоволенні клопотання відбувається негайне припинення негласних заходів і знищення вже отриманої інформації (ст. 250 КПК України).

За вітчизняним кримінальним процесуальним законодавством правом на проведення негласних слідчих (розшукових) дій наділено слідчого, який здійснює досудове розслідування кримінального правопорушення, або за його дорученням їх проведення можуть здійснювати уповноважені оперативні підрозділи, визначені в ч. 6 ст. 246 КПК України. За рішенням слідчого чи прокурора до проведення негласних слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, можуть залучати також інших осіб, зокрема спеціалістів у цій галузі. Під час виконання доручень слідчого, прокурора щодо проведення негласних слідчих (розшукових) дій співробітник такого оперативного підрозділу користується повноваженнями слідчого відповідно до ч. 2 ст. 41 КПК України.

Оскільки в кримінальних правопорушеннях зазначеної категорії, специфіка яких полягає у вчиненні їх у кіберпросторі та за допомогою засобів інформаційних комп'ютерних технологій, на нашу думку, найрезультативнішими негласними слідчими (розшуковими) діями, що дають змогу зібрати (отримати) якомога більше

доказів винуватості особи, є: зняття інформації з електронних комунікаційних мереж (ст. 263 КПК України), зняття інформації з електронних інформаційних систем (264 КПК України) й установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ст. 268 КПК України).

1. Зняття інформації з електронних комунікаційних мереж (ст. 263)

Зазначена негласна слідча (розшукова) дія полягає в контролі за телефонними розмовами із застосуванням технічних засобів, зокрема спостереження, відбір та фіксація змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, модемний зв'язок тощо), що передаються каналом зв'язку.

2.Зняття інформації з електронних інформаційних систем (ст. 264)

Цю негласну слідчу (розшукову) дію можуть проводити як на підставі ухвали слідчого судді, коли необхідно здійснити пошук, виявлення та фіксації відомостей, що містяться в електронній інформаційній системі або її частині без відома власника, володільця або утримувача, так і без такої ухвали, у разі якщо відомості в електронних інформаційних системах або її частинах не обмежуються власником, володільцем, утримувачем або не потрібно долати системи логічного захисту (ч. 1, 2 ст. 264 КПК України).

Необхідно зауважити, що головними тактичними особливостями під час проведення цієї негласної слідчої (розшукової) дії є використання відповідних програмних засобів, що потребують наявності залучення спеціаліста в цій сфері.

3.Установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ст. 268).

Нерідко під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій, постає необхідність отримати інформацію про конкретне місцезнаходження радіоелектронного засобу. Якщо така інформація може бути отримана лише внаслідок проведення негласних слідчих (розшукових) дій, тоді слідчий, прокурор ініціюють її проведення, звернувшись з відповідним клопотанням до слідчого судді.

Відповідно до Закону України «Про електронні комунікації», радіообладнанням (радіоелектронним засобом) є електричний або електронний

засіб, призначений для випромінювання (приймання) радіохвиль з метою радіозв'язку (радіовизначення) або укомплектований додатковим пристроєм, призначеним для випромінювання (приймання) радіохвиль з метою радіозв'язку (радіовизначення) [180]. Видами радіоелектронних засобів є мобільний телефон і модем.

Цілком слушною є думка В. В. Луцика [127, с. 205], що встановлення місцезнаходження радіоелектронного пристрою може відбуватися як у режимі реального часу, так і в конкретний період минулого. Якщо постає необхідність в отриманні інформації про зв'язок, що відбувався в минулому (постфактум), тоді таку інформацію отримують у порядку тимчасового доступу до речей і документів. Здебільшого така інформація знаходиться в операторів стільникового зв'язку.

Дотримуючись вимог ст. 159–160, 162 КПК України, слідчий за погодженням із прокурором звертається з відповідним клопотанням до слідчого судді.

Однак, щоб чітко встановити місцезнаходження радіоелектронного пристрою, відбувається ще низка відповідних заходів, що спрямовані на визначення конкретного місця знаходження цього пристрою.

Про перебіг і результати проведення розглянутих негласних слідчих (розшукових) дій складають протокол. У разі, якщо їх проводили за безпосередньою участю слідчого, протокол складає він. У разі доручення їх проведення уповноваженим працівникам оперативного підрозділу, протокол складає відповідний працівник.

Згідно з ч. 1 ст. 252 КПК України, фіксація перебігу та результатів негласних слідчих (розшукових) дій має відповідати загальним положенням ст. 104, 106 КПК України.

Однак на практиці до протоколу додають здебільшого тільки технологічну інформацію, що є невід'ємною складовою звуку або відео.

До протоколу зняття інформації з електронних інформаційних систем або її частини та зняття інформації з електронних комунікаційних мереж додають відповідні носії інформації, що містять файли з відеограмою та зображенням

екрана монітора (або скріншот екрана), створеними під час дослідження системи, також їх роздруківки як додатки до протоколу [217, с. 254].

Протокол і додатки до нього можуть бути доказом у кримінальному провадженні.

Тому необхідно акцентувати на оформленні протоколу про перебіг та отримані результати негласних слідчих (розшукових) дій. Під час складання протоколу слідчі та працівники оперативних підрозділів здебільшого обмежуються лише отриманими під час негласних слідчих (розшукових) дій результатами й не відображають перебіг цієї процесуальної дії. Непоодинокими є випадки, коли не зазначають, хто з оперативних працівників чи залучених спеціалістів здійснювали певні дії, не вказують про використане обладнання, співробітника, який його безпосередньо застосовував. Неприпустимо, коли протокол складають через тривалий проміжок часу після закінчення процесуальної дії і не та особа, яка його провела. Під час дослідження протоколу як доказу в кримінальному провадженні суд може дійти висновку щодо недопустимості цього доказу, оскільки його отримано не в порядку, передбаченому КПК України [125].

Отже, проведення окремих негласних слідчих (розшукових) дій у кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, є одним із засобів збирання електронної доказової інформації, а також встановлення винних осіб, які вчинили зазначені кримінальні правопорушення. Використання результатів негласних слідчих (розшукових) дій дає змогу здійснити перевірку висунутих версій та зрозуміти, які тактичні прийоми необхідно застосовувати для подальшого проведення розслідування.

3.4. Використання спеціальних знань під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій

Успіх досудового розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій,

обумовлений ефективним збиранням і дослідженням слідів, що утворюються безпосередньо в засобах інформаційних комп'ютерних технологій. Тому, безумовно, їх виявлення, збирання, вилучення та дослідження потребує використання спеціальних знань [152, с. 85].

Аналіз практики засвідчує, що слідчий, дізнавач, прокурор самостійно не завжди спроможні зорієнтуватися в усіх тонкощах зазначеної категорії кримінальних правопорушень, що пов'язано з недостатнім рівнем технічних знань у галузі інформаційних комп'ютерних технологій. Для того щоб з'ясувати технічні нюанси, потрібна допомога відповідних фахівців, які мають необхідні спеціальні знання.

У контексті як кримінального процесу, так криміналістики вчені спрямовують увагу на дослідження форм використанням спеціальних знань. У науковій літературі сформульовано різні визначення поняття «спеціальні знання».

На нашу думку, що найповніше зазначене поняття тлумачить І. І. Когутич, вважаючи, що це сукупність професійних знань, навичок і вмінь, що отримані внаслідок спеціальної освіти або досвіду роботи, відповідають сучасному розвитку певної галузі правозастосування, науки, техніки, мистецтва чи ремесла, які є достатніми для вирішення відповідними суб'єктами питань, що цікавлять слідчого, прокурора, дізнавача чи суд [93, с. 114].

На підставі аналізу наукової літератури можна виокремити дві форми використання спеціальних знань: 1) непроцесуальну – надання відповідних консультацій, аналіз відповідних джерел тощо; 2) процесуальну – чітко регламентована нормами КПК України, де передбачено дві форми використання спеціальних знань у кримінальному провадженні – судову експертизу та участь спеціаліста під час проведення окремих процесуальних дій.

Свого часу про важливість застосування вмінь спеціаліста під час розслідування зазначав Г. Гросс, стверджуючи, що слідчому необхідно завчасно ознайомитися з уміннями та навичками спеціаліста та розуміти, як він буде корисним для розслідування [47, с. 56].

Згідно з ч. 1 ст. 71 КПК України, спеціалістом є особа, яка володіє спеціальними навичками та знаннями й може надавати пояснення, консультації, висновки, довідки під час досудового розслідування та судового розгляду з питань, що потребують відповідних спеціальних знань. Права й обов'язки спеціаліста визначено в ч. 4 та 5 ст. 71 КПК України.

Слушною є думка М. Г. Щербаковського, що аналіз приписів ст. 71 КПК України дає підстави виокремити дві допоміжні функції спеціаліста в кримінальному провадженні: 1) надання безпосередньої технічної допомоги (фотографування, складання планів, схем тощо); 2) надання консультацій, довідок, висновків та пояснень, що потребують спеціальних знань і навичок [257, с. 43].

Розглянемо особливості надання спеціалістом пояснення, оскільки на практиці переважно використовують такий вид спілкування слідчого, дізнавача, прокурора зі спеціалістом. Законодавчо не визначено, у якій формі – усно чи письмово – мають бути надані пояснення спеціаліста під час досудового розслідування. З огляду на специфіку кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, на наш погляд, оптимальними є пояснення спеціаліста, викладені в письмовій формі. З огляду на вітчизняні криміналістичні дослідження [7, с. 49–50; 251; 257; 297], на нашу думку, можна виокремити такі тактичні рекомендації, якими необхідно користуватися в разі залучення спеціаліста під час розслідування зазначеної категорії кримінальних правопорушень:

1) пропонувати спеціалісту писати письмове пояснення власноруч з метою уникнення неправильного розуміння термінології слів і забезпечення логічного й послідовного викладення фактів, що мають значення для розслідування;

2) не обмежувати спеціаліста у формі й обсягу письмового пояснення. Це забезпечить усебічне та повне відображення результатів застосування ним спеціальних знань і навичок, дасть змогу отримати професійне пояснення щодо певних процесів, виявлення електронних слідів, їх аналіз у зв'язку з подією, яку розслідують;

3) до протоколу відповідної процесуальної дії необхідно долучати письмове пояснення спеціаліста щодо: методів і технічних засобів, що він застосував, його думки щодо виявлення, вилучення, копіювання та збереження електронних слідів, інших матеріальних об'єктів, пов'язаних з подією кримінального правопорушення.

Письмове пояснення спеціаліста долучають як додаток до протоколу, це передбачено п. 2 ч. 2 ст. 105 КПК України та має відповідати загальним вимогам оформлення додатків (ч. 3 ст. 105 КПК України).

Не слід нехтувати й усними поясненнями спеціаліста. Значення усних пояснень під час проведення процесуальних дій полягає в тому, що слідчий оперативно отримує кваліфіковану допомогу зі спеціальних питань, що допомагають оцінити електронні докази, своєчасно вирішити питання про призначення відповідної експертизи, визначити коло питань, адресованих експертові [257, с. 45–46].

Не можна оминути висловлені в науковій літературі думки вчених з приводу того, чи є письмове пояснення спеціаліста джерелом доказу. Зокрема, П. Є. Антонюк і В. В. Пясковський вважають, що долучення письмового пояснення спеціаліста до матеріалів кримінального провадження за результатами участі спеціаліста в процесуальних діях слід розглядати як важливе джерело доказів – документ [8, с. 338–339].

На думку О. А. Самойленко, письмові пояснення спеціаліста є способом додаткового підтвердження такого процесуального джерела доказу, як документ – електронний носій інформації. У письмовому поясненні спеціаліст зазначає процес встановлення фактичних даних, а також методи вилучення (копіювання) та збереження електронних слідів кримінального правопорушення [216, с. 27]. Іншу думку обстоює М. Г. Щербаковський, який вважає, що пояснення спеціаліста має лише рекомендаційний характер і не є джерелом доказів, оскільки спеціаліст не може самостійно формувати докази [257, с. 46].

Розглядаючи роль пояснення як процесуального джерела доказів, М. Я. Никоненко зауважує, що пояснення не можна вважати джерелом доказів, оскільки воно не відповідає вимогам, які висувають до процесуального джерела

доказів, а також не забезпечує достовірність отриманих доказів, сприяє порушенню прав, свобод і законних інтересів учасників кримінального провадження [159, с. 166].

З огляду на зазначені думки науковців, а також відповідні норми чинного кримінального процесуального законодавства України, можна дійти такого висновку. У положеннях ч. 2 ст. 84 КПК України, де є перелік джерел доказів (показання, речові докази, документи та висновок експертів), пояснення спеціаліста як джерела доказу немає. Як джерело доказів про письмові пояснення спеціаліста як додатки до протоколів не йдеться і в приписах ч. 2 ст. 99 КПК України.

Водночас привертає увагу ст. 298-1 КПК України «Процесуальні джерела доказів у кримінальних провадженнях про кримінальні проступки», у якій визначено, що процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених ст. 84 КПК України, також є пояснення осіб, результати медичного освідування, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- й кінозйомки, відеозапису.

Далі законодавець зазначає, що такі процесуальні джерела доказів не можуть бути використані в кримінальному провадженні щодо злочину. Проте зауважує, що на підставі ухвали слідчого судді, винесеної за клопотанням прокурора, передбачені в ст. 298-1 КПК України процесуальні джерела доказів можуть бути використані в кримінальному провадженні щодо злочину (абз. 2 ч. 1 ст. 298-1 КПК України).

Слід зауважити, що в зазначеній статті увагу зосереджено на поясненні осіб, а не на поясненні спеціаліста як процесуальному джерелі доказів. У зв’язку з цим постає питання: чи можна до пояснення осіб відносити і пояснення спеціаліста? Відповідаючи на це питання, звернемося до ч. 8 ст. 95 КПК України, у якій зазначено, що сторони кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюють провадження, мають право отримувати від учасників кримінального провадження пояснення. Спеціаліст, згідно з п. 25 ч. 1

ст. 3 КПК України, належить до учасників кримінального провадження. Тобто термін «пояснення осіб» у положеннях ст. 298-1 КПК України охоплює і пояснення спеціаліста.

Попри те, що такі законодавчі зміни спричинили бурхливу критику в наукових колах, законодавець відносить пояснення, а також висновок спеціаліста до процесуальних джерел доказів у кримінальному провадженні.

Ще одним не менш важливим видом використання спеціальних знань під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, є висновок спеціаліста.

В етимологічному значенні поняття «висновок» слід тлумачити як остаточну думку про що-небудь, підсумок, сформульований на підставі міркувань чи спостережень [29, с. 112].

У кримінальному процесуальному законодавстві немає положення, що висвітлює зміст терміна «висновок спеціаліста». Натомість законодавець у ст. 300 КПК України зазначає, що висновок спеціаліста повинен відповідати вимогам, що ставлять до висновку експерта, зазначеним у ст. 101, 102 КПК України.

Отже, головна відмінність між висновком експерта й спеціаліста полягає в суб'єкті надання такого висновку.

Слід зазначити, що віднесення законодавцем висновку спеціаліста до джерел доказів спричинило бурхливу критику такого нововведення в колах наукової спільноти [9; 91; 225; 249].

Учені привертають увагу до процесуальних недосконалостей, що стосуються висновку спеціаліста як джерела доказів за приписами ст. 298-1 КПК України.

На їхню думку, насамперед порушено структуру та логіку кодифікації норм кримінального процесуального законодавства: зазначені положення про джерело доказів суперечать главі 4 розділу І КПК України (докази і доказування), у якій чітко визначено поняття та види доказів, критерії їх належності й допустимості [9, с. 92].

Крім зазначеного, це нововведення ставить під сумнів доказове значення висновку спеціаліста в кримінальному провадженні, оскільки, згідно з ч. 2 ст. 298-

4 КПК України, висновок спеціаліста може бути перевірений висновком експерта за клопотанням прокурора про проведення експертизи. Тобто перевагу надають висновку експерта [9, с. 92].

Попри критику з боку вітчизняних вчених, на нашу думку, з огляду на специфіку розслідування зазначених кримінальних правопорушень, висновок спеціаліста слід використовувати на вихідному етапі (до внесення відомостей до ЄРДР). Це сприятиме встановленню обставин, що можуть свідчити про вчинення кримінального правопорушення, а також слугувати підґрунтям для прийняття рішення про початок досудового розслідування. Вбачається за доцільне використовувати висновок спеціаліста й на подальших етапах розслідування.

У контексті зазначеного розглянемо позицію ЄСПЛ щодо висновку спеціаліста. Зокрема, у справі «Пічугін проти Росії» Суд констатував, що відмова національних судів визнати звіти, підготовлені спеціалістами як докази, порушує принцип рівності сторін (п. 33). У зв'язку з несправедливим дослідженням доказів допущено порушення ст. 6 Конвенції [230].

Не слід нехтувати консультацією спеціаліста, а також наданням ним довідок, які також мають вагоме значення під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Зі свого боку законодавець не висвітлює в нормах КПК України поняття, суть, види консультацій та довідок спеціаліста. Натомість у Великому тлумачному словнику української мови консультацію визначено як пораду фахівця з якого-небудь питання [29, с. 450]. Оксфордський тлумачний словник визначає консультацію як обговорення когось із кимось перед прийняттям рішення [275]. Отже, під час розслідування зазначених кримінальних правопорушень консультацією є обговорення та порада спеціаліста з питань інформаційних технологій суб'єкта розслідування перед прийняттям рішення.

Аналіз наукової літератури засвідчує [166, с. 96], що консультація спеціаліста, на переконання більшості науковців, надається в усній або письмовій формах як щодо обставин, безпосередньо пов'язаних із подією, яку розслідують,

так і для отримання спеціальних відомостей загального характеру. Консультації спеціаліста можуть здійснювати у двох варіантах: 1) до або під час проведення процесуальних дій; 2) в інших випадках, коли необхідно винести процесуальне рішення чи організаційне (тактичне) рішення.

З огляду на такі думки науковців [72; 131; 166], доходимо висновку, що консультація спеціаліста під час розслідування зазначених кримінальних правопорушень надається для:

– порад під час формулювання слідчих версій та плану розслідування;

– роз'яснення цільового призначення й методики використання технічних засобів у процесі фіксації електронних слідів;

– рекомендацій, у якому саме порядку необхідно здійснювати виявлення, фіксацію, дослідження засобів інформаційних комп'ютерних технологій;

– порад залучення спеціаліста з іншої спеціалізації;

– термінологічних підказок оформлення протоколу відповідної процесуальної дії;

– розуміння дії апаратних (технічних) і програмних засобів;

– з'ясування, який засіб інформаційних комп'ютерних технологій необхідно дослідити насамперед;

– порад щодо направлення вилучених засобів інформаційних комп'ютерних технологій на відповідну експертизу та визначення питань, які необхідно поставити перед експертом;

– роз'яснення про необхідність проведення додаткової процесуальної дії.

