НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ФІЛІМОНОВ МИКИТА ВОЛОДИМИРОВИЧ

УДК 343.141/143:343:533:004

ДИСЕРТАЦІЯ

ОСОБЛИВОСТІ ДОКАЗУВАННЯ ПРИ ЗДІЙСНЕННІ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

081 – Право

08 – Право

Подається на здобуття ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____М.В. Філімонов

Науковий керівник – **Хижняк Євген Сергійович**,
кандидат юридичних наук, доцент

Одеса – 2026

АНОТАЦІЯ

Філімонов М.В. Особливості доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 – Право (галузь знань 08 – Право). – Національний університет «Одеська юридична академія», Одеса, 2026.

Дисертація є першим у вітчизняній науці кримінального процесу комплексним дослідження теоретичних та практичних проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі на основі положень КПК України 2012 року.

На підставі узагальнення доктринальних напрацювань, автор виокремлює основні напрями дослідження проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі, серед яких: 1) наукові дослідження, присвячені криміналістичним проблемам розслідування кримінальних правопорушень, вчинених у кіберпросторі; 2) наукові дослідження, присвячені криміналістичним проблемам розслідування; окремих категорій кримінальних правопорушень, вчинених у кіберпросторі 3) наукові дослідження, які присвячені питанням використання електронних та цифрових доказів у кримінальному процесуальному доказуванні; 4) наукові дослідження, які присвячені питанням використання спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі; 5) наукові дослідження, присвячені питанням кримінологічного аналізу кіберзлочинності та розробки заходів протидії цьому явищу; 6) наукові дослідження, присвячені питанням міжнародно-правового співробітництва у сфері боротьби зі злочинністю; 7) міждисциплінарні дослідження проблем протидії кіберзлочинності та дослідження протидії кіберзлочинності у межах інших галузей науки.

Уточнено поняття кримінального правопорушення, вчиненого у кіберпросторі, під яким запропоновано розуміти передбачене законом України про кримінальну відповідальність суспільно небезпечне винне діяння, що вчиняється суб'єктом кримінального правопорушення у межах або з використанням кіберпростору як особливого соціально-технічного та інформаційного середовища, шляхом застосування інформаційно-комунікаційних технологій, комп'ютерних систем, мереж чи цифрових даних, та посягає на охоронювані кримінальним законом суспільні відносини.

Здійснено класифікацію кримінальних правопорушень, вчинених у кіберпросторі. Автор пропонує здійснювати класифікацію кримінальних правопорушень, вчинених у кіберпросторі залежно від способу реалізації їх об'єктивної сторони.

За цим критерієм виокремлено виключно кіберпросторові кримінальні правопорушення, які можуть бути вчинені виключно у кіберпросторі та варіативно-кіберпросторові кримінальні правопорушення, об'єктивна сторона яких може бути реалізована як у фізичному середовищі, так і у кіберпросторі.

На підставі узагальнення практики Європейського суду з прав людини виокремлено мінімальні гарантії захисту права на повагу до приватного та сімейного життя у кіберпросторі відповідно до вимог статті 8 Конвенції, до яких віднесено: 1) чітке законодавче визначення категорій осіб та даних, щодо яких можливе перехоплення; 2) наявність попереднього судового контролю або ефективного подальшого нагляду за спостереженням; 3) нормативне формулювання критеріїв, за якими ухвалюється рішення про ініціювання перехоплення; 4) обмеження строків зберігання даних та встановлення чіткого порядку їх знищення.

Досліджено міжнародні стандарти та зарубіжний досвід нормативної регламентації досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. Виокремлено основні міжнародні стандарти розслідування кіберзлочинів у процесуальному аспекті, які є спільними для усіх регіональних систем захисту прав людини є наступні, до яких віднесено:

1) обов’язок держав запровадити чітку правову основу для отримання доступу до інформації, яка зберігається в електронних системах; 2) зобов’язання держав адаптувати компетенцію національних органів і включити до неї переслідування транскордонних злочинів, а також забезпечити можливість здійснення кримінального переслідування, коли правопорушник чи наслідки злочину охоплюють кілька держав-учасниць; 3) здійснення правоохоронними органами пошуку та вилучення виключно у межах конкретного кримінального провадження із забезпеченням оригінальності вилучених даних, цілісності доказів, а також обов’язковим документуванням відповідних правових процедур; 4) забезпечення можливості екстрадиції осіб, які вчинили кіберзлочини; 5) визначення основних видів міжнародно-правової допомоги при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі, серед яких: передача запитів між центральними органами, обмін інформацією, доказами, документами, матеріальними та цифровими даними, у т.ч. без вимоги подвійної криміналізації; 6) забезпечення конфіденційності інформації, отриманої у межах міжнародно-правової допомоги; 7) необхідність санкціонування компетентним органом процесуальних дій, які передбачають втручання у приватне життя осіб.

З’ясовано зміст, поняття та здійснено класифікацію електронних доказів у кримінальному провадженні. Доведено, що електронними (цифровими) доказами є фактичні дані в електронній формі, які отримані в передбаченому КПК України порядку, характеризуються цілісністю, автентичністю та придатністю для дослідження та мають значення для встановлення фактів та обставин кримінального провадження.

Класифікацію електронних (цифрових) доказів запропоновано здійснювати за їх формою, на основі якої виокремлювати електронні документи, електронні повідомлення, віртуальні активи, технічні дані та іншу інформацію в електронній (цифровій) формі.

З’ясовано, що до джерел електронних (цифрових) доказів у ході досудового розслідування кримінальних правопорушень, вчинених у

кіберпросторі, належать: 1) електронні пристрої, які містять значиму для кримінального провадження інформацію; 2) електронні комунікаційні системи, які використовувалися в ході підготовки до кримінальних правопорушень у кіберпросторі, їх вчинення та приховування наслідків цих правопорушень; 3) сервери постачальників електронних комунікаційних послуг, хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів.

Досліджено питання допустимості доказів, отриманих із відкритих джерел. Автор доводить, що при формуванні нормативної моделі допустимості доказів, отриманих із відкритих джерел, цілком прийнятною є аналогія із регламентацією допустимості показань з чужих слів, які відповідно до ч.6 ст. 97 КПК України не можуть бути допустимим доказом факту чи обставин, на доведення яких вони надані, якщо показання не підтверджується іншими доказами, визнаними допустимими згідно з правилами, відмінними від положень частини другої цієї статті.

Автор звертається до питання щодо проведення слідчих та негласних слідчих (розшукових) дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Доведено, що положення ч. 6 ст. 236 КПК України в частині використання формулювання «виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку» потребує коригування, оскільки не відповідає вимозі передбачуваності закону та створює передумови для зловживань з боку сторони обвинувачення.

У зв'язку із цим, автором запропоновано змінити положення абзацу другого ч.6 ст. 236 КПК України та наділити слідчого, прокурора повноваженнями здійснювати пошук, виявлення та фіксацію комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення обшуку виключно якщо дозвіл на такий пошук наданий в ухвалі слідчого судді. Водночас, обґрунтовано, що чинна редакція абз. 2 ч.6 статті 236 КПК України може бути актуальною лише

в умовах воєнного стану, коли публічний інтерес розслідування злочинів проти основ національної безпеки превалюють над приватним, але передбачений нею порядок не може виступати ординарною правовою процедурою.

Обґрунтовано доцільність доповнення ст. 263 КПК України нормою, відповідно до якої зняття інформації з електронних комунікаційних мереж до постановлення ухвали слідчого судді може бути розпочато на підставі постанови слідчого, прокурора лише у випадку, ч.1 ст. 250 КПК України.

Досліджено процесуальні особливості розгляду та вирішення клопотань про тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Запропоновано доповнити ст. 163 КПК України нормою, відповідно до якої клопотання слідчого, прокурора про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо розглядається слідчим суддею у день його надходження. Крім того, обґрунтовано доцільність доповнення ст. 165 КПК України частиною 5 у такій редакції: «Ухвала слідчого судді про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо підлягає негайному виконанню».

Розглянуто питання здійснення процесуальних дій в межах міжнародного співробітництва при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. Зазначено, що міжнародне співробітництво у розглядуваному контексті здійснюється як

шляхом виконання запитів у порядку, передбаченому КПК України, так і шляхом постійного обміну інформацією задля забезпечення оперативності досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Досліджено проблеми використання спеціальних знань при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. Під спеціальними знаннями при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі запропоновано розуміти сукупність наукових знань і практичних навичок у сфері інформаційних технологій, комп'ютерних систем і мереж, цифрової та комп'ютерно-технічної криміналістики, телекомунікацій, інформаційної безпеки, програмування, аналізу шкідливого програмного забезпечення та електронних фінансових технологій, здобутих у межах академічної підготовки й професійного досвіду, носіями яких є залучені до кримінального провадження за рішенням слідчого, прокурора, слідчого судді чи суду особи, що використовуються з метою вирішення питань, необхідних для повного, всебічного й об'єктивного встановлення фактичних обставин кримінального провадження.