Слід зазначити, що усна консультація спеціаліста може надаватися на будь-якій стадії розслідування, оскільки має оперативно-тактичне значення, водночас як письмова буде мати вагоміше значення на початковому й наступному етапах розслідування.

Такий вид використання спеціальних знань, як надання довідки спеціалістом, дістав законодавче закріплення у зв'язку зі змінами, внесеними згідно із Законом України від 15 березня 2022 року № 2137-IX «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації»

щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам [177] до ч. 1 ст. 71 КПК України.

Тому для визначення поняття «довідка» звернемося за допомогою до Великого тлумачного словника української мови, у якому сформульовано таке визначення довідки: 1) відомості, що повідомляють кому-небудь за результатами запиту; 2) документ зі стислими відомостями [29, с. 231]. З огляду на таку дефініцію, довідку надає спеціаліст на запит суб'єкта розслідування щодо відомостей про характеристики апаратних і програмних засобів інформаційно-комп'ютерних технологій, їх особливостей функціонування, роз'яснення певної термінології тощо. Тобто довідка спеціаліста має інформаційний характер для суб'єкта розслідування, натомість консультація спеціаліста є порадою з певних питань, що виникають під час розслідування кримінальних правопорушень зазначеної категорії.

Слід зауважити, що кримінальний процесуальний закон передбачає обов'язкову участь (залучення) відповідного спеціаліста конкретної професії в проведенні всіх слідчих (розшукових) дій за участю малолітньої або неповнолітньої особи (ст. 226, 227 КПК України), огляду трупа, огляду трупа, пов'язаного з ексгумацією (ст. ст. 238, 239 КПК України), освідування особи (ч. 2 ст. 241 КПК України). Також спеціаліста обов'язково залучають, коли постає необхідність здійснити певні дії із засобами інформаційних комп'ютерних технологій, саме:

– під час виготовлення копії інформації за допомогою певних засобів (абз. 4 ч. 2 ст. 168 КПК України);

– у разі тимчасового вилучення комп'ютерних систем або їх частин, особа, яка їх вилучає, залишає на вимогу володільця копії інформації з таких комп'ютерних систем (за наявності технічної можливості здійснення такого копіювання). Копії інформації з комп'ютерних систем або їх частин, які вилучають, виготовляють з використанням відповідних засобів та із залученням спеціаліста (абз 5 ч. 2 ст. 168 КПК України).

Сьогодні в суб'єкта розслідування є широкі можливості щодо вибору спеціалістів з різних підприємств, установ, організацій і не тільки державних, а й приватних. Це обумовлено ч. 5 ст. 71 КПК України, положення якої зобов'язують спеціаліста прибути за викликом слідчого, прокурора та виконувати їхні вказівки. Головним критерієм є наявність в особи спеціальних знань. Переважно це спеціалісти в галузі інформаційних технологій, які, відповідно до постанови Кабінету Міністрів України від 29 квітня 2015 року «Про затвердження переліку галузей і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» [186], спеціалізуються на: інженерії програмного забезпечення, комп'ютерних науках, комп'ютерних інженеріях, системному аналізі, кібербезпеці, інформаційних системах і технологіях.

Перед залученням спеціаліста доцільно перевіряти в нього не тільки наявні дипломи та свідоцтва про відповідну технічну спеціалізацію спеціаліста, а й наявність досвіду роботи у сфері інформаційних технологій, що засвідчуватиме навички застосування теоретичних знань, наявність відповідних сертифікатів про постійне підвищення професійних знань. З'ясування цього й особисте спілкування слідчого, прокурора з фахівцем надасть можливість визначити, чи зможе він допомогти в розслідуванні. Доцільно копії таких документів долучати до матеріалів проведення процесуальної дії для усунення можливостей непорозуміння щодо фаховості спеціаліста [251, с. 136].

Здебільшого для участі в проведенні огляду місця події як спеціалістів залучають працівників Експертної служби МВС України. Їх участь визначено в 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 [184]. Для участі в проведенні слідчих (розшукових) дій також залучають як спеціалістів співробітників і працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України [185].

Окремо зазначимо щодо форми залучення спеціаліста під час досудового розслідування. Кримінальний процесуальний закон не визначає, як має відбуватися

процесуальне оформлення залучення спеціаліста. Слідча практика засвідчує, що суб'єкт розслідування залучення спеціаліста оформляє постановою. Оскільки, відповідно до ч. 3 ст. 110 КПК України, процесуальні рішення слідчого, дізнавача, прокурора приймають у формі постанови, то вбачається обґрунтованим здійснювати залучення спеціаліста на підставі постанови.

З огляду на зазначені Інструкції, можна виокремити тактичні рекомендації щодо залучення спеціаліста до участі в процесуальних діях під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій:

– перед виїздом для участі в слідчих (розшукових) діях необхідно поінформувати спеціаліста про вид слідчої (розшукової) дії, інші відомі обставини (кількість і характеристика засобів інформаційних комп'ютерних технологій тощо) для того, щоб він підготував відповідне технічне обладнання;

– залучений спеціаліст консультує слідчого, дізнавача, прокурора з питань можливості дослідження виявлених об'єктів, речей, документів, а також відбору необхідних зразків для проведення експертного дослідження, доцільності вирішення інших питань, потреби залучення інших спеціалістів;

– спеціаліст за дорученням прокурора чи слідчого виготовляє фототаблиці, фотознімки, схеми, які долучають як додатки до протоколу;

– носії інформації (диск, флеш-накопичувач та інші носії інформації), на яких зафіксовано аудіо-, відеозапис процесуальної дії, долучають як додатки до протоколу;

– у разі технічної неможливості виготовлення фототаблиць, спеціаліст повідомляє про це слідчого, дізнавача, прокурора із зазначенням причин неможливості їх виготовлення.

Спеціаліст може бути залучений і під час проведення негласних слідчих (розшукових) дій. Таке залучення є правом слідчого, прокурора, а не їхнім обов'язком. Тому з дотриманням режиму секретності (спеціаліст повинен мати відповідний допуск до державної таємниці) під час проведення негласних слідчих (розшукових) дій, а також відповідно до специфіки питань її проведення слідчий і

прокурор самостійно приймають рішення про можливість залучення до негласних слідчих (розшукових) дій спеціаліста відповідної кваліфікації та фаху [216, с. 27–28].

Значущості залучення спеціаліста в кримінальних правопорушеннях цієї категорії набуває під час проведення таких слідчих (розшукових) дій, як огляд місця події та обшук, адже вони безпосередньо пов'язані з виявленням, вилученням засобів інформаційних комп'ютерних технологій та їх дослідженням.

До прикладу, у процесі проведення опитування прокурорів 87 % респондентів висловилися за обов'язкове залучення спеціаліста під час проведення зазначених вище слідчих (розшукових) дій [162].

Необхідно зазначити і про те, що 55 % опитаних прокурорів вважають, що нехтування залученням спеціаліста та використанням його консультацій, пояснень, довідок і висновків негативно позначається на результатах ефективного досудового розслідування зазначеної категорії кримінальних правопорушень [162].

Слід зауважити, що залучення до проведення окремих слідчих (розшукових) дій спеціаліста дасть змогу спрямувати перебіг процесуальної дії у відповідне русло, ефективно дослідити та вилучити засоби інформаційних комп'ютерних технологій, зрозуміти місця зберігання електронних доказів, а також допоможе слідчому, дізнавачу, прокурору оформити протокол з урахуванням відповідної термінології.

Наступним процесуальним видом використання спеціальних знань є залучення експерта для проведення судової експертизи.

На законодавчому рівні судову експертизу визначають як дослідження, що проводять на підставі спеціальних знань у відповідній галузі стосовно об'єктів, процесів і явищ з метою надання висновку з питань, що є або будуть предметом судового розгляду [196].

Своєю чергою в КПК України визначено, хто може бути експертом у кримінальному провадженні: це особа, яка володіє науковими, технічними або іншими спеціальними знаннями, причому така особа, згідно із Законом України

«Про судову експертизу» [198], повинна мати право на проведення експертизи, їй має бути доручено проведення такої експертизи (ч. 1 ст. 69 КПК України).

Здійснивши аналіз відповідних положень чинного кримінального процесуального законодавства та Закону України «Про судову експертизу», А. В. Дудич обґрунтовано виокремлює сукупність важливих професійних і процесуальних вимог, які пред'являють до експерта у зв'язку із залученням його до кримінального провадження [68, с. 41–50]:

1) володіння науковими технічними або іншими спеціальними знаннями, щоб надати відповідний висновок;

2) бути фахівцем з відповідною вищою освітою, мати освітньо-кваліфікаційний рівень не нижче від спеціаліста, пройти відповідну підготовку, а також бути атестованим і мати кваліфікацію експерта з певної спеціальності;

3) бути внесеним до Державного реєстру атестованих судових експертів;

4) бути дієздатним і не мати не зняту або непогашену судимість, а також необхідно, щоб на експерта протягом року не накладалося адміністративне стягнення за вчинення корупційного правопорушення або дисциплінарне стягнення (позбавлення кваліфікації експерта).

За результатами проведеного експертного дослідження на підставі використання спеціальних знань експерт складає висновок, який є процесуальним джерелом доказів відповідно до ч. 2 ст. 84 КПК України.

Ми цілком поділяємо думку Д. В. Давидова й О. О. Волобуєва [60, с. 152], що висновок експерта відрізняється за своєю сутністю від інших джерел доказів, оскільки:

– він є результатом дослідження особи, яка володіє спеціальними знаннями за фахом, компетенцією та має право на проведення такого дослідження;

– дослідження проводять на підставі трьох видів інформації: 1) яка міститься в матеріалах кримінального провадження (отримана з показань, речових доказів, документів); 2) яка отримана під час застосування відповідних методів (бесіда, спостереження, експеримент тощо); 3) яка становить професійні знання експерта;

– предмет дослідження визначає сторона, яка залучила експерта, тобто коло питань, які були поставлені йому для вирішення;

– предмет дослідження обмежується знаннями експерта та видом експертизи.

Законодавець висвітлює зміст висновку експерта – це докладний опис досліджень і сформульовані за їх результатами висновки, обґрунтовані відповіді на поставлені запитання (ч. 1 ст. 101 КПК України).

У вітчизняній науковій літературі чимало уваги зосереджено на дослідженні сутності висновку експерта як джерела доказів [60; 68–70; 88].

Не ставлячи за мету розгляд висловлених науковцями думок з цього питання, вважаємо за доцільне акцентувати на міркуваннях А. В. Столітнього щодо надання в кримінальному провадженні висновку експерта в електронному форматі. Науковець пропонує перехід на електронний формат спілкування між експертом (через відповідну експертну установу) і суб'єктами кримінального провадження (слідчий, прокурор, адвокат, слідчий суддя). Таке спілкування слід здійснювати через особистий віртуальний кабінет відповідної електронної системи. Поділяємо таку позицію щодо можливості запровадження електронної форми висновку експерта, тож це потребує нормативного врегулювання та вдосконалення технічних можливостей ЄРДР [232, с. 102–109].

Водночас зауважимо, що ця електронна система повинна мати відповідний кіберзахист – сукупність відповідних заходів, спрямованих на захист від кібератак [193].

У ч. 2 ст. 242 КПК України визначено, коли слідчий або прокурор в обов'язковому порядку зобов'язані забезпечити проведення експертизи.

Зі свого боку зазначимо, що направлення обвинувального акта до суду без отримання під час досудового розслідування висновку експерта призводить до затягування судового розгляду. Крім того, призначення та поява результатів експертизи під час судового провадження може зумовити необхідність зміни, висунення нового обвинувачення або навіть відмови прокурора від обвинувачення. Це суперечить завданням кримінального провадження щодо швидкого, повного й

неупередженого розслідування та судового розгляду, вчиненого кримінального правопорушення (ст. 2 КПК України).

У науковій літературі триває дискусія щодо наявності в Україні відомчого підпорядкування експертних установ, яким надано право проведення судових експертиз. Зокрема, Н. М. Ахтирська та О. Ю. Костюченко стверджують, що таке підпорядкування (наприклад, Служба безпеки України, МВС тощо) створює ризик порушення принципу неупередженості та незалежності експерта під час проведення експертизи та складання висновку. Задля уникнення ризику упередженого ставлення до результатів дослідження вчені цілком обґрунтовано пропонують виключити експертні установи з відомчого підпорядкування. На обґрунтування своєї позиції також наводять відповідне рішення ЄСПЛ у справі «Проскурніков проти Росії», де висловлено сумніви, що експерти, які є співробітниками відомчих експертних установ (правоохоронних органів), можуть бути незалежними експертами в кримінальних провадженнях [106, с. 32, 36].

Під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, важливим *є своєчасне призначення та проведення експертизи*. З огляду на класифікацію та специфіку таких кримінальних правопорушень, під час проведення досудового розслідування постає потреба проводити *різні види судових експертиз.*

На підставі зазначених в Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5 [80], видів судових експертиз розглянемо окремі з них, які можуть проводити під час розслідування зазначених кримінальних правопорушень, доповнюючи відмітними особливостями.

1. Криміналістична:

– почеркознавча (у разі необхідності встановлення того, ким виконані рукописні тести, хто є автором твору чи тексту тощо). Об'єктом дослідження можуть бути: письмові документи з почерком і підписами (записні й телефонні книжки, нотатки, листи тощо) [167, с. 63];

– лінгвістична експертиза мовлення, у межах якої проводять авторознавчі та семантико-текстуальні дослідження. Її проводять у випадках ідентифікації автора тексту. Об'єктом дослідження є мовна (текстова) інформація, яку передають комп'ютерними мережами, зафіксована на матеріальному носії [234, с. 168];

– технічна у випадку необхідності встановлення документа, виготовленого шляхом монтажу із застосуванням комп'ютерної техніки. Об'єктами дослідження є засоби підроблення реквізитів документів, печатки та штампи, форми і пристрої для друку (принтери, ксерокси тощо) [167, с. 63];

– трасологічна – коли необхідно ідентифікувати або визначити родову належність індивідуально визначених об'єктів за матеріально фіксованими слідами;

– дактилоскопічна – у випадках встановлення особи за слідами її рук, які залишені на місці події. Наприклад, встановлення того, кому належать сліди рук на засобі інформаційних комп'ютерних технологій;

– портретна (у разі ідентифікації особи (трупа) за фотознімком і відеозаписом). Об'єктом дослідження є фотографії, відеозаписи, зокрема на електронних носіях і в пам'яті комп'ютера [167, с. 63];

– експертиза відеозапису. Її проводять для встановлення технічних умов і технології отримання відеозапису, ототожнення особи за фізичними параметрами голосу, а також ототожнення особи за лінгвістичними ознаками усного мовлення;

– експертиза матеріалів, речовин і виробів (підвид експертизи наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів). Таку експертизу здебільшого проведять під час розслідування кримінальних правопорушень у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, що вчинені з використанням інформаційних технологій.

2. Інженерно-технічна:

– експертиза комп'ютерної техніки і програмних засобів (проводять з метою дослідження засобів інформаційних комп'ютерних технологій, їх апаратної та програмної складових);

– експертиза телекомунікаційних систем і засобів.

Такі експертизи детально ми проаналізуємо далі в дисертаційному дослідженні.

3. Економічна:

– експертиза документів фінансово-кредитних операцій, яку проводять у разі необхідності визначення питань, пов'язаних із банківськими операціями з відкриття рахунків, руху коштів на рахунках, використанням і погашенням кредитів тощо.

4. Експертиза об'єктів інтелектуальної власності: визначення властивостей комп'ютерних програм, баз даних, якщо вони є результатом інтелектуальної діяльності, а також визначення їх вартості та розрахунок збитків, завданих унаслідок правопорушення.

5. Психологічна експертиза (у разі необхідності встановлення індивідуально-психологічних особливостей, рис характеру, психічного життя і поведінки). У межах цієї експертизи можуть проводити опитування із застосуванням спеціального технічного засобу – комп'ютерного поліграфа.

6. Мистецтвознавча: здебільшого проводять під час розслідування кримінальних правопорушень проти громадського порядку та моральності. Об'єктами дослідження є твори образотворчого мистецтва (живопис, скульптура, графіка), кіно- та відеопродукція, фотоматеріали тощо. Такі твори можуть бути зафіксовані на будь-яких носіях (паперових, цифрових тощо) [246, с. 463].

Під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, оскільки сліди вчинення протиправних дій знаходяться в засобах інформаційно-комп'ютерних технологій (їх апаратних і програмних засобах), у більшості випадків призначають експертизу комп'ютерної техніки та програмних засобів.

Поділяємо думку Б. Б. Теплицького, що комп'ютерно-технічну експертизу слід включати до класу інженерно-технічних експертиз, оскільки за своїм походженням інформаційно-комп'ютерні технології належать до інженерно-технічних розробок [234, с. 164].

Не вдаючись до полеміки з приводу тлумачення поняття «комп'ютерна технічна експертиза», вважаємо вдалим визначення, запропоноване О. А. Самойленко, що це «дослідження технічних властивостей комп'ютерного обладнання, програмного забезпечення, інформації, що міститься на електронних носіях, з метою встановлення фактичних даних, які мають значення для кримінального провадження, а також пов'язані з використанням комп'ютерної техніки» [217, с. 300].

Експертиза комп'ютерної техніки та програмних продуктів, як і будь-яка судова експертиза, має основні завдання, що повинні бути вирішені експертом залежно від об'єкта дослідження.

З огляду на завдання експертизи комп'ютерної техніки та програмних продуктів, зазначених у розділі II (Інженерно-технічна експертиза) п. 13.1 Інструкції про призначення та проведення судових експертиз та експертних досліджень [80], а також висловлених думок з цього питання у вітчизняній науковій літературі [89, с. 36–37; 234, с. 179], окреслимо основні завдання цієї експертизи:

– встановлення робочого стану комп'ютерних і технічних засобів;

– встановлення обставин, пов'язаних з використанням інформаційно-комп'ютерних технологій, інформації та програмного забезпечення;

– визначення функціонального призначення представленого програмного системного та прикладного забезпечення, а також їх характеристик, вимог, алгоритму й структурних особливостей;

– пошук, виявлення, аналіз й оцінювання комп'ютерної інформації (комп'ютерних даних) і програмного забезпечення, що містяться на комп'ютерних носіях;

– встановлення відповідності програмних продуктів певним версіям чи вимогам;

– виявлення причин блокування сайтів (віруси, DDoS атаки), а також несанкціонованого втручання в роботу сайту, сервера, комп'ютера, електронної пошти тощо.