На підставі узагальнення наукових та науково-практичних джерел сформульовано висновок про те, що при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі актуальними є як процесуальні, так і непроцесуальні форми використання спеціальних знань. Процесуальні форми здебільшого проявляються у залученні відповідних спеціалістів при проведенні слідчих (розшукових) дій. Непроцесуальна форма використання спеціальних знань проявлятиметься здебільшого у консультативній та довідковій діяльності суб'єктів спеціальних знань.

Сформульовано висновок про те, що найпоширенішими видами експертиз, які призначаються у кримінальних провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі є комп'ютерно-технічна експертиза та експертиза електронних комунікацій.

Розглянуто окремі питання призначення та проведення судових експертиз при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Сформульовано відповідні зміни та доповнення до положень чинного КПК України.

Ключові слова: кримінальне провадження, суб'єкти кримінального провадження, кримінальне процесуальне доказування, докази, електронні (цифрові) докази, кіберпростір, слідчий, прокурор, слідчий суддя, слідчі (розшукові) дії, негласні слідчі (розшукові) дії, спеціальні знання, судові експертизи.

SUMMARY

Filimonov M.V. The Peculiarities of proof during the pre-trial investigation of criminal offenses committed in cyberspace. – Qualifying scientific work as a manuscript.

Dissertation for obtaining the Doctor of Philosophy degree in specialty 081 – Law (field of knowledge 08 – Law). – National University «Odesa Law Academy», Odesa, 2026.

The dissertation represents the first comprehensive and systematic study in the national science of criminal procedure devoted to the theoretical and practical problems of proof in the course of the pre-trial investigation of criminal offenses committed in cyberspace, carried out on the basis of the provisions of the Criminal Procedure Code of Ukraine of 2012, contemporary doctrinal approaches, judicial practice, and international legal standards.

On the basis of a generalization and critical analysis of doctrinal developments and scholarly sources, the author identifies the principal directions of research concerning the problems of investigating criminal offenses committed in cyberspace. These include: 1) scientific studies devoted to forensic and criminalistic issues of investigating criminal offenses committed in cyberspace; 2) research focused on the peculiarities of investigating specific categories of cyber-related criminal offenses; 3) studies addressing the use of electronic and digital evidence in criminal procedural proof; 4) research concerning the application of special knowledge and expertise in the investigation of such offenses; 5) criminological studies aimed at analyzing the phenomenon of cybercrime and developing measures for its prevention and counteraction; 6) works devoted to issues of international legal cooperation in combating crime; and 7) interdisciplinary research on countering cybercrime within the framework of other branches of scientific knowledge.

The concept of a criminal offense committed in cyberspace has been specified and clarified. It is proposed to understand such an offense as a socially dangerous and culpable act provided for by the criminal law of Ukraine, committed by a subject of criminal liability within or through the use of cyberspace as a specific socio-

technical and informational environment, by means of information and communication technologies, computer systems, networks, or digital data, and encroaching upon social relations protected by criminal law.

A classification of criminal offenses committed in cyberspace has been developed. The author proposes that such offenses be classified depending on the method of implementation of their objective elements. According to this criterion, two groups are distinguished: exclusively cyberspace-based criminal offenses, which can be committed solely within cyberspace, and variably cyberspace-related criminal offenses, the objective elements of which may be realized both in the physical environment and in cyberspace, depending on the specific circumstances of their commission.

On the basis of an analysis and generalization of the case law of the European Court of Human Rights, the minimum guarantees for the protection of the right to respect for private and family life in cyberspace in accordance with the requirements of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms have been identified. These guarantees include: a clear legislative definition of the categories of persons and data subject to interception; the existence of prior judicial authorization or effective subsequent oversight of surveillance measures; normative formulation of the criteria for initiating interception; as well as the establishment of limitations on data retention periods and a clearly defined procedure for their destruction.