Достатньо складно перелічити всі об’єкти дослідження зазначеної експертизи, оскільки зі стрімким розвитком інформаційних комп’ютерних технологій об’єкти цієї експертизи постійно вдосконалюються та змінюються.

Обираючи за основу класифікацію об’єктів дослідження експертизи комп’ютерної техніки та програмних продуктів, запропоновану Б. Б. Теплицьким [234], ураховуючи сучасний стан засобів інформаційних комп’ютерних технологій, виокремимо такі види об’єктів:

1) апаратні: комп’ютерна техніка (персональні комп’ютери, ноутбуки, ультрабуки, нетбуки, планшети, мобільні телефони, смартгодинники тощо); периферійні пристрої (принтер, клавіатура, монітор, мікрофон, сканер тощо); мережеві апаратні засоби (сервер, модем, роутер й інше серверне обладнання); комплектування всіх зазначених вище компонентів (відеокарта, блок живлення, процесор персонального комп’ютера, апаратний блок, плата розширення, носій інформації тощо);

2) програмні: системне програмне забезпечення (комплекс програм, призначених для управління роботою засобів інформаційних комп’ютерних технологій, що охоплюють 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: графічні й текстові файли, створені за допомогою інформаційних комп’ютерних технологій (планшет, ноутбук, телефон тощо) (інформація, що знаходиться в мережі Інтернет, електронні записні книжки тощо); аудіовізуальні (мультимедійні) дані (фото-, відеофайли, GIF тощо); інформація у форматах баз даних та іншого прикладного програмного забезпечення.

У науковій літературі експертизу комп’ютерної техніки та програмних продуктів умовно поділяють на три самостійні експертні підвиди [84, с. 141–142]:

1) експертиза комп’ютерної техніки встановлює обставини та факти, що мають значення для розслідування та пов’язані із функціонуванням й експлуатацією комп’ютерної системи. Основними завданнями цього підвиду

експертизи є встановлення технічного стану, комплектації та відповідних можливостей інформаційних комп'ютерних технологій;

2) експертиза програмних продуктів, що встановлює обставити й факти, пов'язані з розробкою та використанням програмних продуктів комп'ютерної системи. Завданням цього підвиду експертизи є визначення функціонального призначення, алгоритму, вимог, технічних параметрів, а також стану й особливостей програмного забезпечення.

Слід зазначити, що в цьому підвиді також можна виокремити експертизу шкідливих програмних засобів – комплексне дослідження на підставі спеціальних знань у галузі комп'ютерної техніки, програмних продуктів, телекомунікаційних систем (обладнання) і засобів програм (файлів, скриптів, кодів) щодо можливості їх застосування для несанкціонованого втручання в роботу засобів інформаційних комп'ютерних технологій, що може призвести до витоку, втрати, підроблення чи блокуванню інформації [160, с. 6];

3) інформаційно-комп'ютерна експертиза встановлює факти й обставини, пов'язані зі створенням, обробкою та збереженням інформації на комп'ютерних носіях. Її головним завданням є пошук, виявлення, відтворення і технічний аналіз інформації, створеної користувачем чи програмами в засобах інформаційних комп'ютерних технологій (комп'ютерних системах) [84, с. 141–142].

Якщо розглядати діяльність суб'єкта розслідування щодо залучення експерта для проведення експертизи комп'ютерної техніки та програмних засобів у кримінальному провадженні, можна виокремити такий комплекс дій:

1) прийняття рішення про проведення експертизи;

2) формулювання запитань на вирішення експерта;

3) визначення матеріалів кримінального провадження, що містять вихідні дані для експертизи;

4) вибір експертної установи й експерта;

5) відбір і підготовка об'єктів дослідження та порівняльних матеріалів (зразків);

6) ділова взаємодія слідчого й експерта (комісії експертів) у процесі підготовки та призначення експертизи [89, с. 48–49].

Проаналізуємо алгоритм дій суб'єкта розслідування в межах призначення експертизи комп'ютерної техніки та програмних засобів.

Рішення про необхідність проведення експертизи виникає, коли в процесі проведення процесуальних дій було вилучено засоби інформаційних комп'ютерних технологій або інші носії інформації та для їх дослідження потрібні спеціальні знання, які має експерт. Юридичною підставою для проведення експертизи комп'ютерної техніки та програмних засобів є процесуальний документ. Аналіз положень кримінального процесуального законодавства (ст. 110, 242–244 КПК України) і Закону України «Про судову експертизу» (ст. 7-1) дає підстави стверджувати, що до таких процесуальних документів під час досудового розслідування належать постанова слідчого, дізнавача, прокурора, а також ухвала слідчого судді у випадках, коли звертається сторона захисту.

Судова експертиза повинна бути призначена своєчасно та з огляду на:

– властивості й стан об'єктів експертного дослідження;

– необхідність і можливості отримання порівняльних зразків;

– особливості експертного дослідження (складність, наявність відповідних методик, час проведення тощо);

– слідчу ситуацію [104, с. 218].

Суб'єкту розслідування слід ураховувати, що чинне законодавство України не визначає строки проведення експертизи, тому зволікання в призначенні та проведенні експертизи позначається на загальних строках досудового розслідування. Нині строки проведення судової експертизи визначено у відомчих документах. Зокрема, відповідно до Інструкції про призначення та проведення судових експертиз [80], строк проведення експертного дослідження встановлює керівник експертної установи (або його заступник чи керівник структурного підрозділу), він не повинен перевищувати 90 календарних днів.

З огляду на визначені строки проведення судових експертиз в інструкціях, цілком слушною видається думка О. Ю. Костюченко та Н. М. Ахтирської, що на

практиці численними є випадки суттєвих порушень встановлених строків, а посилання експертних установ на надмірне навантаження не враховує ЄСПЛ як виправдання порушення розумних строків. Учені слушно пропонують не відомче, а законодавче закріплення строків проведення судових експертиз [106, с. 33].

Розглядаючи формулювання питань, що ставлять на вирішення експерту, необхідно враховувати такі вимоги до них [110, с. 420]:

– вони не мають виходити за межі спеціальних знань експерта, не стосуватися галузей права;

– повинні бути визначеними, стислими, конкретними та сформульованими в логічній послідовності;

– мають вирізнятися повнотою, бути комплексними.

Узагальнюючи думки вітчизняних науковців, висловлені в криміналістичній літературі й дисертаційних дослідженнях [51; 72; 138; 160; 164; 234], можна виокремити такі питання, що ставлять перед експертом для проведення експертизи комп'ютерної техніки та програмних засобів. На нашу думку, такі питання можна розділити залежно від об'єкта дослідження на:

1) питання, що стосуються апаратних об'єктів: 1) якої моделі надано на дослідження засіб інформаційних комп'ютерних технологій та які є його технічні характеристики; 2) які технічні несправності має наданий на дослідження засіб інформаційно-комп'ютерних технологій або його окремі блоки та пристрої, чи впливають ці несправності на його роботу; 3) чи відповідає представлена документація цим засобам інформаційних комп'ютерних технологій; якщо ні, то які компоненти було змінено, демонтовано; 4) які умови складання засобу інформаційно-комп'ютерних технологій (комп'ютера) і його комплектуючих; чи є додаткові пристрої, що не входять до базового комплекту; 5) чи є на засобі інформаційних комп'ютерних технологій сліди ремонту, пошкоджень, демонтажу мікросхем, заміни блоків; 6) чи є в засобі інформаційних комп'ютерних технологій додаткові блоки (жучки) з вірусними програмами; якщо є, то яке їх призначення; 7) чи можливе відключення апаратних засобів захисту і як це впливає на роботу

системи; 8) чи було дотримано правил експлуатації; чи могла ця проблема виникнути внаслідок недотримання правил технічної експлуатації;

2) питання, що стосуються носіїв інформації: 1) коли та ким створені досліджувані файли на наданому носії; 2) чи міститься на наданому носії інформація, що має ключові слова «...»; 3) чи містилися на носії файли, що були згодом знищені; якщо так, то що це за файли та який їх зміст; 4) чи є можливість відновити пошкоджену інформацію на відповідному носії; 5) чи інфіковано носій, тобто чи заражена інформація на цьому носії комп'ютерним вірусом; якщо так, то які зміни він вносить в інформацію, чи є можливість нейтралізувати його без заподіяння шкоди інформації; 6) яка інформація була записана раніше на цей носій (помічена як стерті файли і чи є можливість її відновити); 7) як та яку інформацію перенесено на досліджуваний носій; 8) чи потрібні спеціальні апаратні або програмні засоби дешифрування і перекодування для роботи з інформацією на носії; 9) чи немає на носієві спеціальних програм, які знищують інформацію у випадку незаконного втручання, відсутності ключів і паролів або використання на іншому комп'ютері;

3) питання, що стосуються програмних об'єктів: 1) як саме (та в який час) встановлено зазначений програмно-комп'ютерний засіб; 2) яке призначення цього програмного забезпечення; 3) чи містяться на досліджуваному засобі інформаційних комп'ютерних технологій (персональному комп'ютері, ноутбуці тощо) програмні продукти, призначені для злому пароля та несанкціонованого доступу до комп'ютерних систем; 4) чи можливе виконання певного завдання (вказати, яке саме) за допомогою наданого програмного продукту; 5) чи є такі програмні продукти ліцензійними копіями, чи вони є оригінальними розробками; 6) чи відповідає стиль програмування досліджуваного програмного продукту стилю програмування певної особи; 7) чи відповідають прийоми й засоби програмування, що були використані для створення досліджуваного програмного продукту, тим прийомам і засобам, якими послуговується користувач;

4) питання, що стосуються шкідливих програмних засобів: 1) чи є надана на дослідження програма (файл, скрипт, вихідний код) шкідливим програмним

засобом; 2) чи міститься на наданому на дослідження засобі інформаційних комп'ютерних технологій (носії інформації, дампі оперативної пам'яті, побітовій копії) програма (файл, скрипт, вихідний код) із функціональними можливостями, притаманними шкідливим програмним засобам; 3) які функціональні можливості поданої на дослідження програми (файлу, скрипту, вихідного коду); 4) чи містяться на наданому на дослідження засобі інформаційних комп'ютерних технологій (носії інформації, дампі оперативної пам'яті, побітовій копії) сліди функціонування шкідливих програмних засобів; якщо так, то які саме.

Цей перелік питань не є вичерпним і може бути доповнений залежно від об'єкта й завдань дослідження, що постають перед експертом.

Також важливим є пакування об'єкта для направлення його на проведення експертизи комп'ютерної техніки та програмних засобів. Наприклад, зовнішній носій інформації необхідно упакувати й опечатати на місцях відкриття упаковки. Внутрішній носій інформації, який є частиною спецтехніки, за можливості необхідно відокремити від техніки й підготувати до передачі експерту або передати разом з обладнанням, яке слід упакувати [89, с. 53].

Здійснивши упакування об'єкта, який буде направлений на дослідження, слід визначитися з експертною установою, де будуть проводити судову експертизу.

Науковці зосереджують увагу на необхідності взаємодії суб'єкта розслідування з експертом у кримінальному провадженні. Надзвичайно актуальним це питання є під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Попри різноманітність визначень поняття взаємодії слідчого (іншого суб'єкта розслідування) з експертом, сформульованих науковцями в криміналістичній літературі [92; 206; 240], усі вони єдині в тому, що це поняття слід тлумачити як погоджену (спільну) діяльність адміністративно не залежних один від одного суб'єкта розслідування та експерта, запрошеного для надання допомоги у вирішенні питань, що потребують спеціальних знань під час розслідування.

У криміналістичній літературі виокремлюють дві форми взаємодії між суб'єктом розслідування та експертом: процесуальну і непроцесуальну.

Процесуальна форма взаємодії між суб'єктом розслідування та експертом відбувається: 1) у складі слідчо-оперативної групи, коли експерта залучають як спеціаліста; 2) під час проведення процесуальних дій, де експерта залучають як спеціаліста; 3) під час проведення експертизи в кримінальному провадженні, де його залучають як експерта [128, с. 265].

До непроцесуальної форми взаємодії належать: 1) консультація суб'єкта розслідування з експертом до призначення експертизи та в процесі її проведення; 2) звернення експерта до суб'єкта розслідування за роз'ясненням щодо завдання дослідження після отримання постанови про призначення експертизи; 3) уточнення висновку експерта суб'єктом розслідування після його отримання [240].

Важливу роль під час розслідування цієї категорії кримінальних правопорушень також відіграє експертиза телекомунікаційних систем і засобів.

Розглядаючи цей вид експертизи, вважаємо слушною думку І. О. Шапошнікової, що відмінність між експертизою комп'ютерної техніки і програмних засобів й експертизою телекомунікаційних систем і засобів полягає в об'єкті дослідження. Зокрема, якщо кримінальне правопорушення полягає в розповсюдженні шкідливих програм (ст. 361-1 КК України) чи інформації, що міститься на засобі інформаційних комп'ютерних технологій, але має обмежений доступ (ст. 361-2 КК України), то призначати необхідно експертизу комп'ютерної техніки та програмної продукції. Проте якщо об'єктивною стороною кримінального правопорушення є зчитування інформації з мереж мобільного чи супутникового зв'язку, зміна таких даних (ст. 361, 363, 363-1 КК України), то слід призначати експертизу телекомунікаційних систем і засобів [252].

На підставі дослідження наукових джерел, що стосуються призначення та проведення експертизи телекомунікаційних систем і засобів [66; 217, с. 310; 234, с. 188] й аналізу Інструкції [80], виокремимо такі об'єкти дослідження та окреслимо орієнтовний перелік вирішуваних питань, що ставлять перед експертом.

Об’єктами дослідження є: телекомунікаційні системи, засоби, мережі та їх складові, інформація, яка ними передається, приймається та обробляється (Інтернет IP вузли, вебсторінки, приймачі радіосигналів, наземні станції супутникового зв’язку, використання доменних імен у мережі Інтернет тощо).

Наведемо перелік питань, що можуть бути поставлені на вирішення експерту: 1) який тип, марка і модель телекомунікаційного засобу; 2) чи телекомунікаційний засіб (об’єкт) знаходиться в робочому стані; 3) які особливості підключення до мережі телекомунікаційного засобу; 4) які технічні параметри в цього телекомунікаційного засобу (системи); 5) чи змінював користувач налаштування телекомунікаційної мережі, у який час, які їх значення; 6) чи є можливим керування роботою пристрою через засоби телекомунікації; 7) який загальний характер підключень до телекомунікаційної мережі виконував об’єкт; 8) який програмний засіб здійснював підключення до телекомунікаційної мережі; 9) чи здатний технічний засіб у процесі функціонування долати систему технічного захисту інформації; 10) чи дає змогу технічний засіб долати певну систему технічного захисту інформації; 11) яка топологія апаратних засобів, об’єднаних у телекомунікаційну систему; 12) чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації; 13) чи здійснювали доступ до телекомунікаційної системи та в який спосіб; 14) чи використовували ресурси та інформації в телекомунікаційній системі та в який спосіб; 15) чи є ознаки втручання в роботу телекомунікаційної системи; 16) чи могли апаратні засоби об’єднуватися в телекомунікаційну мережу та за якими ознаками; 17) які шляхи маршрутизації даних у телекомунікаційній системі; 18) чи можливе використання телекомунікаційного засобу для відповідних завдань.

Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій, обумовлено особливістю цієї категорії кримінальних правопорушень, оскільки їх вчинення пов’язано з використанням засобів інформаційних технологій. Серед процесуальних джерел доказів важливе значення має саме висновок експерта. Тому, щоб це джерело доказу було допустимим, необхідно враховувати всі

зазначені вище тактичні та процесуальні особливості отримання висновку експерта.

Висновки до розділу 3

Дослідження організаційно-тактичних особливостей розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій, дає підстави для таких висновків:

1. Визначено, що періодизація процесу розслідування кримінальних правопорушень, вчинених з використанням інформаційних комп'ютерних технологій, передбачає такі етапи: 1) вихідний етап; 2) початковий етап; 3) наступний етап; 4) завершальний етап.

2. Акцентовано, що в більшості вітчизняних досліджень, які стосувалися розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, увагу зосереджено саме на слідчих ситуаціях початкового етапу розслідування, натомість інші етапи розслідування залишалися поза увагою. Проаналізовано слідчі ситуації всіх чотирьох етапів розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій.

Слідчі ситуації, що можуть виникати на вихідному етапі розслідування зазначених кримінальних правопорушень, можна класифікувати на: 1) ситуації, коли є заява потерпілого чи повідомлення особи про вчинене кримінальне правопорушення; 2) ситуації, коли було виявлено з інших джерел обставини, що можуть свідчити про вчинення кримінального правопорушення.

Слідчі ситуації початкового етапу розслідування цієї категорії кримінальних правопорушень можна поділити на: 1) спосіб вчинення невідомий, особа кіберзлочинця невідома; 2) спосіб вчинення відомий, особа кіберзлочинця невідома; 3) спосіб вчинення невідомий, особа кіберзлочинця відома; 4) спосіб вчинення відомий, особа кіберзлочинця відома.

Слідчі ситуації, що складаються після вручення повідомлення про підозру, наступного етапу (третього) розслідування слід класифікувати на такі: 1) підозрюваний визнає свою вину, наявні фактичні дані вказують на його винуватість; 2) підозрюваний не визнає свою вину, наявні фактичні дані вказують на його винуватість; 3) підозрюваний визнає вину, але наявні фактичні дані не вказують на його винуватість або відсутність фактів й обставин, що вказують на його вину; 4) підозрюваний не визнає вину, наявні фактичні дані не вказують на його винуватість або відсутність фактів й обставин, що вказують на його вину.

Слідчі ситуації завершального етапу: 1) ситуація, коли на підставі зібраних під час досудового розслідування доказів потрібно закрити кримінальне провадження; 2) ситуація, де на підставі зібраних під час досудового розслідування доказів підозрюваний може бути звільнений від кримінальної відповідальності; 3) ситуація, коли на підставі зібраних під час досудового розслідування доказів слід звернутися до суду з обвинувальним актом, клопотанням про застосування примусових заходів медичного або виховного характеру.

3. Одним із напрямів проведення ефективного розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій, є висунення версій та розроблення плану розслідування. Висунення версій можна здійснювати на кожному з етапів розслідування таких кримінальних правопорушень (версії вихідного, початкового, наступного та завершального етапів).

4. Зазначено, що планування розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, слід тлумачити як наперед продуманий план дій слідчого (дізнавача, прокурора) у конкретному кримінальному провадженні з розслідування зазначених протиправних діянь, що складений як слідчим (дізнавачем, прокурором), так і за допомогою програмних засобів.

Запропоновано закріпити в КПК України обов'язок складання плану розслідування органом досудового розслідування з подальшим долученням його до матеріалів кримінального провадження. Зазначене буде свідченням того, що в процесі досудового розслідування було перевірено всі можливі версії вчинення

кримінального правопорушення та проведене розслідування було об'єктивним і неупередженим.

Запропоновано під час планування розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, використовувати можливості ШНМ. Використання їх сприятиме: 1) підвищенню ефективності та швидкості розслідування слідчим зазначених протиправних діянь; 2) економії часу щодо планування розслідування; 3) обранню найдоцільніших тактик і методів, які слід застосовувати в процесі досудового розслідування кримінальних правопорушень зазначеної категорії; 4) зниженню ймовірності того, що розслідування зайде в «глухий кут»; 5) забезпеченню захисту інтересів людини в кіберпросторі; 6) зменшенню кількості процесуальних і тактичних помилок з боку правоохоронних органів; 7) дотриманню вимог розумного строку під час кримінального провадження.

5. Проаналізовано тактичні та процесуальні особливості проведення огляду місця події, обшуку й допиту під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, а також досліджено особливості проведення окремих слідчих (розшукових) дій у зазначених кримінальних правопорушеннях в умовах воєнного стану.

Аргументовано, що в процесі проведення огляду місця події чи обшуку можна встановити певні визначальні риси потерпілого й підозрюваного в зазначених кримінальних правопорушеннях. Наприклад, дослідження засобу інформаційних комп'ютерних технологій, який належить потерпілому чи підозрюваному, під час проведення огляду місця події чи обшуку дасть змогу сформувати уявну картину про особу потерпілого чи підозрюваного, встановити його вподобання, «професійні звички» і «почерк» за наявними даними в засобі (ігри, застосунки, сайти тощо). Це згодом надасть можливість встановити з допитуваною особою психологічний контакт, обрати відповідну тактику допиту й застосувати відповідні тактичні прийоми під час допиту.

6. Запропоновано вдосконалити процес відеозапису екрана, створивши для слідчого операційну систему на базі Linux і додаткову програму для фіксації

протиправних дій. Ця програма повинна фіксувати всі дії слідчого з дослідження та фіксації доказової інформації, що залишена в електронному середовищі. Зокрема, програма має зафіксувати момент входу до операційної системи, відкриття відповідних програм фіксації, час здійснення дії, який ресурс досліджується тощо. Отримані дані відеозапису (компакт-диск, флеш-носій) мають бути долучені до протоколу огляду.

7. Доведено значущість залучення спеціаліста, а також висвітлено зміст і специфіку надання ним консультацій, пояснень, довідок та висновків під час розслідування зазначеної категорії кримінальних правопорушень.

Розглянуто процесуальні й тактичні особливості залучення експерта під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій.

ВИСНОВКИ

Здійснене дисертаційне дослідження надало можливість сформулювати наукові висновки, рекомендації та пропозиції, що можуть мати важливе теоретичне значення для криміналістичної науки, а також бути використаними під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. Основними з них є такі:

1. Першим задокументованим випадком у світі, пов'язаним зі злочинним використанням комп'ютера, можна вважати протиправні дії програміста М. А. Беннета, який змінив код програмного забезпечення Національного міського банку Міннеаполіса 1966 року.

Одним із перших фундаторів дослідження «комп'ютерного злочину» у світі є американець Д. Б. Паркер, який у книзі «Crime by Computer» (1976) сформулював визначення поняття «комп'ютерне зловживання» (*computer abuse).*

На важливості наукового вивчення такого криміногенного явища, як «комп'ютерні злочини», першим поміж вітчизняних учених 1991 року акцентував П. Д. Біленчук.

Однією з перших закріпила спеціальні норми про «комп'ютерні злочини» ФРН. Зокрема, у травні 1986 року було внесено зміни в КК ФРН, згідно з якими було закріплено кримінальну відповідальність за комп'ютерне шахрайство (§263a); незаконне отримання відомостей, які можуть бути відтворені або передані електронним або магнітним шляхом (§ 202a); комп'ютерний саботаж (§303b).

Дослідження українських учених-криміналістів, що стосуються проблемних питань розслідування «комп'ютерних злочинів», можна об'єднати в декілька груп за часовими межами: 1) дослідження українських науковців із часу проголошення незалежності України до початку XXI століття (1991–2000 роки); 2) наукові дослідження з методики розслідування «комп'ютерних злочинів», проведені протягом 2001–2014 років. Необхідність проведення наукових досліджень зумовлена стрімким розвитком і запровадженням інформаційних технологій у всіх

сферах суспільного життя, що своєю чергою спричинило істотне збільшення кількості таких кримінальних правопорушень. Також у цей період Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність, а в новому КК 2001 року було передбачено самостійний розділ про зазначені кримінальні правопорушення; 3) дослідження, що проводили в період з 2014 року й донині. Необхідність активізації проведення криміналістичних досліджень цієї групи кримінальних правопорушень зумовлена насамперед військовою агресією рф проти України, зокрема з використання кіберпростору. Крім того, упродовж зазначеного періоду прийнято низку нормативних документів, спрямованих на запобігання кримінальним правопорушенням аналізованої категорії.

2. Криміналістичну класифікацію кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій, запропоновано розглядати за кримінально-правовими та криміналістичними критеріями. За кримінально-правовими критеріями їх можна класифікувати в межах розділів Кримінального кодексу України, за криміналістичними – за особою злочинця, мотивом і метою, особою потерпілого, наслідками тощо.

3. Міжнародно-правові засади розслідування визначено в міжнародних нормативно-правових актах: Європейській конвенції про взаємну допомогу у кримінальних справах; Декларації ООН про злочинність і суспільну небезпеку; Конвенції ООН проти транснаціональної організованої злочинності; Конвенції про кіберзлочинність.

Інші країни гостро реагують на виклики кіберзлочинності, що засвідчує створення спеціальних структурних підрозділів з розслідування або допомоги в розслідуванні цих протиправних діянь у системі їх правоохоронних органів. Для забезпечення ефективного розслідування кримінальних правопорушень, що вчиняються з використанням комп'ютерних інформаційних технологій, має вагоме значення розширення міжнародного співробітництва між державами в цій сфері.

4. Визначено, що елементи криміналістичної характеристики досліджуваної категорії кримінальних правопорушень знаходяться в кореляційному зв'язку

(імовірних залежностях), а саме спосіб вчинення – зі слідами вчинення, обстановка – з особою злочинця.

5. Способом вчинення окреслених кримінальних правопорушень слід вважати сукупність послідовних дій суб'єкта (суб'єктів), що охоплюють дії з готування, вчинення та приховування, які спрямовані на досягнення певного злочинного результату з використанням інформаційних комп'ютерних технологій.

З огляду на реалії сьогодення, можна виокремити найтиповіші та найпоширеніші способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій: 1) використання шкідливого програмного забезпечення; 2) вчинення DoS/DDoS атак; 3) несанкціонований доступ до інформації; 4) шахрайство, вчинене з використанням інформаційних комп'ютерних технологій; 5) поширення шкідливого (протиправного) контенту (спам, погрози, створення, поширення та збут дитячої порнографії, заклики до вчинення насильства, домагання тощо); 6) порушення авторських чи суміжних прав з використанням інформаційних комп'ютерних технологій; 7) комплекс способів і використання інформаційних комп'ютерних технологій як засіб користування кіберпростором для вчинення інших кримінальних правопорушень.

Характер залишених електронних слідів залежить від таких факторів: виду операційної системи злочинця та потерпілого, особливостей засобів інформаційних комп'ютерних технологій та їх програмного забезпечення тощо. Однак під час розслідування кримінальних правопорушень цієї категорії не слід нехтувати матеріальними й ідеальними слідами.

6. У структурі обстановки як елементу криміналістичної характеристики зазначених протиправних діянь слід виокремити: 1) кіберпростір, що передбачає місце, час, віртуальну взаємодію учасників кримінального правопорушення; 2) матеріальне середовище – (ділянка території, сукупність різних предметів, поведінка учасників події, психологічні відносини).

Типовими ознаками, що характеризують особу кіберзлочинця, можуть бути: 1) загальні (вік, освіта, професія); 2) психологічні (темперамент, характер, інтереси

та схильності, мотиви й стиль поведінки, певні психічні відхилення); 3) спеціальні («професійні звички» та «почерк» кіберзлочинця).

7. Виокремлення слідчих ситуацій, що можуть виникати під час розслідування кримінальних правопорушень, які вчиняють з використанням інформаційних комп'ютерних технологій, здійснюють залежно від етапу розслідування, криміналістичної характеристики та повідомлення про підозру особі.

8. Версії розслідування можуть бути сформовані залежно від етапів розслідування. *Версії вихідного етапу:* вчинено кримінальний проступок; вчинено злочин; немає ознак вчинення зазначених кримінальних правопорушень. *Версії початкового етапу:* версії, що стосуються місцеперебування злочинця; версії про місце використання засобів інформаційно-комп'ютерних технологій; версії, що стосуються часу вчинення; версії, що стосуються слідів. *Версії наступного етапу:* підозрюваний не вчиняв зазначеного протиправного діяння, а справжній злочинець використав його засіб інформаційних комп'ютерних технологій; справжній злочинець навмисно вирішив заплутати слідчого, щоб пустити його «хибним шляхом»; кримінальне правопорушення вчинив хтось зі знайомих підозрюваного, і він хоче взяти вину на себе; підозрюваний не розумів характер своїх дій та вчинків; правопорушення було вчинено групою осіб, і підозрюваний не бажає свідчити проти них; підозрюваний, спланувавши кримінальне правопорушення, розрахував, що фактичні дані не будуть вказувати на нього; підозрюваний вважає, що він ретельно знищив усі сліди свого протиправного діяння. *Версії завершального етапу:* чи всі фактичні дані вказують на необхідність закриття кримінального правопорушення; чи всі фактичні дані вказують на доведення невинуватості підозрюваного; чи є достатніми зібрані докази, що вказують на доведення винуватості підозрюваного.

Обґрунтовано, що планування розслідування зазначених кримінальних правопорушень слід здійснювати в письмовій формі. Це обумовлено специфікою таких кримінальних правопорушень, складністю термінології, недостатністю навичок у слідчих з розслідування, необхідністю залучення спеціаліста, а також

особливостями проведення слідчих (розшукових) і негласних слідчих (розшукових) дій та організаційних заходів тощо. План розслідування може бути складено як шляхом письмового викладення слідчим його змісту, що є результатом його розумової діяльності, так і за допомогою застосування програмних засобів.

9. Схарактеризовані тактичні особливості проведення огляду місця події в кримінальних правопорушеннях, що вчиняються з використанням інформаційних комп'ютерних технологій, а саме: забезпечення цілісності й охорони місця проведення огляду події; визначення, що буде об'єктами огляду, їх кількість, специфіка та послідовність проведення; підготовка відповідного обладнання; з'ясування в осіб інформації, якою вони володіють з приводу події.

Аргументовано доцільність запрошення понятих для участі в проведенні огляду місця події з міркувань, що зазначені особи потім можуть бути допитані під час судового розгляду як свідки, своїми показаннями сприятимуть підтвердженню зібраних (отриманих) доказів як допустимих.

Під час складання протоколу огляду слід дотримуватися таких рекомендацій: кожен досліджуваний засіб інформаційних комп'ютерних технологій повинен бути чітко описаний в протоколі (марка, модель, заводський та інвентарний номери, технічні особливості, його місце розташування тощо); якщо відбувалося дослідження програмних засобів, необхідно зазначити, як вони були досліджені та в якому саме засобі інформаційно-комп'ютерних технологій; окремо зазначати час дослідження кожного засобу інформаційних комп'ютерних технологій; важливим є правильний запис усіх серійних номерів, хеш-сум, назв пристроїв тощо; у разі використання певних програм для дослідження засобів інформаційних комп'ютерних технологій необхідно зазначити про це; особливу цінність для розслідування будуть мати лог-файли (Log file), файли в яких містять інформацію про роботу засобу інформаційних комп'ютерних технологій.

Сформовано тактичні рекомендації проведення обшуку: 1) у клопотанні про обшук слід чітко визначити засоби інформаційно-комп'ютерних технологій, які необхідно відшукати, а до проведення обшуку ознайомитися з їх характеристикою; 2) якщо під час обшуку виявлено доступ чи можливість доступу до комп'ютерних

систем або їх частин, мобільних терміналів систем зв'язку, які не зазначені в ухвалі слідчого судді, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, слідчий, прокурор має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них містяться, на місці проведення обшуку. У разі їх вилучення такі речі вважають тимчасово вилученим майном (ч. 6 ст. 236 КПК України); 3) варто встановити психологічний контакт з особою, у якої відбувається обшук; 4) зосередити увагу на всіх пристроях збереження даних (флешки, диски тощо); 5) у разі необхідності провести груповий обшук.

Під час планування допиту доцільно використовувати можливості штучного інтелекту, який слідчий, дізнавач, прокурор зможуть залучати як у процесі підготовки до допиту, так і під час його проведення. Штучний інтелект буде рекомендувати, які питання необхідно ставити залежно від виду та специфіки розслідування кримінального правопорушення та спрямовувати перебіг допиту в ефективне русло.

Зазначено, що в окреслених кримінальних правопорушеннях під час проведення допиту потерпілого та підозрюваного є певні особливості встановлення психологічного контакту між його учасниками. Особливість встановлення психологічного контакту полягає в тому, що він може виникати між слідчим і потерпілим/підозрюваним, з одного боку, а також між спеціалістом і потерпілим/підозрюваним – з другого.

Запропоновано рекомендації зі створення необхідної атмосфери, за якої в підозрюваного й потерпілого під час допиту формуватиметься повага до суб'єкта розслідування. Цього може бути досягнуто завдяки: 1) ретельній підготовці до допиту в зазначених категоріях кримінальних правопорушень; 2) обговоренню заздалегідь зі спеціалістом питань, на які буде спрямовано увагу в процесі допиту; 3) розумінню питань, що ставитиме спеціаліст під час допиту; 4) активності й інтересу слідчого, дізнавача, прокурора в з'ясуванні всіх технічних обставин кримінального правопорушення; 5) проведенню допиту відповідно до обговореного зі спеціалістом плану.

У кримінальних правопорушеннях зазначеної категорії, специфіка яких полягає у вчинення їх у кіберпросторі та за допомогою засобів інформаційних комп'ютерних технологій, найрезультативнішими є негласні слідчі (розшукові) дії, які дають змогу зібрати (отримати) якомога більше доказів винуватості особи, а саме: зняття інформації з електронних комунікаційних мереж (ст. 263 КПК України); зняття інформації з електронних інформаційних систем (ст. 264 КПК України) й установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ст. 268 КПК України). Використання результатів негласних слідчих (розшукових) дій дозволяють здійснити перевірку висунутих версій та зрозуміти, які тактичні прийоми необхідно застосовувати надалі для проведення розслідування.

10. Визначено, що в кримінальних правопорушеннях, які вчиняють з використанням інформаційних комп'ютерних технологій, передбачено дві форми використання спеціальних знань у кримінальному провадженні – залучення експерта для проведення судової експертизи та залучення спеціаліста для надання допомоги під час проведення окремих процесуальних дій.

Залучення спеціаліста в кримінальних правопорушеннях цієї категорії набуває значущості під час проведення огляду місця події та обшуку, адже вони безпосередньо пов'язані з виявленням, вилученням засобів інформаційних комп'ютерних технологій та їх дослідженням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Г. К., Стороженко С. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2017. № 1 (77). С. 169–176. URL: https://journal.lduvs.lg.ua/index.php/journal/article/view/341.

2. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. ... канд. юрид. наук : 12.00.08. Київ, 2002. 246 с.

3. Аналіз трафіку. *Вікіпедія :* [сайт]. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D1%82%D1%80%D0%B0%D1%84%D1%96%D0%BA%D1%83.

4. Анапольська А. І. Розслідування шахрайств і пов’язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2011. 18 с.

5. Англо-український словник термінів з інформаційних технологій та кібербезпеки : уклад. А. Я. Гладун, О. О. Пучков, І. Ю. Субач, К. О. Хала. Київ : КПІ ім. І. Сікорського, 2018. 380 с.

6. Анонімус (угрупування). *Вікіпедія :* [сайт]. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%BE%D0%BD%D1%96%D0%BC%D1%83%D1%81_(%D1%83%D0%B3%D1%80%D1%83%D0%BF%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F).

7. Антонюк П. Є. Щодо сутності письмового пояснення спеціаліста у кримінальному провадженні. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали II Міжнар. наук.-практ. конф. (Київ, 19 листоп. 2020 р.) / за заг. ред. О. Г. Рувіна, Н. В. Нестор. Київ : Ліра-К, 2020. С. 47–50.

8. Антонюк П. Є., Пясковський В. В. Письмове пояснення спеціаліста в системі процесуальних джерел доказів на досудовому розслідуванні кримінальних

правопорушень. *Криміналістика і судова експертиза.* 2021. Вип. 66. С. 332–341. DOI: https://doi.org/10.33994/kndise.2021.66.32.

9. Антонюк П. Є., Свобода Є. Ю., Михальчук Т. В. Висновок спеціаліста як джерело доказів у кримінальному провадженні: аналіз процесуальної спроможності. *Криміналістика і судова експертиза.* 2021. Вип. 66. С. 88–95. DOI: https://doi.org/10.33994/kndise.2021.66.10.

10. Ахтирська Н. М., Костюченко О. Ю. Процесуальні та організаційні аспекти збору електронних доказів під час міжнародного співробітництва. *Науковий вісник Ужгородського національного університету.* 2022. Вип. 72. С. 192–198.

11. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–174. URL: http://www.lsej.org.ua/1_2019/47.pdf.

12. Ахтирська Н. М. Актуальні питання розслідування кіберзлочинів : навч. посіб. Київ : Київ. ун-т, 2018. 229 с.

13. Ахтирська Н. М. Міжнародне співробітництво під час кримінального провадження: теоретичні та практичні аспекти : монографія. Київ : Логос, 2019. 576 с.

14. Ахтирська Н. М. Одержання доказів в електронній формі в світлі другого додаткового протоколу до Конвенції про кіберзлочинність. *Криміналістика і судова експертиза.* 2022. Вип. 67. С. 188–200. DOI: https://doi.org/10.33994/kndise.2022.67.21.

15. Бараненко Р. В. Кіберзлочин, комп’ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник Національного технічного університету України «Київський політехнічний інститут».* 2021. Вип. 1 (49). С. 85–90. (Серія «Політологія. Соціологія. Право»).