International standards and foreign experience in the normative regulation of the pre-trial investigation of criminal offenses committed in cyberspace have been examined. The main procedural standards of cybercrime investigation common to all regional human rights protection systems have been identified. These include: 1) the obligation of states to introduce a clear and foreseeable legal framework for obtaining access to information stored in electronic systems; 2) the obligation to adapt the competence of national authorities to include the prosecution of cross-border crimes and to ensure the possibility of criminal prosecution where the offender or the consequences of the offense involve several states; 3) the conduct of

searches and seizures strictly within the limits of specific criminal proceedings while ensuring the originality, authenticity, and integrity of seized data and mandatory documentation of all legal procedures; 4) the possibility of extraditing persons who have committed cybercrimes; the definition of the principal forms of international legal assistance, including the exchange of information, evidence, documents, material and digital data, including without the requirement of double criminality; 5) ensuring the confidentiality of information obtained within the framework of international cooperation; 6) mandatory authorization by a competent authority of procedural actions involving interference with private life.

The content, concept, and classification of electronic evidence in criminal proceedings have been examined. It has been substantiated that electronic (digital) evidence should be understood as factual data in electronic form obtained in accordance with the procedure established by the Criminal Procedure Code of Ukraine, characterized by integrity, authenticity, reliability, and suitability for examination, and having evidentiary value for establishing facts and circumstances in criminal proceedings.

The classification of electronic (digital) evidence is proposed to be carried out according to its form, distinguishing electronic documents, electronic messages and communications, virtual assets, technical or service data, and other types of information existing in digital form.

It has been established that the sources of electronic (digital) evidence during the pre-trial investigation of criminal offenses committed in cyberspace include: 1) electronic devices containing information relevant to criminal proceedings; 2) electronic communication systems used during the preparation, commission, and concealment of criminal offenses; 3) servers of electronic communications service providers, cloud service resources, and 4) data processing centers of relevant service providers.

The issue of admissibility of evidence obtained from open sources has been investigated. The author substantiates that, when developing a regulatory model for the admissibility of such evidence, it is appropriate to apply an analogy with the

regulation of hearsay testimony, which, in accordance with criminal procedural legislation, cannot serve as admissible evidence of a fact or circumstance unless corroborated by other admissible evidence.

Particular attention is devoted to the conduct of investigative and covert investigative (search) actions in the course of the pre-trial investigation of criminal offenses committed in cyberspace. It is proved that the wording of Part 6 of Article 236 of the Criminal Procedure Code of Ukraine, concerning the «detection of access or the possibility of access to computer systems or their parts, mobile communication terminals», requires legislative clarification, as it does not comply with the requirement of legal certainty and foreseeability and creates preconditions for potential abuses by the prosecution.

In this regard, it is proposed to amend the relevant provisions and to empower investigators and prosecutors to search for, detect, and record computer data located in computer systems or their parts only if such actions are expressly authorized by an investigating judge. At the same time, it is substantiated that the current wording may be justified only under martial law conditions, when the public interest in investigating crimes against national security prevails over private interests, but such a procedure cannot serve as an ordinary legal mechanism.

The expediency of supplementing Article 263 of the Criminal Procedure Code of Ukraine with a provision allowing the interception of information from electronic communication networks prior to a judicial order only in urgent cases established by law is also substantiated.

Procedural peculiarities of examining and resolving motions for temporary access to information held by telecommunications operators and providers regarding communications, subscribers, the provision of telecommunications services, including the receipt of services, their duration, content, and transmission routes, have been analyzed. Proposals are made to amend the legislation to ensure that such motions are considered by an investigating judge on the day of submission and that court orders granting temporary access are subject to immediate execution.

Issues related to the implementation of procedural actions within the framework of international cooperation during the pre-trial investigation of cybercrimes are also considered. It is emphasized that such cooperation is carried out both through the execution of requests in accordance with the procedure established by the Criminal Procedure Code of Ukraine and through the continuous exchange of information aimed at ensuring the efficiency and promptness of investigations.

The problems of using special knowledge during the investigation of criminal offenses committed in cyberspace have been studied. Special knowledge is defined as a set of scientific knowledge and practical skills in the fields of information technology, computer systems and networks, digital and computer forensics, telecommunications, information security, programming, malware analysis, and electronic financial technologies, acquired through academic training and professional experience and applied by specialists involved in criminal proceedings to ensure a full, comprehensive, and objective establishment of factual circumstances.