16. Безпека комп’ютерних систем: злочинність у сфері комп’ютерної інформації та її попередження / за ред. О. П. Снігерьова. Запоріжжя, 1998. 316 с.

17. Биленчук П. Д., Минченко А. В. Компьютерная преступность: правовые, психологические и технико-криминалистические аспекты. *Именем Закона.* 1991. № 43. С. 6.

18. Біленчук П. Д., Гель А. П., Семаков Г. С. Криміналістична тактика і методика розслідування окремих видів злочинів : навч. посіб. Київ : МАУП, 2007. 512 с.

19. Біленчук П. Д. Криміналістична характеристика портрету комп'ютерного злочинця. *Проблеми юридичної науки та правоохоронної практики.* 1994. С. 260–262.

20. Біленчук П. Д., Дубовий О. П., Салтевський М. В., Тимошенко П. Ю. Криміналістика : підручник / за ред. П. Д. Біленчука. Київ : Атіка, 1998. 416 с.

21. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : монографія. Київ : Укр. акад. внутр. справ, 1994. 72 с.

22. Біленчук П. Д., Котляревський О. І. Портрет комп'ютерного злочинця : навч. посіб. Київ : B&B, 1997. 48 с.

23. Біленчук П. Д., Кофанов А. В., Кобилянський О. Л., Паніотов Є. К. Транснаціональна злочинність: криміналістичний аналіз : монографія / за ред. П. Д. Біленчука. Київ : КИЙ, 2011. 52 с.

24. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2008. 245 с.

25. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2007. 19 с.

26. Ботнет – Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82.

27. 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. / за заг. ред. Л. П. Скалозуба, І. В. Бондаренко. Київ : Аванпост Прим, 2010. 245 с.

28. Велика українська енциклопедія : у 20 т. / [редкол.: В. Ю. Шепітько (голова) та ін.]. Харків : Право, 2016. Т. 20 : Криміналістика, судова експертиза, юридична психологія. 952 с.

29. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2001. 1440 с.

30. Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2002. 19 с.

31. Вертузаєв М. С. Комп'ютерна злочинність в Україні: міфи та реальність. *Науковий вісник Української академії внутрішніх справ.* 1997. Вип. 1. С. 203–213.

32. Весельський В. К. Слідча ситуація як категорія криміналістичної тактики. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2011. № 25. С. 193–199.

33. Весельський В. К., Зав'ялов С. М., Пясковський В. В. Сучасні можливості використання даних про спосіб вчинення злочину у боротьбі зі злочинністю : навч. посіб. Київ : КНТ, 2009. 160 с.

34. Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ : монография / под ред. Б. П. Смагоринского. Волгоград : ВА МВД России, 2004. 304 с.

35. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Вид. 2-ге, доповн. Київ : Нац. акад. внутр. справ, 2020. 104 с.

36. Вирок Києво-Святошинського районного суду Київської області від 9 листоп. 2021 р. Справа № 369/7959/21. URL: https://reyestr.court.gov.ua/Review/100915432.

37. Вирок Київського районного суду міста Полтави від 12 серп. 2022 р. Справа № 552/4247/22. URL: https://reyestr.court.gov.ua/Review/105802658.

38. Вирок Смілянського міськрайонного суду Черкаської області від 29 квіт. 2022 р. Справа № 703/3236/21. URL: https://reyestr.court.gov.ua/Review/104124210.

39. Вирок Суворовського районного суду міста Одеси від 16 берез. 2021 р. Справа № 523/15231/20. URL: https://reyestr.court.gov.ua/Review/95592285.

40. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій : наук.-практ. посіб. / за заг. ред. Я. Ю. Кондратьєва. Київ, 2004. 144 с.

41. Вказана Microsoft програма для знищення даних з високою ймовірністю є складовою кібератаки на державні органи. URL: https://cip.gov.ua/ua/news/vkazana-microsoft-programa-dlya-znishennya-danikh-z-visokoyu-imovirnistyu-ye-chastinoyu-kiberataki-na-derzhavni-organi.

42. Волобуєв А. Ф. Використання спеціальних знань при розслідуванні розкрадань з використанням комп'ютерної техніки. *Актуальные вопросы судебной экспертизы и криминалистики на современном этапе судебно-правовой реформы :* сб. науч.-практ. материалов (к 75-летию основания Харьковского НИИ судебных экспертиз). Харьков : Право, 1998. С. 228–230.

43. Волобуєв А. Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки. *Вісник Луганського інституту внутрішніх справ МВС України.* 1998. Вип. 2. С. 179–185.

44. Волобуєв А. Ф. Проблеми розслідування «комп'ютерних» злочинів. *Вісник Університету внутрішніх справ.* 1996. Вип. 1. С. 63–70.

45. Гавловський В. Д., Цимбалюк В. С. Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій. *Боротьба з контрабандою: проблеми та шляхи їх вирішення.* Київ, 1998. С. 148–154.

46. Галаган В. І. Проведення слідчих (розшукових) дій: процесуальні та криміналістичні аспекти. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2017. Вип. 1 (5). С. 73–79.

47. Ганс Гросс. Руководство для судебных следователей как система криминалистики. Киев : Центр учеб. лит., 2021. 1080 с.

48. Геселев О. В., Присяжнюк І. І., Соколова Я. А., Щербакова Г. В. Сучасні проблеми криміналістики : навч. посіб. Київ : Нац. акад. прокуратури України ; Кіровоград : Антураж А, 2012. 424 с.

49. Глушков В. М. Основы безбумажной информатики. М. : Наука, 1987. 552 с.

50. Голубєв В. О. Комп'ютерні злочини в банківській діяльності. Запоріжжя : Павел, 1997. 118 с.

51. Голубєв В. О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : ЗІДМУ, 2003. 296 с.

52. Голубєв В. О. Теоретико-правові проблеми боротьби з комп'ютерною злочинністю. *Вісник Запорізького юридичного інституту.* 1999. № 4. С. 52–60.

53. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використанням комп'ютерних технологій. Запоріжжя : Просвіта, 2001. 252 с.

54. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використанням комп'ютерних технологій : навч. посіб. Запоріжжя : ЗІДМУ, 2002. 292 с.

55. Голубєв В. О., Юрченко О. М. Злочини у сфері комп'ютерної інформації: способи скоєння, засоби захисту. Запоріжжя : Запоріз. юрид. ін-т, 1998. 156 с.

56. Голубєв В.О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту.* 1997. № 2. С. 39–40.

57. Гора І. В., Іщенко А. В., Колесник В. А. Криміналістика : посібник. Київ : Паливода А. В., 2004. 236 с.

58. Гора І. В., Колесник В. А. Криміналістика : посібник. Київ : Паливода А. В., 2003. 146 с.

59. Гусєва В. О. Методика розслідування злочинів проти авторитету органів державної влади у сфері правоохоронної діяльності : монографія. Харків : У справі, 2020. 452 с.

60. Давидова Д. В., Волобуєв О. О. Висновок експерта як процесуальне джерело доказів: окремі аспекти теорії та практики. *Південноукраїнський правничий часопис.* 2015. № 2. С. 151–154. URL: http://www.sulj.oduvs.od.ua/archive/2015/2/46.pdf.

61. Даньшин М. В. Класифікація способів приховування злочинів у криміналістиці : автореф. дис. … канд. юрид. наук : 12.00.09. Харків, 2000. 19 с.

62. Декларація ООН про злочинність і суспільну небезпеку : міжнар. док. від 12 груд. 1996 р. URL: https://zakon.rada.gov.ua/laws/show/995_371#Text.

63. Джордж Е., Меріда Ф., Расмуссен У., Волзов В., Джонс Н. Посібник з питань електронних доказів: базовий посібник для співробітників правоохоронних органів, прокурорів та суддів. Версія 2.1. Відділ протидії кіберзлочинності. Страсбург, Франція. 2020. 218 с.

64. Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис. … канд. юрид. наук : 12.00.09. Одеса, 2014. 20 с.

65. Динту В. А. Місце кіберпростору у системі обстановки злочину. *Науковий вісник Херсонського державного університету.* 2016. Вип. 2. Т. 3. С. 72–75.

66. Довідник проведення судових експертиз та експертних досліджень. Кропивницький, 2019. URL: https://www.advrada.kr.ua/files/a-kndise-dovidnyk.pdf.

67. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : міжнар. док. від 28 січ. 2003 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.

68. Дудич А. В. Експерт як учасник кримінального провадження : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2017. 253 с.

69. Дуфенюк О. М. Експертиза у кримінальному провадженні за законодавством України та Польщі: порівняльне дослідження : монографія. Львів : ЛьДУВС, 2018. 272 с.

70. Експертизи у судовій практиці : наук.-практ. посіб. / за заг. ред. В. Г. Гончаренка. Київ : Юрінком Інтер, 2005. 387 с.

71. Європейська конвенція про взаємну допомогу у кримінальних справах : міжнар. док. від 20 квіт. 1959 р. URL: https://zakon.rada.gov.ua/laws/show/995_036#Text.

72. Європіна І. В. Криміналістичне забезпечення протидії комп'ютерній злочинності : дис. … канд. юрид. наук : 12.00.09. Київ, 2011. 218 с.

73. Журавель В. Проблеми періодизації досудового розслідування. *Вісник Національної академії правових наук України.* 2014. № 2 (77). С. 136–144.

74. Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 232 с.

75. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення. *Computer Emergency Response Team of Ukraine.* URL: https://cert.gov.ua/recommendation/2502.

76. Захист інформації в комп'ютерних системах : підручник / уклад.: О. М. Гапак, С. І. Балога. Ужгород : АУТДОР-ШАРК, 2021. 184 с.

77. Злочини майбутнього / пер. з англ. І. Мазарчук, Я. Малишко. Харків, 2019. 592 с.

78. Іванов В. Г. Основи інформатики та обчислювальної техніки : підручник / за заг. ред. В. Г. Іванова. Харків : Право, 2012. 312 с.

79. Інструкція з організації діяльності слідчих підрозділ Національної поліції України : наказ МВС України від 6 лип. 2017 р. № 570. URL: https://zakon.rada.gov.ua/laws/show/z0919-17#Text.

80. Інструкція про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98.

81. Інформаційні технології в бізнесі. Частина 1 : навч. посіб. / за заг. ред. І. Б. Шевчука. Львів : АТБ, 2020. 455 с.

82. Інформаційно-комунікаційні технології в бізнесі : навч. посіб. / уклад. М. О. Чупріна. Київ : КПІ ім. І. Сікорського, 2020. 116 с. URL: https://ela.kpi.ua/bitstream/123456789/33703/1/Infor_tech.pdf.

83. Калюга К. В. Окрема криміналістична теорія про зовнішні ознаки та властивості особи злочинця : монографія. Запоріжжя : КСК-Альянс, 2017. 296 с.

84. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис.* 2017. № 1 (9). С. 140–144.

85. Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Київ : Атіка, 2010. 168 с.

86. Керівництво з розслідування злочинів : наук.-практ. посіб. / за ред. В. Ю. Шепітька. Харків : Одіссей, 2009. 960 с.

87. Кіберполіція викрила юного хакера у створенні та продажі шкідливого програмного забезпечення. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-yunogo-xakera-u-stvorenni-ta-prodazhi-shkidlyvogo-programnogo-zabezpechennya-1585/.

88. Клименко Н. І. Судова експертологія: курс лекцій : навч. посіб. Київ : Ін Юре, 2007. 526 с.

89. Климчук М. П., Коміссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2022. 112 с.

90. Книженко С. О., Матюшкова Т. П. Правові, організаційні і тактичні основи проведення дистанційного досудового розслідування. *Бюлетень обміну досвідом роботи МВС України.* 2015. № 201. С. 116–125.

91. Коваленко А. В. Висновок спеціаліста як нове процесуальне джерело доказів у кримінальному провадженні (проблеми та перспективи). *Актуальні питання розвитку права та законодавства: наукові дискусії :* матеріали Міжнар. наук.-практ. конф. (Львів, 18–19 груд. 2020 р.). Львів : Центр правн. ініціатив, 2020. Ч. 2. С. 187–190.

92. Ковальов В. В. Взаємодія слідчого з працівниками експертної служби МВС України : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2008. 20 с.

93. Когутич І. І. Окремі питання сутності та форм використання спеціальних знань у кримінальному провадженні. *Вісник Академії адвокатури України*. 2005. Число 2 (33). С. 112–123.

94. Козак Н. С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : автореф. дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2011. 18 с.

95. Колесниченко А. Н., Матусовский Г. А. О системе версий и методике их построения. *Криминалистическая и судебная экспертиза*. 1970. № 7. С. 7–13.

96. Колесниченко А. Н. Планирование советского предварительного следствия : дис. ... канд. юрид. наук : 12.00.09. Харьков, 1952. 261 с.

97. Колесниченко А. Н. Роль следственных версий и построение их при расследовании преступлений. *Ученые записки Харьковского юридического института*. 1957. Вып. 9. С. 163–171.

98. Конвенція ООН проти транснаціональної організованої злочинності : міжнар. док. від 15 листоп. 2000 р. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text.

99. Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.

100. Коновалова В. Е. Версия: концепция и функции в судопроизводстве. Харьков : Консум, 2000. 176 с.

101. Коновалова В. О., Шепітько В. Ю. Юридична психологія : підручник. Харків : Право, 2008. 240 с

102. Коновалова В. Е. Допрос: тактика и психология. Харьков : Консум, 1999. 157 с.

103. Коновалова В. О. Вбивство: мистецтво розслідування : монографія. Харків : Факт, 2001. 311 с.

104. Копча В. В. Криміналістична техніка, тактика і методика : навч. посіб. Одеса : Гельветика, 2022. 286 с.

105. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … канд. юрид. наук : 081. Київ, 2021. 255 с.

106. Костюченко О., Ахтирська Н. Міжнародні стандарти правової регламентації судової експертизи та їх впровадження в Україні. *Вісник Київського*

національного університету імені Тараса Шевченка. 2022. № 3 (122). С. 31–39. DOI: https://doi.org/10.17721/1728-2195/2022/3.122-6.

107. Крижевський А. В. Криміналістична характеристика шахрайств у сфері мобільного зв'язку : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2012. 20 с.

108. Криміналістика : підручник : у 2 т. / [В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. Харків : Право, 2019. Т. 1. 456 с.

109. Криміналістика у питаннях і відповідях : навч. посіб. / [А. В. Іщенко, В. В. Пясковський, А. В. Самодін та ін.]. Київ : Центр учб. літ., 2016. 118 с.

110. Криміналістика : підручник / [В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін.]. Київ : Центр учб. літ., 2015. 544 с.

111. Криміналістика : підручник / [П. Д. Біленчук, В. К. Лисиченко, Н. І. Клименко та ін.] ; за ред. П. Д. Біленчука. 2-ге вид., випр. і доповн. Київ : Атіка, 2001. 544 с.

112. Криміналістика : підручник / [Р. І. Благута, О. І. Гарасимів, О. М. Дуфенюк та ін.] ; за заг. ред. Є. В. Пряхіна. 3-тє вид, переробл. та доповн. Львів : ЛьвДУВС, 2016. 948 с.

113. Криміналістика : підручник / за ред. В. В. Тіщенка. Одеса : Гельветика, 2017. 556 с.

114. Криміналістика : підручник : у 2 т. / [В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. Харків : Право, 2019. Т. 2. 382 с.

115. Криміналістика. Академічний курс : підручник / [Т. В. Варфоломеєва, В. Г. Гончаренко, В. І. Бояров та ін.]. Київ : Юрінком Інтер, 2011. 504 с.

116. Криміналістика. Криміналістична тактика і методика розслідування злочинів : підручник / за ред. В. Ю. Шепітька. Харків : Право, 1998. 376 с.

117. Криміналістика: питання і відповіді : навч. посіб. / [А. В. Кофанов, О. Л. Кобилянський, Я. В. Кузьмічов та ін.]. Київ : Центр учб. літ., 2011. 280 с.

118. Кримінальне право України. Загальна частина : підручник / [А. А. Васильєв, Є. О. Гладкова, О. О. Житний та ін.] ; за заг. ред. О. М. Литвинова. Харків : Харків. нац. ун-т внутр. справ, 2020. 428 с.

119. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

120. Кримінальний кодекс України : Закон УРСР від 28 груд. 1960 р. № 2001-05. URL: https://zakon.rada.gov.ua/laws/show/2002-05#Text.

121. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

122. Кузьмін С. А. 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. Київ : Паливода А. В., 2019. 168 с.

123. Ламо А. *Вікіпедія :* [сайт]. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%B4%D1%80%D1%96%D0%B0%D0%BD_%D0%9B%D0%B0%D0%BC%D0%BE.

124. Левков В. М. Криміналістичні версії : текст лекції. Харків : Юрид. ін-т, 1990. 24 с.

125. Леонов А. Особливості проведення негласних слідчих (розшукових) дій під час досудового розслідування кримінальних проваджень. *Закон і Бізнес.* URL: https://zib.com.ua/ua/136530-osoblivosti_provedennya_nsrd_v_kriminalnomu_provadzhenni.html.

126. Лук'янчиков Б. Є., Лук'янчиков Є. Д., Петряєв С. Ю. Криміналістика : навч. посіб. : у 2 ч. Київ : КПІ ім. І. Сікорського, 2017. Ч. II : Криміналістична тактика. Методика розслідування. 474 с.

127. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал.* 2014. № 4. С. 202–205.

128. Максимів Л. В. Окремі аспекти взаємодії слідчого з експертом та спеціалістом у кримінальному провадженні в умовах воєнного стану. *Вісник Луганського держаного університету внутрішніх справ ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 262–271. DOI: 10.33766/2524-0323.99.262-271.

129. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.

130. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ.* 2016. № 3 (74). С. 111–120.

131. Марушевич А. Д. Консультація як одна з форм використання спеціальних знань у кримінальному провадженні. *Юридичний науковий електронний журнал.* 2020. № 4. С. 307–310.

132. Матусовский Г.А. Экономические преступления: криминалистический анализ. Харьков : Консум, 1999. 480 с.

133. Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави :* зб. матеріалів наук.-практ. конф. : у 2 ч. (Київ, 22 берез. 2011 р.). Київ : Вид-во НА СБ України, 2011. Ч. 2. С. 43–48.

134. Методика розслідування окремих видів злочинів : навч. посіб. / за заг. ред. Є. В. Пряхіна. 2-ге вид., переробл. та доповн. Львів : ЛьвДУВС, 2019. 312 с.

135. Методичні рекомендації щодо особливостей проведення допиту, впізнання в режимі відеоконференції під час досудового розслідування / [О. О. Юхно, С. Є. Абламський, О. О. Бондаренко та ін.]. *Законодавче забезпечення правоохоронної діяльності :* навч. посіб. / за заг. ред. В. В. Сокуренка. Харків : Стильна типографія, 2017. С. 327–354.

136. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 19 с.

137. Моїсеєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів. *Правові основи захисту комп'ютерної інформації від протиправних посягань :* матеріали міжвуз. наук.-практ. конф. (Донецьк, 22 груд. 2000 р.). Донецьк : Дон. ін-т внутр. справ, 2001. С. 81–85.

138. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 221 с.

139. На Міністерство охорони здоров'я США здійснено кібератаку. URL: https://ukrainian.voanews.com/a/5331180.html.

140. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

141. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. С. 359– 364. URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf.

142. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*. 2020. Вип. 88. С. 202–212. (Серія «Юридичні і політичні науки»).

143. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Криміналістика і судова експертиза*. 2021. Вип. 66. С. 453–460.URL : http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf.

144. Неділько Я. В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 292–301. DOI: https://doi.org/10.33994/kndise.2022.67.30.

145. Неділько Я. В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій. *Knowledge, Education, Law, Management.* 2021. № 8 (44). Vol. 2. С. 119–124. DOI: https://doi.org/10.51647/kelm.2021.8.2.19.

146. Неділько Я. В. Строки досудового розслідування у контексті змін до кримінального процесуального кодексу України. *Проблеми реформування*

кримінальної юстиції України : зб. матеріалів Міжнар. наук.-практ. конф. (Чернівці, 17–18 трав. 2018 р.). С. 198–201.

147. Неділько Я. В. Класифікація особи кіберзлочину як елемента криміналістичної характеристики. *Пріоритетні напрямки розвитку правової системи України* : матеріали Міжнар. наук.-практ. конф. (Львів, 25–26 січ. 2019 р.). С. 112–114.

148. Неділько Я. В. Спосіб вчинення злочину як елемент криміналістичної характеристики кіберзлочинів. *Conceptul de dezvoltare a statului de drept in repiblica Moldova si Ucraina in contextual proceselor de eurointegrare* (Chisinau, 1–2 noiembrie 2019). Chisinau, Republica Moldova, 2019. С. 236–238.

149. Неділько Я. В. Проблемні питання підслідності кіберзлочинів. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці* : матеріали Міжнар. круглого столу (Харків, 12 груд. 2019 р.). Харків, 2019. С. 105–109.

150. Неділько Я. В. Поняття кіберзлочину та особливості його закріплення в національному законодавстві. «*Інтернет речей»: проблеми правового регулювання та впровадження* : матеріали ІІ наук.-практ. конф. (Київ, 29 листоп. 2018 р.). Київ, 2018. С. 112–114.

151. Неділько Я. В. Особливості проведення допиту підозрюваного у кіберзлочинах. *Кримінальний процес та криміналістика: сучасний стан та перспективи* : тези доп. Всеукр. наук.-практ. конф.(Харків, 26 листоп. 2020 р.). С. 252–255.

152. Неділько Я. В. Основні аспекти використання спеціальних знань під час розслідування кіберзлочинів. *Актуальні питання кримінального права, кримінології та судочинства* : матеріали Всеукр. наук.-практ. конф., присвяч. 165-й річниці з дня народж. проф. Л. С. Білогриць-Котляревського (Київ, 15 трав. 2020 р.). Київ, 2020. С. 85–88.

153. Неділько Я. В. Використання штучної нейронної мережі при плануванні розслідування кіберзлочинів. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали

ІІ Міжнар. наук.-практ. інтернет-конф. (Київ, 19 листоп. 2020 р.). Київ, 2020. С. 382–385.

154. Неділько Я. В. Особливості проведення огляду під час розслідування кіберзлочинів. *Донецький юридичний інститут МВС України: освітні традиції, перевірені часом* : матеріали Міжнар. наук.-практ. конф. до 60-річчя заснування закладу освіти (Маріуполь, 28 квіт. 2021 р.). Маріуполь, 2021. С. 279–292. URL: http://repo.dli.donetsk.ua/bitstream/123456789/1704/1/210512_1543_A5_442pages_i.pdf.

155. Неділько Я. В, Ахтирська Н. М. Особливості встановлення психологічного контакту слідчого з підозрюваним під час допиту щодо кіберзлочинів. *Актуальні проблеми кримінального процесу та криміналістики :* тези доп. Міжнар. наук.-практ. конф. (Харків, 29 жовт. 2021 р.). Харків, 2021. С. 254–256.

156. Неділько Я. В. Використання штучного інтелекту під час розслідування кіберзлочинів. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України* : матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.). Київ, 2022. С. 275–278.

157. Неділько Я. В. Особливості проведення огляду комп’ютерних даних під час розслідування кіберзлочинів в у мовах воєнного стану. *Актуальні питання розвитку юридичної науки та практики :* матеріали Міжнар. наук.-практ. конф. (Київ, 12 трав. 2022 р.). Київ, 2022. С. 288–290.

158. Неділько Я. В. Процесуальна регламентація надання пояснень спеціалістом під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій. *Використання цифрової інформації в розслідуванні кримінальних правопорушень* : матеріали Міжнар. наук.-практ. круглого столу (Харків, 12 груд. 2022 р.). Харків, 2022. С. 62–65. DOI: https://doi.org/10.31359/978-966-998-460-9.

159. Никоненко М. Я. Пояснення в системі джерел доказів у кримінальному провадженні про кримінальні проступки. *Науковий вісник Міжнародного гуманітарного університету.* 2020. № 43. С. 163–167.

160. Нізовцев Ю. Ю. Шкідливі програмні засоби: поняття, різновиди та судово-експертне дослідження : метод. посіб. Київ : ІСТЕ СБ України, 2021. 130 с.

161. Нізовцев Ю. Ю., Омельян О. С. Судово-експертне дослідження ознак віддалених кібератак на відмову в обслуговування : метод. посіб. Київ : ІСТЕ СБ України, 2021. 124 с.

162. Опитування прокурорів проводилось з 15 по 25 липня 2022 року. URL: https://forms.gle/pSPC5mdMt8qpwwSb8.

163. Пазиніч В. І. Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 16 с.

164. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. … канд. юрид. наук : 12.00.09. Київ, 2004. 215 с.

165. Пасека О. М. Поняття особи неповнолітнього правопорушника. *Науковий вісник Міжнародного гуманітарного університету.* 2014. № 1–9. С. 215–217. (Серія «Юриспруденція»).

166. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Харків, 2007. 228 с.

167. Пиріг І. В., Бідняк Г. С. Використання спеціальних знань на досудовому розслідуванні : навч. посіб. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2019. 140 с.

168. Погорецький М. А. Впровадження інституту негласних (розшукових) слідчих дій в правозастосовну практику. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 2 (28). С. 56–63.

169. Погорецький М., Шеломенцев В. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.

170. Поливанюк В. Д. Особливості розслідування злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2008. 17 с.

171. Постанова Верховного Суду від 10 груд. 2020 р. у справі № 473/2485/17. URL: https://reyestr.court.gov.ua/Review/93542041?fbclid=IwAR3jxE53dVyLUD1lhPaN08HS-REq2M_pTYeX_WZ-kqzmEF16-bhnDAi-bNs.

172. Постанова Верховного Суду від 30 верес. 2021 р. у справі № 556/450/18. URL: https://reyestr.court.gov.ua/Review/100109396.

173. Постанова Верховного Суду від 6 жовт. 2021 р. у справі № 756/11581/15-к. URL: https://verdictum.ligazakon.net/document/100214768?utm_source=jurliga.ligazakon.net&utm_medium=news&utm_content=jl01.

174. ПриватБанк виявив небезпечний фішинговий сайт. URL: https://finclub.net/ua/news/privatbank-viyaviv-nebezpechnij-fishingovij-sajt.html.

175. Про авторське право і суміжні права : Закон України від 1 груд. 2022 р. № 211-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

176. Про віртуальні активи : Закон України від 17 лют. 2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text_.

177. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15 берез. 2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

178. Про електронні довірчі послуги : Закон України від 5 жовт. 2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

179. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

180. Про електронні комунікації : Закон України від 16 груд. 2022 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

181. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора :* [сайт]. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

182. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушення, їх виявленні та розслідуванні : наказ МВС України від 7 лип. 2017 р. № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

183. Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України : наказ МВС України від 7 лип. 2017 р. № 591. URL: https://zakon.rada.gov.ua/laws/show/z1024-17#Text.

184. Про затвердження 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 : наказ МВС України від 3 листоп. 2015 р. № 1339. URL: https://zakon.rada.gov.ua/laws/show/z1392-15.

185. Про затвердження Інструкції про участь співробітників та працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України як спеціалістів в кримінальному провадженні : наказ Служби безпеки України від 19 берез. 2016 р. № 138. URL: https://zakon.rada.gov.ua/laws/show/z0564-16.

186. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : постанова Кабінету Міністрів України від 29 квіт. 2015 р. № 266. URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#Text.

187. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : наказ Офісу Генерального

прокурора від 30 черв. 2020 р. № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text.

188. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

189. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

190. Про національну програму інформатизації : Закон України від 4 лют. 1998 р. № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

191. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

192. Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ Генеральної прокуратури України, МВС України, СБУ, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.

193. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

194. Про основні засади забезпечення кібербезпеки України : проект Закону України від 19 черв. 2015 р. № 2126а. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

195. Про правовий режим воєнного стану : Закон України від 12 трав. 2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.

196. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

197. Про рішення Ради національної безпеки і оборони України від 10 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» : Указ

Президента України від 1 лют. 2022 р. № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289.

198. Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.

199. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n8.

200. Проведення допиту/опитування дитини в умовах збройного конфлікту та/або воєнного стану : метод. рек. Київ, 2022. 64 с.

201. Пройдаков Е. М., Теплицький Л. А. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування. Вид. 1-ше. Київ : СофтПрес, 2005. 546 с.

202. Протидія злочинам у сфері використання інформаційних технологій : інтегр. навч.-практ. посіб. / за ред. М. В. Карчевського. Харків : Право, 2019. 188 с.

203. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. Київ : Скіф, 2012. 728 с.

204. Пчеліна О. В. Криміналістична класифікація злочинів. *Право і суспільство.* 2014. № 6–1. Ч. 2. С. 304–309.

205. Пчеліна О. В. Тактичні завдання розслідування злочинів у сфері службової діяльності. *Актуальні проблеми вітчизняної юриспруденції.* 2016. № 2. С. 155–158.

206. Пчолкін В. Д. Взаємодія слідчих та працівників оперативних підрозділів у ході розслідування злочинів. *Теорія та практика судової експертизи і криміналістики.* 2009. Вип. 9. С. 97–103.

207. Рішення ЄСПЛ «Бєлоусов проти України» (заява № 4494/07) від 7 листоп. 2013 р. URL: https://zakon.rada.gov.ua/laws/show/974_989#n51.

208. Рішення ЄСПЛ «Вергельський проти України» (заява № 19312/06) від 12 берез. 2009 р. URL:

https://zakon.rada.gov.ua/laws/show/974_460?find=1&text=7+%D1%82%D1%80%D0%B0%D0%B2%D0%BD%D1%8F+2007#w2_4.

209. Рішення ЄСПЛ «Матанович проти Хорватії» (заява № 2742/12) від 4 квіт. 2017 р. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-172466%22]}.

210. Розслідування окремих видів злочинів : навч. посіб. / за ред. М. А. Погорецького, Д. Б. Сергєєвої. Київ : Алерта, 2015. 536 с.

211. Руденко О. Г., Бодянський Є. В. Штучній нейронні мережі : навч. посіб. Київ : СМІТ, 2006. 404 с.

212. Салтевский М. В. О структуре криминалистической характеристики хулиганства и типичных следственных ситуациях. *Криминалистика и судебная экспертиза.* 1982. Вып. 25. С. 13–21.

213. Салтевский М. В., Мешков В. М. Криминалистические аспекты установления времени как элемента объективной стороны преступления. *Криминалистика и судебная экспертиза.* 1990. № 40. С. 126.

214. Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2006. 588 с.

215. Салтевський М. В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навч. посіб. Харків : Нац. юрид. акад. України ім. Я. Мудрого, 2000. 35 с.

216. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навч.-метод. посіб. Одеса : Нац. ун-т «Одеська юридична академія», 2020. 112 с.

217. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. Одеса : ТЕС, 2020. 372 с.

218. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09. Харків, 2007. 20 с.

219. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ : КНТ, 2009. 328 с.

220. Самойленко О. А. Природа кіберпросторі як об’єкта криміналістичного дослідження. *Криміналістика і судова експертиза.* 2018. Вип. 63 (1). С. 174–184.

221. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. 226 с.

222. Сергєєва Д. Б. Поняття та види негласних слідчих (розшукових) дій за новим КПК України. *Актуальні питання досудового розслідування слідчими органів внутрішніх справ: проблеми теорії та практики* : матеріали Всеукр. наук.-практ. конф. (Київ, 5 лип. 2013 р.). Київ : Нац. акад. внутр. справ, 2013. 312 с.

223. Сергєєва Д. Б. Судовий контроль за проведенням негласних слідчих (розшукових) дій. *Вісник Харківського національного університету внутрішніх справ* (спеціальний випуск). 2021. № 3. С. 73-78.

224. Синчук В. Л. Кореляційні залежності між елементами криміналістичної характеристики та їх використання у методиці розслідування вбивств : дис. … канд. юрид. наук : 12.00.09. Харків, 2004. 223 с.

225. Сімакова-Єфремян Е. Б. До питання про введення у кримінальне процесуальне законодавство поняття «висновок спеціаліста». *Теорія та практика судової експертизи і криміналістики.* 2019. № 20. С. 110–120.

226. Скарбик П. Нейронні мережі в медицині. URL: https://itechua.com/other/49101.

227. Скригонюк М. І. Криміналістика : підручник. Київ : Атіка, 2005. 496 с.

228. Словник іншомовних слів / уклад. : С. М. Морозов, Л. М. Шкарапута. Київ : Наук. думка, 2000. 680 с.

229. Советская криминалистика. Методика расследования отдельных видов преступлений / под ред. В. К. Лисиченко. Киев : Выща шк., 1988. 405 с.

230. Справа ЄСПЛ «Пічугін проти Росії» від 7 жовт. 2014 р. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-174061%22].

231. Старушкевич А. В. Особа злочинця та потерпілого як елемент криміналістичної характеристики сексуальних убивств : навч. посіб. Київ, 1997. 63 с.

232. Столітній А. В. Електронний висновок експерта в кримінальному провадженні. *Криміналістика і судова експертиза.* 2019. Вип. 64. С. 102–111.

233. Судова статистика. URL: https://court.gov.ua/inshe/sudova_statystyka/.

234. 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 : дис. … канд. юрид. наук : 12.00.09. Київ, 2021. 268 с.

235. Тихомиров Д. О. До проблеми розмежування кіберзлочину і кіберпроступку. *Актуальні проблеми управління інформаційною безпекою держави :* зб. матеріалів наук.-практ. конф. (Київ, 22 берез. 2011 р.) : у 2 ч. Київ : Вид-во НА СБ України, 2011. Ч. 2. С. 75–77..

236. Тлумачний словник з інформатики / [Г. Г. Півняк, Б. С. Бусигін, М. М. Дівізінюк та ін.] ; за заг. ред. Г. Г. Півняка. Дніпропетровськ : Нац. гірнич. ун-т, 2010. 600 с.

237. Туркот М. С., Лазукова О. В. Особливості організації і процесуального керівництва досудовим розслідуванням в умовах дії особливих правових режимів. *Вісник Національної академії прокуратури.* 2019. № 2. С. 44–59. DOI: https://doi.org/10.34285/visnyknapu2019.02.044.

238. Федоренко О. А., Стрільців О. М., Тарасенко О. С. Використання технологій штучного інтелекту у правоохоронній діяльності : аналіт. огляд. Київ, 2022. 106 с.

239. Фейкову «Дію» створив 21-річний: продав її за 100 гривень. URL: https://www.pravda.com.ua/news/2021/10/27/7311820/.

240. Фондова лекція з навчальної дисципліни «Криміналістика». Київ : НАВС, 2016. 47 с. URL: https://www.naiau.kiev.ua/files/kafedru/ksm/taktukaspecznaniy.doc.

241. Хакер з Нідерландів зламав Twitter Трампа. URL: https://www.pravda.com.ua/news/2020/10/22/7270850/.

242. Хакера, який злив GTA 6, упіймали в Лондоні. URL: https://dev.ua/news/gta-6-hacker-1664203309.

243. Хакери зламали сайти українських міністерств та залишили повідомлення про злив даних. URL: https://imi.org.ua/news/hakery-zlamaly-sajty-ukrayinskyh-ministerstv-ta-zalyshyly-povidomlennya-pro-zlyv-danyh-i43309.

244. Хахановський В. Г., Гавловський В. Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право.* 2020. № 2. С. 99–109. URL: http://nbuv.gov.ua/UJRN/Infpr_2020_2_11.

245. Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2019. № 1. С. 13–19. URL: http://nbuv.gov.ua/UJRN/krvis_2019_1_4.

246. Ходченко І. Л. Теоретичні аспекти судової мистецтвознавчої експертизи. *Криміналістика і судова експертиза.* 2017. Вип. 62. С. 460–465.

247. Цимбал П., Бондик В., Омельчук Л. Взаємодія слідчого та спеціаліста при розслідуванні злочинів, пов'язаних із неналежним виконанням професійних обов'язків медичними працівниками. *Підприємництво, господарство і право.* 2012. № 11 (203). С. 134–137.

248. Цуцкірідзе М. С. Проблемні питання досудового розслідування в зоні проведення антитерористичної операції. *Особливості процесуального доказування у кримінальних провадженнях про злочини, вчинені на тимчасово окупованих територіях :* матеріали круглого столу (Київ, 26 лип. 2016 р.). Київ : Нац. акад. прокуратури України, 2016. С. 148–149.

249. Черненко А. П., Шиян А. Г. Висновок спеціаліста як процесуальне джерело доказів у кримінальному провадженні. *Актуальні проблеми експертного забезпечення досудового розслідування :* матеріали наук.-практ. семінару (Дніпро, 29 трав. 2020 р.). Дніпро : ДДУВС, 2020. С. 149–152.

250. Черняк Н. П., Гаркуша А. Г. Процесуальні особливості проведення допиту та пред'явлення для впізнання в режимі відеоконференції за законодавством України. *Jurnalul juridic national: teorie şi practică.* 2016. № 5. С. 199–203.

251. Чигрина Г. Л. Електронні документи: залучення спеціаліста до збирання та використання під час кримінального провадження. *Jurnalul Juridic naţional: Teorie şi Practică*. 2017. № 3. С. 134–137.