It is concluded that both procedural and non-procedural forms of applying special knowledge are relevant in such investigations. Procedural forms are primarily manifested in the involvement of specialists in investigative actions, whereas non-procedural forms are mainly expressed through consultative and advisory activities. The most common types of forensic examinations in proceedings concerning cybercrimes are computer-technical examinations and electronic communications examinations.

Based on the conducted research, appropriate amendments and supplements to the provisions of the current Criminal Procedure Code of Ukraine are formulated.

Keywords: criminal proceedings, participants in criminal proceedings, criminal procedural proof, evidence, electronic (digital) evidence, cyberspace, investigator, prosecutor, investigating judge, investigative (search) actions, covert investigative (search) actions, special knowledge, forensic examinations.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Філімонов М.В. Окремі питання призначення експертизи електронних комунікацій під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. *Правові новели*. 2024. № 24. С. 347-355. URL: http://legalnovels.in.ua/journal/24_2024/48.pdf

2. Філімонов М.В. До питання щодо стану наукової розробленості проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі у юридичній доктрині. *Право і суспільство*. 2024. №6. С. 340-345. URL: http://pravoisuspilstvo.org.ua/archive/2024/6_2024/51.pdf

3. Філімонов М.В. Міжнародні стандарти та зарубіжний досвід нормативної регламентації розслідування кримінальних правопорушень, вчинених у кіберпросторі. *Право і суспільство*. 2025. №3. Т. 2. С. 657-662. URL: http://pravoisuspilstvo.org.ua/archive/2025/3_2025/part_2/91.pdf

4. Філімонов М.В. Питання забезпечення права особи на повагу до приватного життя у кіберпросторі в практиці Європейського суду з прав людини. *Юридичний науковий електронний журнал*. 2025. № 4. С. 632-634. URL: http://lsej.org.ua/4_2025/155.pdf

5. Філімонов М.В. Належний процесуальний порядок ознайомлення із інформацією, що міститься на цифрових пристроях: окремі питання у контексті практики ККС ВС. *Правові новели*. 2025. № 25. С.456-461. URL: http://legalnovels.in.ua/journal/25_2025/60.pdf

наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Філімонов М.В. Використання цифрової інформації з відкритих джерел у кримінальному процесуальному доказуванні: постановка проблеми. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень* : у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 трав. 2023 р.) / за загальною редакцією С.В. Ківалова. Одеса: Видавництво «Юридика». 2023. Т. 2. С. 377-380.

2. Філімонов М.В. Втручання в електронне приватне спілкування у практиці європейського суду з прав людини: окремі питання. *Актуальні питання розвитку юридичної науки в період воєнного стану* : Міжнародна науково-практична конференція. Науково-дослідний інститут публічного права, 17 травня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 358-360. DOI https://doi.org/10.36059/978-966-397-395-1-105.

3. Філімонов М.В. Допустимість доказів, отриманих із веб-сайтів та інтернет-ресурсів: проблеми, доктрини та тенденції судової практики. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів* : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 463-465.

4. Філімонов М.В. Окремі питання допустимості доказів, отриманих у результаті зняття інформації з електронних інформаційних систем. *Європейські орієнтири України: нові виміри у воєнний час* : матеріали міжнар.наук.- практ. конф. (м. Одеса, 16 травня 2025 р.). Одеса, 2025. С. 639-641.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

абз. – абзац

ВП ВС – Велика палата Верховного Суду

ВС – Верховний Суд

ГПК України – Господарський процесуальний кодекс України

ЕОМ – електронно-обчислювальні машини

ЄРДР – Єдиний реєстр досудових розслідувань

ЄДРСР – Єдиний державний реєстр судових рішень

ЄСПЛ – Європейський суд з прав людини

ЄС – Європейський Союз

ЗУ – Закон України

КАС України – Кодекс адміністративного судочинства України

КК України – Кримінальний кодекс України

ККС ВС – Касаційний кримінальний суд у складі Верховного Суду

ОП ККС ВС – Об'єднана палата Касаційного кримінального суду Верховного Суду

КПК України – Кримінальний процесуальний кодекс України 2012 року

НАБУ – Національне антикорупційне бюро України

США – Сполучені Штати Америки

ФРН – Федеративна Республіка Німеччина

ЦПК України – Цивільний процесуальний кодекс України

ШІ – штучний інтелект

п. - пункт

ст. – стаття

ч. – частина

ВСТУП

Обґрунтування вибору теми дослідження. У сучасних умовах стрімкої інформатизації усіх сфер суспільного життя, кіберпростір дедалі частіше стає ключовим середовищем соціальної, економічної, політичної та професійної діяльності, що водночас, зумовило зростання кількості кримінальних правопорушень, вчинених з використанням високих інформаційних технологій. Це в свою чергу породжує низку питань щодо адаптації чинного кримінального процесуального законодавства до таких умов.