252. Шапошнікова І. Основні аспекти вибору типу і проведення експертизи у справах про кіберзлочинність. URL: https://yur-gazeta.com/publications/practice/inshe/osnovni-aspekti-viboru-tipu-i-provedennya-ekspertizi-u-spravah-pro-kiberzlochinnist.html.

253. Шевчук В. М. Криміналістика: традиції, новації, перспективи : добірка наук. пр. / упоряд. Н. А. Чмутова. Харків : Право, 2020. 1280 с.

254. Штучний інтелект, машинне навчання та нейронні мережі. URL: https://evergreens.com.ua/ua/articles/machine-learning-overview.html.

255. Штучні нейронні мережі. Короткі теоретичні відомості. URL: https://learn.ztu.edu.ua/mod/resource/view.php?id=17833.

256. Щербаковський М. Г. Розслідування комп'ютерних злочинів : посібник. Харків : Харків. нац. ун-т внутр. справ, 2010. 112 с.

257. Щербаковський, М. Г. Консультаційна функція спеціаліста у кримінальному провадженні. *Криміналістика і судова експертиза*. 2017. Вип. 62. С. 43–51.

258. Щиголь О.В., Кучинська О.П. Окремі проблеми процесуального статусу потерпілого в кримінальному провадженні. *Вісник кримінального судочинства.* 2019. № 1. С. 18-25.

259. Що таке фішинг і як від нього захиститися. URL: https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html.

260. Щур Б. В. Криміналістична класифікація злочинів: співвідношення із суміжними поняттями. *Науковий вісник Львівського державного університету внутрішніх справ.* 2010. № 2. С. 337–344.

261. Юдкова К. В. Особливості визначення поняття «інформаційні технології». *Інформація і право.* 2015. № 1 (13). С. 63–67.

262. Юный хакер создал опасный троян. URL: https://senior.ua/news/yunyy-haker-sozdal-opasnyy-troyan.

263. 18 USC ch. 47: FRAUD AND FALSE STATEMENT. URL: https://uscode.house.gov/view.xhtml;jsessionid=81EAFEE43F266018EF6D1D74A0A0BAB0?req=granuleid%3AUSC-prelim-title18-chapter47&saved=%7CKHRpdGxlOjE4IHNlY3Rpb246MTAzMCBlZGl0aW9uOnByZWxpbSk%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim.

264. Adli istatistikler 2021. ANKARA HİZMETE ÖZEL. URL: https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022140538 2021H%C4%B0ZMETE%C3%96ZELK%C4%B0TAP.pdf.

265. AlphaZero again beat Stocfist in a match of 1000 games. URL: https://sudonull.com/post/7278-AlphaZero-again-beat-Stockfish-in-a-match-of-1000.

266. BRIGADA CENTRAL DE INVESTIGACIÓN TECNOLÓGICA (B.C.I.T.). URL: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#.

267. Bundesgesetzblatt. Ausgegeben zu Bonn am 23. Mai 1986 Nr. 21. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl186s0721.pdf.

268. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Academic Press, 2011. 807 p. URL: https://www.perlego.com/book/1813633/digital-evidence-and-computer-crime-forensic-science-computers-and-the-internet-pdf.

269. CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI. URL: https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html.

270. Chatterjee M. Data Science vs Machine Learning and Artificial Intelligence. URL: https://www.mygreatlearning.com/blog/difference-data-science-machine-learning-ai/.

271. China’s AI-Enabled ‘Smart Courts’ To Recommend Laws & Draft Legal Docs; Judges To Take Consult AI Before Verdict. URL: https://eurasiantimes.com/chinas-ai-enabled-smart-court-to-recommendlaws-judges/.

272. Code pénal. Version en vigueur au 25 avril 2022. URL: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070719/.

273. Compas (software). URL: https://en.wikipedia.org/wiki/COMPAS_(software).

274. Computer Misuse Act 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/1991-02-01.

275. Consultation. Oxford Learner's Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/english/consultation?q=consultation.

276. Criminal investigation Department. URL: https://www.police.gov.sg/Who-We-Are/Organisation-Structure/Specialist-Staff-Departments/Criminal-Investigation-Department.

277. Criminal Procedure Code 2010. URL: https://sso.agc.gov.sg/Act/CPC2010?ProvIds=P14-#top.

278. Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors / by A. Reyes, R. Brittson, K. O'Shea, J. Steele. Rockland, MA : Syngress Pub, 2007. 412 p.

279. Cybercrime. URL: https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html.

280. DoS-атака. *Вікіпедія :* [сайт]. URL: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0.

281. European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

282. European Patent Application. URL: https://www.musicbusinessworldwide.com/files/2020/11/1_merged.pdf.

283. Federal Bureau of Investigation Internet Crime Report 2021. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

284. Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG). URL: https://www.buzer.de/BKAG_Bundeskriminalamtgesetz.htm.

285. How the Dutch police are using AI to unravel cold cases. May 23, 2018. URL: https://thenextweb.com/news/how-the-dutch-police-is-using-ai-to-unravel-cold-cases.

286. Informe sobre la cibercriminalidad en España. URL: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf.

287. Kalat D. Nervous System #1: The Thief and the Scientist *The Story of the First White Hat Hacker.* Legaltech News, February 5. 2018. URL: https://media.thinkbrg.com/wp-content/uploads/2021/03/19180241/01_The-Thief-and-the-Scientist_Feb2018.pdf.

288. Kaplina O. V., Kuchynska O. P., Krukevych O. M. Interrogation of minor and juvenile witnesses in criminal proceedings. *Current state and prospects for improvement. Journal of National Academy of Legal Sciences of Ukraine*. 2021. № 28 (3). P. 268–276. DOI: 10.37635/jnalsu.28(3).2021.268-276.

289. Kuchynska O., Tsyganyuk Y., Shulgin S. Consideration of state of human health during applying restrictive measures. *Wiadomosci Lekarskie.* 2021. Vol. LXXIV, Issue 12. P. 3031–3035.

290. Kuzminas v. Russian, 21 December 2021 No. 69810/11. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-214203%22]}.

291. Leavitt H. J., Whisher Th. L. Management in the 1980's. *Harvard Business Review* (November 1958). URL: https://hbr.org/1958/11/management-in-the-1980s.

292. Les statistiques policières de criminalité pour l'année 2021 sont en ligne! URL: https://www.police.be/5998/fr/actualites/les-statistiques-policieres-de-criminalite-pour-lannee-2021-sont-en-ligne#:~:text=La%20cybercriminalit%C3%A9%20poursuit%20son%20ascension&text

=2021%20n'a%20pas%20d%C3%A9rog%C3%A9,9%20%25%20par%20rapport%20%C3%A0%202020.

293. Machine Learning, ML. URL: https://www.it.ua/knowledge-base/technology-innovation/machine-learning.

294. Manzhai O., Kuryliuk Yu., Miroshnykov I., Syiploki M., Vazhynskyi V. Criminal and legal protection of information relations. International Journal of Computer Science and Network Security. 2022. Vol. 22 No. 5. P. 284–288.

295. McCulloch W. S., Pitts W. A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysic.* 1943. № 5. P. 115–133. DOI: https://doi.org/10.1007/BF02478259.

296. Merative, formerly IBM Watson Health. URL: https://en.wikipedia.org/wiki/IBM_Watson_Health.

297. Miroshnykov I., Karpenko M., Chernychenko I., Vazhynskyi V., Litvin Yu. Use Of Scientific And Technical Means During Interrogation In Criminal Proceedings. *International Journal of Computer Science and Network Security.* 2022. Vol. 22. No. 9. P. 515–520. DOI: https://doi.org/10.22937/IJCSNS.2022.22.9.66.

298. Montalbano E. Massive DDoS Attack Disrupts Belgium Parliament (May 6, 2021). URL: https://threatpost.com/ddos-disrupts-belgium/165911/.

299. Nedilko Ya. Tactical Features of Conducting a Search in the Investigation of Cybercrimes. *European Reforms Bulletin.* 2021. № 3. С. 73–77. URL: http://aord.com.ua/wp-content/uploads/2021/11/European-Reforms-Bulletin_3_2021-2.pdf.

300. Nedilko Y. Typical investigative situations at the initial stage of cybercrime investigation. *Актуальні питання розвитку юридичної науки та практики :* матеріали Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених, присвяч. Дню науки Інституту права (Київ, 21 трав. 2021 р.) : у 2 т. Київ, 2021. Т. 2. С. 345.

301. Oxford Learner's Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/english/computer?q=computer.

302. Phillips K., Davidson J. C., Farr R. R., Burkhardt C., Caneppele S., Aiken M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sci.* 2022. No. 2. P. 379–398. DOI: https://doi.org/10.3390/forensicsci2020028.

303. PKS 2021 Länder – Falltabellen. URL: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/LandFalltabellen/landFalltabellen.html?nn=194190.

304. Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investig.* 2022. Vol. 11. Issue 53. P. 259–269. DOI: https://doi.org/10.34069/AI/2022.53.05.26.

305. Police Nationale. URL: https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite.

306. Pratik R. Artificial Intelligence: A Rising Star of Mobile Technology. URL: https://www.intuz.com/blog/artificial-intelligence-a-rising-star-of-mobile-technology.

307. Reference Incident Classification Taxonomy. URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

308. Report: 267 million Facebook users IDs and phone numbers exposed online (UPDATE: now 309 million). URL: https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/.

309. Royal Canadian Mounted Police Cybercrime Strategy. URL: https://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-cybercrime-strategy.

310. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab.

311. Siber suçlardan elde edilen gelirlere ilişkin soruşturmalarda kuruluşlararası ve uluslararası işbirliği Protokolleri hakkında genel kılavuz. URL: https://rm.coe.int/3156-25-guide-interagency-international-cooperationprotocolturkey-tr/16807be2e3.

312. SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI. URL: https://www.egm.gov.tr/siber/hakkimizda2.

313. Spotify. URL: https://uk.wikipedia.org/wiki/Spotify.

314. Stetsyk B., Vakulyk O., Serhieieva D., Luchko O., Makarov M. Normative content of the principle of immediacy of research of testimonies, things and documents during criminal procedural evidence. *Cuestiones Políticas.* 2022. Vol. 40. № 72. P. 108–124. DOI: https://doi.org/10.46398/cuestpol.4072.06.

315. Sur Internet, nul n'est à l'abri d'une action malveillante ou de messages non sollicités. URL: https://www.ssi.gouv.fr/en-cas-dincident/.

316. SWEDEN. Data Act of 11 May 1973. URL: https://resources.law.cam.ac.uk/cipil/documents/Historic/Sweden%20Data%20Act%20 1973%20-%20Historic.pdf.

317. Tonry M. The Oxford Handbook of Crime and Public Policy Oxford Handbooks. Oxford Universaty Press, 2009. 640 p.

318. Turkey using AI software ASENA in fight against drugs. URL: https://www.hurriyetdailynews.com/turkey-using-ai-software-asena-in-fight-against-drugs-173912.

319. Tymchyshyn O., Semeniaka A., Bondar S., Akhtyrska N., Kostiuchenko A. The use of big data and data mining in the investigation of criminal offences. *Amazonia Investiga.* 2022. Vol. 11. Issue 56. P. 278–290. DOI: https://doi.org/10.34069/AI/2022.56.08.27.

320. Ustawa o Policji z dnia 6 kwietnia 1990 r. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19900300179/U/D19900179Lj.pdf.

321. Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210002447/T/D20212447L.pdf.

322. Ustawa z dnia 6 czerwca 1997 r. Kodeks postepowania karnego. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970890555/U/D19970555Lj.pdf.

323. Winmill B., Metcalf D., Band M. Cybercrime: issues and challenges in the United States. *Digital Evidence and Elecronic Signature Law Review.* 2010. Vol. 7. P. 19–34. DOI: https://doi.org/10.14296/deeslr.v7i0.1921/.

ДОДАТКИ

ДОДАТОК 1

Зауваження та пропозиції
кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка
стосовно проекту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо уточнення окремих положень з метою забезпечення захисту прав учасників кримінального провадження» №9211 від 17.04.2023 р.

Як вбачається з пояснювальної записки до проекту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо уточнення окремих положень з метою забезпечення захисту прав учасників кримінального провадження» №9211 від 17.04.2023 р. його прийняття має на меті зниження тиску та втручання правоохоронних органів у здійснення господарської діяльності, зокрема високотехнологічних компаній, а також стимулювання розвитку цифрової економіки та у середньостроковій перспективі покращення інвестиційного клімату в Україні.

Розробка та прийняття даного Законопроекту №9211 від 17.04.2023 р. є доцільною та своєчасною. В основному новели, запропоновані у Законопроекті, слід підтримати. Разом з тим вважаємо необхідне висловити деякі зауваження та пропозиції:

1) Статтю 3 КПК України запропоновано доповнити новим пунктом 13-1) наступного змісту: *«пристрої для обробки, передавання та зберігання інформації в електронному вигляді або їх складові – будь-яке обладнання та його складові, призначене для зберігання, обробки та передавання інформації в електронному вигляді за допомогою апаратних і програмних засобів. Цим поняттям, зокрема, охоплюються: інформаційні (автоматизовані, інформаційно-комунікаційні) системи; комп'ютери (суперкомп'ютери, мейнфрейми, кластери, сервери, робочі станції, персональні комп'ютери, ноутбуки тощо); комп'ютерна периферія (зокрема, термінали, принтери, сканери, плотери, джерела безперебійного живлення); мобільні термінали систем зв'язку (мобільні телефони, смартфони, планшети та інше); технічні засоби електронних комунікацій, мережеве обладнання (маршрутизатори, концентратори, комутатори, модеми, мережеві контролери тощо); мікропроцесорні системи (наприклад, мікроконтролери та*

програмовані логічні контролери), а також банкомати й інші стаціонарні платіжні термінали для обслуговування населення».

Слід зазначити, що у статті 3 КПК України наводиться загальний перелік основних термінів. Частина 3 зазначеної статті констатує, що інші терміни в КПК визначаються спеціальними нормами Кримінального процесуального кодексу або іншими Законами. Тому, на наш погляд, у пункті 13-1 статті 3 КПК України не зовсім доречно наводити такий широкий перелік засобів (пристроїв), оскільки цей перелік буде постійно доповнюватися новими гаджетами, що потребуватиме від законодавця постійного внесення змін до їх переліку. крім того частина з них взагалі не є пристроями для збереження інформації. Відповідно пропонуємо закріпити наведене визначення не пунктом 13-1) законопроекту, а у статті 2 Закону України «Про електронні комунікації».

2) **У Кримінальному процесуальному кодексі України вважаємо за доцільне використовувати загальне поняття «інформаційні комп'ютерні технології – електронні пристрої, де є поєднання програмних та апаратних засобів, що здійснюють зберігання, обробку та передавання інформації в цифровому вигляді».**
3) З метою удосконалення окремих положень Кримінального процесуального законодавства України, що стосуються правового врегулювання електронних доказів у кримінальному провадженні, необхідно враховувати міжнародні нормативні акти, зокрема Другий додатковий протокол до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів. Потрібно зазначити, що для забезпечення відповідності міжнародним стандартам процедури збору доказів у кримінальному провадженні, **доцільно ухвалити Закон України про ратифікацію Другого додаткового протоколу до Конвенції про кіберзлочинність.** Другий додатковий протокол був підписаний Україною 30 листопада 2022 року. Крім того, для адаптації вітчизняного законодавства до законодавства Європейського Союзу у Кримінальному процесуальному кодексі України доцільно було б передбачити окремі положення, які стосувалися особливостей визначення, збирання та зберігання електронних доказів у кримінальному провадженні.
4) Законодавцю доцільно окремо забезпечити засоби охорони адвокатської таємниці у випадку проведення обшуку у адвоката та під час вилучення

його пристроїв, відповідно до практики ЄСПЛ у рішеннях "Юдицька та інші проти РФ", "Колесниченко проти РФ".

5) Окремо треба зазначити про особливості вилучення комп'ютерної техніки під час розслідування кримінальних проваджень щодо тероризму (рішення ЄСПЛ "Шер та інші проти Сполученого Королівства"). Врахувати відповідні положення Контртерористичної стратегії Ради Міністрів ЄС від 8 лютого 2023 року).

Зауваження та пропозиції висловлені завідуючою кафедри кримінального процесу та криміналістики, к.ю.н., доцентом Костюченко О.Ю., доцентом кафедри, к.ю.н., доцентом Ахтирською Н.М. та асистентом кафедри Неділком Я.В.

Завідуюча кафедрою
кримінального процесу та криміналістики
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
к.ю.н., доцент Олена КОСТЮЧЕНКО

ДОДАТОК 2

№ з/п	Питання	Прокурори
1	2	3
1.	**Який у Вас досвід роботи в органах прокуратури?**	
	А) до одного року	109
	Б) від 1 до 3 років	17
	В) від 3 до 5 років	4
	Г) більше 5 років	70
2.	**Чи здійснювалось Вами процесуальне керівництво у кримінальних провадженнях щодо кримінальних правопорушень у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ XVI КК України)?**	
	А) так	54
	Б) ні	146
3.	**Чи доводилось Вам особисто проводити слідчі (розшукові) дії у зазначених кримінальних провадженнях?**	
	А) так	39
	Б) ні	161
4.	**На Вашу думку, чи необхідно обов'язково залучати спеціаліста для участі у проведенні огляду, обшуку та допиту при розслідуванні кримінальних правопорушень зазначеної категорії?**	
	А) так	174
	Б) не обов'язково	14
	В) важко відповісти	12
5.	**Чи обов'язково слідчим повинен складатися письмовий план при розслідуванні зазначених кримінальних правопорушень?**	
	А) так	120
	Б) ні	48

	В) важко відповісти	32
6.	**Як Ви ставитесь, щоб план розслідування зазначених кримінальних правопорушень складала спеціальна "комп'ютерна програма" чи "нейронна мережа" (використання штучного інтелекту в розслідуванні кримінальних правопорушень)?**	
	А) позитивно	105
	Б) негативно	42
	В) важко відповісти	53
7.	**На Вашу думку, що негативно впливає на результати ефективного досудового розслідування та здійснення процесуального керівництва у кримінальних провадженнях цієї категорії (можете обрати декілька відповідей)?**	
	А) недостатній фаховий рівень слідчих	127
	Б) відсутність необхідних сучасних методичних розробок	123
	В) недосконаліть чинного законодавства	70
	Г) нехтування залученням спеціаліста та використанням його консультацій, пояснень, довідок та висновків	110
	Ґ) слабке програмне забезпечення новітніми технологіями	
8.	**Що необхідно здійснити для підвищення ефективності розслідування зазначених кримінальних правопорушень (можете обрати декілька відповідей)?**	
	А) вдосконалити чинне законодавство	81
	Б) постійно підвищувати рівень професійної підготовки слідчих, прокурорів шляхом проведення тренінгів, семінарів тощо	162
	В) подальша розробка методики щодо особливостей розслідування зазначених кримінальних правопорушень	164

ДОДАТОК 3

ЗАТВЕРДЖУЮ
Директор
Тренінгового центру прокурорів України
доктор юридичних наук, професор

Олеся ОТРАДНОВА

«26» квітня 2023 року

АКТ
про впровадження результатів дисертаційного дослідження аспіранта кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Неділька Ярослава Валентиновича на тему: «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» у навчальний процес Тренінгового центру прокурорів України

Комісія у складі: заступника директора Тренінгового центру прокурорів України, доктора юридичних наук, доцента Орлеана Андрія Михайловича; начальника відділу організації підготовки кадрів прокуратури, кандидата юридичних наук, доцента Лісової Нелі Валеріївни та експерта аналітичного відділу підготовки прокурорів Пилипенка Ігоря Вікторовича склала цей акт про те, що матеріали дисертації Неділька Ярослава Валентиновича «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» можуть бути використані у професійній діяльності прокурорів під час здійснення процесуального керівництва щодо кримінальних правопорушень даної категорії, а також під час проведення тренінгів та тренінгових курсів для прокурорів та інших працівників правоохоронних органів.

Результати дисертаційного дослідження знайшли своє відображення в багатьох довідкових та інших матеріалах для практичних працівників, серед яких рекомендованими є такі публікації та розробки:

1. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

2. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–175. URL: http://www.lsej.org.ua/1_2019/47.pdf.

3. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf.

4. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*: Збірник наукових праць. Юридичні і політичні науки. Випуск 88. 2020. С. 202–211.

5. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Криміналістика і судова експертиза*. Вип. 66. 2021. С. 453–460. URL : http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf.

6. Nedilko Ya. Tactical Features of Conducting a Search in the Investigation of Cybercrimes. *European Reforms Bulletin № 3 2021. С. 73-77. URL:* http://aord.com.ua/wp-content/uploads/2021/11/European-Reforms-Bulletin_3_2021-2.pdf.

7. Неділько Я.В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). *Knowledge, Education, Law, Management 2021 № 8 (44) vol. 2 С. 119-124*. ISSN 2353-8406. DOI https://doi.org/10.51647/kelm.2021.8.2.19

8. Неділько Я.В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза. Випуск 67. С.292-301*

Голова комісії: **Андрій ОРЛЕАН**

Члени комісії: **Неля ЛІСОВА**

Ігор ПИЛИПЕНКО

ЗАТВЕРДЖУЮ
Декан факультету правничих наук,
кандидат юридичних наук, доцент
Цельєв О. В.
«19» квітня 2023 року

АКТ ВПРОВАДЖЕННЯ

результатів дисертаційного дослідження Неділька Ярослава Валентиновича в освітній процес факультету правничих наук Національного університету «Києво-Могилянська академія»

Комісія кафедри кримінального та кримінального процесуального права у складі: завідувача кафедри, доктора юридичних наук, професора Галагана Володимира Івановича, доцента кафедри, доктора юридичних наук, доцента Удовенко Жанни Володимирівни та доцента кафедри, кандидата юридичних наук, доцента Шкелебей Вікторії Анатоліївни, розглянула матеріали дисертації аспіранта кафедри кримінального процесу та криміналістики Навчально-наукового інститут права Київського національного університету імені Тараса Шевченка Неділька Ярослава Валентиновича на тему «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій».

Комісія дійшла до висновку, що зазначені матеріали можуть використовуватися у освітньому процесі факультету правничих наук Національного університету «Києво-Могилянська академія» під час викладання курсів «Кримінальне процесуальне право», «Криміналістика», «Використання криміналістичної техніки у кримінальному провадженні», «Складання процесуальних документів на досудовому розслідуванні». З цією метою студентам рекомендуються для використання під час підготовки до занять наступні оприлюднені наукові праці:

1. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

2. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–175. URL: http://www.lsej.org.ua/1_2019/47.pdf.

3. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf.

4. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*: Збірник наукових праць. Юридичні і політичні науки. Випуск 88. 2020. С. 202–211. URL: https://derzhava-i-pravo.com.ua/files/issues/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B0%20%D1%96%20%D0%BF%D1%80%D0%B0%D0%B2%D0%BE.%20%D0%92%D0%B8%D0%BF%D1%83%D1%81%D0%BA%2088.pdf.

5. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Криміналістика і судова експертиза*. Вип. 66. 2021. С. 453–460. URL : http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf.

6. Неділько Я. В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). *Knowledge, Education, Law, Management*. 2021. № 8 (44). Vol. 2. С. 119–124. URL : https://doi.org/10.51647/kelm.2021.8.2.19.

7. Неділько Я. В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза*. Вип. 67. 2022. С. 292–301. URL : https://doi.org/10.33994/kndise.2022.67.30.

Члени комісії:

доктор юридичних наук, професор В. І. Галаган

доктор юридичних наук, доцент Ж. В. Удовенко

кандидат юридичних наук, доцент В. А. Шкелебей

Особистий підпис ЗАСВІДЧУЮ Начальник ВК Відділ кадрів

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

вул. Богомольця, 10, м. Київ, 01601,
тел. 254-93-33, info@police.gov.ua
Ідентифікаційний код 40108578

_____ № _____

На № _____ від _____

Про склад комісії

АКТ
про впровадження результатів дисертаційного дослідження Неділька Ярослава Валентиновича на тему: «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» у практичну діяльність

Комісія у складі: ***першого заступника Голови Національної поліції України - начальник кримінальної поліції Михайла КУЗНЄЦОВА, начальника Департаменту оперативно-технічних заходів Національної поліції України Валентина КОПАЄВА та начальника Департаменту кіберполіції Національної поліції України Юрія ВИХОДЦЯ*** 07.04.2023 склали цей акт про те, що висновки та пропозиції щодо виявлення та фіксації доказів під час розслідування зазначеної категорії кримінальних правопорушень, сформовані у дисертаційному дослідженні Неділька Ярослава Валентиновича, є доцільними і підлягають практичному застосуванню. Висловлені рекомендації стосовно організації та проведення досудового розслідування тільки посилять боротьбу із кримінальними правопорушеннями зазначеної категорії і сприятимуть їх ефективному розслідуванню.

Окрім цього, результати дисертаційного дослідження висвітлені у ряді публікацій, серед яких у системі проведення службової підготовки можуть бути рекомендовані:

1. Неділько Я.В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України 4`2018.* С. 49-60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf

2. Ахтирська Н.М., Неділько Я.В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал.* С. 171-175. URL: http://www.lsej.org.ua/1_2019/47.pdf

3. Неділько Я.В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємство, господарство і право. 7/2020.* URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf

4. Неділько Я.В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право:* Збірник наукових праць. Юридичні і політичні науки. Випуск 88 / Ін-т держави і права імені В. М. Корецького НАН України. Київ: Вид-во «Юридична думка», 2020. 346 с. С. 202

5. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Міжвідомчий науково-методичний збірник «Криміналістика і судова експертиза» 2021.* С. 453-460. DOI: https://doi.org/10.33994/kndise.2021.66.43 URL: http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf

6. Nedilko Ya. Tactical Features of Conducting a Search in the Investigation of Cybercrimes. *European Reforms Bulletin № 3 2021. С. 73-77. URL: http://aord.com.ua/wp-content/uploads/2021/11/European-Reforms-Bulletin_3_2021-2.pdf*

7. Неділько Я.В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). *Knowledge, Education, Law, Management 2021 № 8 (44) vol. 2 С. 119-124.* ISSN 2353-8406. DOI https://doi.org/10.51647/kelm.2021.8.2.19

8. Неділько Я.В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза. Випуск 67. С.292-301*

Голова комісії:

Перший заступник Голови –
начальник кримінальної поліції
кандидат юридичних наук **Михайло КУЗНЄЦОВ**

Члени комісії:

Начальник Департаменту
оперативно-технічних заходів
кандидат юридичних наук **Валентин КОПАЄВ**

Начальник Департаменту кіберполіції
доктор філософії в галузі права **Юрій ВИХОДЕЦЬ**

«ЗАТВЕРДЖУЮ»
Перший проректор
Запорізького національного університету,
доктор юридичних наук, професор
Олександр БОНДАР
«01» травня 2023 р.

АКТ
про впровадження

результатів дисертаційного дослідження аспіранта кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Неділько Ярослава Валентиновича «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» в навчальний процес кафедри кримінального права та правоохоронної діяльності юридичного факультету Запорізького національного університету

Комісія у складі: в.о. завідувача кафедри кримінального права та правоохоронної діяльності, кандидата юридичних наук, доцента Ларкіна М.О. (голова комісії), доцента кафедри кримінального права та правоохоронної діяльності, кандидата юридичних наук, доцента Войтовича Є.М. та доцента кафедри кримінального права та правоохоронної діяльності, кандидата юридичних наук Шалдирвана П.В. склала цей акт про те, що результати дисертаційного дослідження аспіранта кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка Неділько Я.В. «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» використовуються в навчальному процесі кафедри кримінального права та правоохоронної діяльності при проведенні лекційних та семінарських занять для здобувачів денної та заочної форм навчання з навчальних дисциплін: «Криміналістика», «Кримінальне право», «Кримінальний процес», спецкурсів, а також при проведенні наукових семінарів, конференцій, круглих столів.

Результати наукового дослідження знайшли своє відображення в навчально-методичних матеріалах для студентів, де, як джерела рекомендовані наступні публікації:

1. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

2. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–175. URL: http://www.lsej.org.ua/1_2019/47.pdf.

3. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf.

4. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*: Збірник наукових праць. Юридичні і політичні науки. Випуск 88. 2020. С. 202–211.

5. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Криміналістика і судова експертиза*. Вип. 66. 2021. С. 453–460. URL : http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf.

6. Nedilko Ya. Tactical Features of Conducting a Search in the Investigation of Cybercrimes. *European Reforms Bulletin № 3 2021. С. 73-77.* URL: http://aord.com.ua/wp-content/uploads/2021/11/European-Reforms-Bulletin_3_2021-2.pdf.

7. Неділько Я. В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів). *Knowledge, Education, Law, Management*. 2021. № 8 (44). Vol. 2 С. 119–124. URL : https://doi.org/10.51647/kelm.2021.8.2.19.

8. Неділько Я. В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза*. Вип. 67. 2022. С. 292–301. DOI: https://doi.org/10.33994/kndise.2022.67.30.

Голова комісії: Михайло ЛАРКІН

Члени комісії: Євген ВОЙТОВИЧ

Павло ШАЛДИРВАН

ВЕРХОВНИЙ СУД
КАСАЦІЙНИЙ КРИМІНАЛЬНИЙ СУД
вул. П. Орлика, 4а, м. Київ, 01043, код ЄДРПОУ 41721784

03 травня 2023 р.

АКТ ВПРОВАДЖЕННЯ

Комісія у складі: заступника керівника апарату – керівника секретаріату Касаційного кримінального суду у складі Верховного Суду Хім'яка Ю.Б., керівника департаменту аналітичної та правової роботи Верховного Суду Бабанли Р.Ш., начальника відділу аналітичної та правової роботи Касаційного кримінального суду управління аналітичної допомоги касаційним судам та Великій Палаті Верховного Суду департаменту аналітичної та правової роботи апарату Верховного Суду Загиней-Заболотенко З.А. склала цей акт про те, що комісією розглянуто окремі результати дисертаційного дослідження аспіранта кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка – Неділька Ярослава Валентиновича на здобуття наукового ступеня доктора філософії права на тему: «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій».

Комісія вважає, що отримані в результаті зазначеного дисертаційного дослідження наукові результати, що стосуються проблемних питань протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних комп'ютерних технологій, є доцільними та належним чином обґрунтованими і можуть бути враховані під час здійснення Касаційним кримінальним судом у складі Верховного Суду своїх повноважень, зокрема в частині вивчення судової практики в порядку ст. 44 Закону України «Про судоустрій і статус суддів», а також у процесі аналітичної діяльності, яка здійснюється департаментом аналітичної та правової роботи Верховного Суду.

Заступник керівника апарату –
керівник секретаріату Касаційного
кримінального суду у складі Верховного Суду,
кандидат юридичних наук — Ю. Б. Хім'як

Керівник департаменту
аналітичної та правової роботи
Верховного Суду,
доктор юридичних наук — Р. Ш. Бабанли

Начальник відділу аналітичної та правової роботи
Касаційного кримінального суду управління
аналітичної допомоги касаційним судам та Великій Палаті
Верховного Суду департаменту аналітичної та
правової роботи апарату Верховного Суду,
доктор юридичних наук — З. А. Загиней-Заболотенко

ВЕРХОВНИЙ СУД
Касаційний кримінальний суд
216/0/158-23 від 03.05.2023

ДОДАТОК 4

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації:

1. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

2. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–174. URL: http://www.lsej.org.ua/1_2019/47.pdf.

3. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. С. 359– 364. URL: http://pgp-journal.kiev.ua/archive/2020/7/62.pdf.

4. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*. 2020. Вип. 88. С. 202–212. (Серія «Юридичні і політичні науки»).

5. Неділько Я. В. Планування розслідування кіберзлочинів з використанням штучної нейронної мережі. *Криміналістика і судова експертиза*. 2021. Вип. 66. С. 453–460.URL : http://digest.kndise.gov.ua/wp-content/uploads/2021/04/Nedilko.pdf.

6. Неділько Я. В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних технологій (кіберзлочинів), в умовах воєнного стану. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 292–301. DOI: https://doi.org/10.33994/kndise.2022.67.30.

Наукові праці, в яких опубліковані наукові результати дисертації, у зарубіжних спеціальних виданнях:

7. Nedilko Ya. Tactical Features of Conducting a Search in the Investigation of Cybercrimes. *European Reforms Bulletin.* 2021. № 3. С. 73–77. URL:

http://aord.com.ua/wp-content/uploads/2021/11/European-Reforms-Bulletin_3_2021-2.pdf.

8. Неділько Я. В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій. *Knowledge, Education, Law, Management.* 2021. № 8 (44). Vol. 2. С. 119–124. DOI: https://doi.org/10.51647/kelm.2021.8.2.19.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Неділько Я. В. Строки досудового розслідування у контексті змін до кримінального процесуального кодексу України. *Проблеми реформування кримінальної юстиції України* : зб. матеріалів Міжнар. наук.-практ. конф. (Чернівці, 17–18 трав. 2018 р.). С. 198–201.

10. Неділько Я. В. Класифікація особи кіберзлочину як елемента криміналістичної характеристики. *Пріоритетні напрямки розвитку правової системи України* : матеріали Міжнар. наук.-практ. конф. (Львів, 25–26 січ. 2019 р.). С. 112–114.

11. Неділько Я. В. Спосіб вчинення злочину як елемент криміналістичної характеристики кіберзлочинів. *Conceptul de dezvoltare a statului de drept in repiblica Moldova si Ucraina in contextual proceselor de eurointegrare* (Chisinau, 1–2 noiembrie 2019). Chisinau, Republica Moldova, 2019. С. 236–238.

12. Неділько Я. В. Проблемні питання підслідності кіберзлочинів. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці* : матеріали Міжнар. круглого столу (Харків, 12 груд. 2019 р.). Харків, 2019. С. 105–109.

13. Неділько Я. В. Поняття кіберзлочину та особливості його закріплення в національному законодавстві. «*Інтернет речей»: проблеми правового регулювання та впровадження* : матеріали II наук.-практ. конф. (Київ, 29 листоп. 2018 р.). Київ, 2018. С. 112–114.

14. Неділько Я. В. Особливості проведення допиту підозрюваного у кіберзлочинах. *Кримінальний процес та криміналістика: сучасний стан та*

перспективи : тези доп. Всеукр. наук.-практ. конф.(Харків, 26 листоп. 2020 р.). С. 252–255.

15. Неділько Я. В. Основні аспекти використання спеціальних знань під час розслідування кіберзлочинів. *Актуальні питання кримінального права, кримінології та судочинства* : матеріали Всеукр. наук.-практ. конф., присвяч. 165-й річниці з дня народж. проф. Л. С. Білогриць-Котляревського (Київ, 15 трав. 2020 р.). Київ, 2020. С. 85–88.

16. Неділько Я. В. Використання штучної нейронної мережі при плануванні розслідування кіберзлочинів. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали II Міжнар. наук.-практ. інтернет-конф. (Київ, 19 листоп. 2020 р.). Київ, 2020. С. 382–385.

17. Nedilko Y. Typical investigative situations at the initial stage of cybercrime investigation. *Актуальні питання розвитку юридичної науки та практики :* матеріали Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених, присвяч. Дню науки Інституту права (Київ, 21 трав. 2021 р.) : у 2 т. Київ, 2021. Т. 2. С. 345.

18. Неділько Я. В. Особливості проведення огляду під час розслідування кіберзлочинів. *Донецький юридичний інститут МВС України: освітні традиції, перевірені часом* : матеріали Міжнар. наук.-практ. конф. до 60-річчя заснування закладу освіти (Маріуполь, 28 квіт. 2021 р.). Маріуполь, 2021. С. 279–292. URL: http://repo.dli.donetsk.ua/bitstream/123456789/1704/1/210512_1543_A5_442pages_i.pdf.

19. Неділько Я. В, Ахтирська Н. М. Особливості встановлення психологічного контакту слідчого з підозрюваним під час допиту щодо кіберзлочинів. *Актуальні проблеми кримінального процесу та криміналістики :* тези доп. Міжнар. наук.-практ. конф. (Харків, 29 жовт. 2021 р.). Харків, 2021. С. 254–256.

20. Неділько Я. В. Використання штучного інтелекту під час розслідування кіберзлочинів. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України* : матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.). Київ, 2022. С. 275–278.

21. Неділько Я. В. Особливості проведення огляду комп’ютерних даних під час розслідування кіберзлочинів в у мовах воєнного стану. *Актуальні питання розвитку юридичної науки та практики :* матеріали Міжнар. наук.-практ. конф. (Київ, 12 трав. 2022 р.). Київ, 2022. С. 288–290.

22. Неділько Я. В. Процесуальна регламентація надання пояснень спеціалістом під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій. *Використання цифрової інформації в розслідуванні кримінальних правопорушень* : матеріали Міжнар. наук.-практ. круглого столу (Харків, 12 груд. 2022 р.). Харків, 2022. С. 62–65. DOI: https://doi.org/10.31359/978-966-998-460-9.