Вчинення кримінальних правопорушень у цифровому середовищі обумовлює виникнення ситуації, за якої більшість доказів мають нематеріальний характер, існують у електронній формі, яка відкриває широкі можливості до їх спотворення або знищення, дозволяє зберігати їх на віддалених серверах, навіть поза межами національної юрисдикції. За таких умов, перед доктриною постає низка питань щодо визначення належності та допустимості відповідних доказів, порядку перевірки їх достовірності, а також можливостей застосування спеціальних знань та технічних засобів.

Аналіз наукових джерел та правозастосовної практики засвідчує, що чинне кримінальне процесуальне законодавство не встигає за темпами розвитку цифрових технологій, що породжує проблеми вибору належної процесуальної форми здійснення кримінального процесуального доказування у випадках, коли мова йде про досудове розслідування кримінальних правопорушень, вчинених у кіберпросторі. Цей аспект має ключове значення у контексті забезпечення допустимості відповідних доказів та досягнення визначених ст. 2 КПК України завдань кримінального провадження щодо забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини.

До питання про здійснення кримінального провадження щодо кримінальних правопорушень, вчинених у кіберпросторі у науці

кримінального процесу звертались І.В. Басиста, Л.С. Бєлік, І.І. Васильковський, В.В. Вапнярчук, А.Р. Воробчак, П.П. Галушко, Н.В. Глинська, В.О. Гусєва, О.Ю. Довженко, О.М. Дуфенюк, О.Л. Дульський, І.Г. Каланча, А.В. Коваленко, В.А. Колесник, В.А. Коршенко, Д.І. Клепка, Г.Р. Крет, І.О. Крицька, А.І. Кунтій, І.І. Липкан, Є.Д. Лук'янчиков, В.В. Луцик, Я.В. Неділько, Д.В. Пашнєв, І.В. Пиріг, Ю.О. Пілюков, В.О. Попелюшко, А.В. Ратнова, А.В. Рейнгольд, О.С. Саінчин, О.А. Самойленко, І.А. Смаль, В.В. Сисолятін, Е.Б. Сімакова-Єфремян, А.В. Скрипник, Р.Л. Степанюк, С.Ю. Стратонов, В.А. Сусукайло, Б.Б. Теплицький, О.О. Торбас, А.Я. Хитра, Д.М. Цехан, Ю.В. Циганюк, Ю.М. Чорноус, М.Г. Щербаковський, М.Ю. Яцишин та ін.

Вагомим є внесок у наукове дослідження відповідної проблематики зарубіжних вчених, серед яких С. Бреннер (Susan Brener), А. Бурштейн (Aaron Burstein), А. Вебер (Amalie Weber), Н. Катял (Neal Katyal), О. Керр (Orin Kerr), Д. Коен (Julie Cohen), Л. Лессіг (Lawrence Lessig), Г. Перріт (Henry Perritt), Л. Сачарофф (Laurent Sacharoff), Д. Хантер (Dan Hunter).

Утім, у більшості монографічних дослідженнях, присвячених досудовому розслідуванню кримінальних правопорушень, вчинених у кіберпросторі розкриваються здебільшого питання методики їх розслідування, а також питання правової природи та порядку збирання електронних доказів, натомість, інші аспекти кримінального процесуального доказування висвітлюються лише побічно. Це обумовлює актуальність теми дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконано в межах плану науково-дослідної роботи кафедри кримінального процесу «Реформування кримінального процесуального, кримінально-виконавчого права та оперативно-розшукової діяльності в умовах євроінтеграції та протидії злочинності в епоху цифрового суспільства» у межах виконання теми науково-дослідної роботи Національного університету «Одеська юридична академія»

«Правове та соціальне життя людини в людиноцентристському вимірі в цифрову еру» на 2021–2025 роки (державний реєстраційний номер – 0122U000266).

Мета і завдання дослідження. Метою дисертаційного дослідження є вирішення наукового завдання, яке полягає у формулюванні цілісної концепції кримінального процесуального доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Для досягнення поставленої мети у дисертації вирішувались такі завдання:

– з'ясувати стан наукового дослідження проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– уточнити поняття кіберпростору та кримінальних правопорушень, вчинених у кіберпросторі;

– виокремити основні стандарти, які сформовані у практиці ЄСПЛ щодо забезпечення права на повагу до приватного життя у кіберпросторі;

– виокремити міжнародні стандарти та узагальнити зарубіжний досвід розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– уточнити поняття електронних (цифрових) доказів у кримінальному провадженні та здійснити їх класифікацію;

– встановити поняття та зміст джерел електронних (цифрових) доказів у кримінальному провадженні;

– з'ясувати особливості проведення слідчих (розшукових) дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– з'ясувати особливості проведення негласних слідчих (розшукових) та інших процесуальних дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– з’ясувати специфіку використання спеціальних знань при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– сформулювати пропозиції щодо вдосконалення кримінального процесуального законодавства в частині розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Об’єктом дослідження виступають правовідносини, виникають у зв’язку із кримінальним процесуальним доказуванням при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Предметом дослідження є особливості доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Методи дослідження. Методологічним підґрунтям дисертаційного дослідження виступає комплекс філософських, загальнонаукових та спеціально-наукових методів наукового пізнання. За допомогою діалектичного методу з’ясовано зміст та сутність понять «кіберпростір» та «кримінальні правопорушення, вчинені у кіберпросторі» (підрозділ 1.2). Системний метод та метод системно-структурного аналізу використовувався при визначенні системи міжнародних стандартів розслідування кримінальних правопорушень, вчинених у кіберпросторі (підрозділ 1.2), визначенні системи електронних доказів та їх джерел (підрозділи 2.1, 2.2), а також удосконалення кримінального процесуального законодавства у частині оптимізації кримінального процесуального доказування при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі (розділи 2,3). За допомогою функціонального методу розкрито проблеми забезпечення належної кримінальної процесуальної форми окремих процесуальних дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі (підрозділи 3.1,3.2). За допомогою герменевтичного методу було встановлено зміст положень КПК України, що регламентують порядок

проведення окремих процесуальних дій у кримінальному провадженні щодо кримінальних правопорушень, вчинених у кіберпросторі (розділи 2,3). Формально-юридичний метод використовувався при дослідженні положень Конституції України, міжнародно-правових актів, кримінального процесуального законодавства України, рішень Європейського суду з прав людини (розділи 1,2,3). За допомогою порівняльно-правового методу було проаналізовано положення кримінального процесуального законодавства окремих зарубіжних країн щодо порядку здійснення досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі (підрозділ 1.4). Логіко-нормативний метод використовувався при формулювання змін та доповнень до КПК України (розділи 2,3).

Теоретичну основу дисертаційного дослідження складають праці вітчизняних та зарубіжних учених в галузі конституційного, кримінального, кримінального процесуального права, оперативно-розшукової діяльності, кібербезпеки тощо.

Нормативну основу дослідження становлять Конституція України, міжнародно-правові акти, Кримінальний процесуальний кодекс України, окремі закони України, підзаконні акти, акти законодавства окремих зарубіжних країн (Великої Британії, США, Франції).

Емпіричну базу дисертаційного дослідження становлять: рішення Європейського суду з прав людини, постанови Верховного Суду, судові рішення, розміщені у Єдиному державному реєстрі судових рішень.

Наукова новизна одержаних результатів полягає у тому, що дисертація є першим у вітчизняній науці кримінального процесу комплексним дослідження теоретичних та практичних проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі на основі положень КПК України 2012 року.

У межах проведеного наукового дослідження одержано такі результати, що мають наукову новизну:

вперше:

– визначено коло даних, які можуть міститися у хмарних ресурсах і центрах обробки даних як джерелах електронних (цифрових) доказів у провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі, зокрема встановлено, що ними є: 1) дані, які зберігаються у хмарних ресурсах надавачів хмарних послуг і центрів обробки даних, що перебувають у володінні надавачів послуг таких центрів; 2) дані про доступ до цієї інформації користувача хмарних послуг або центру обробки даних; 3) дані про наявність резервних копій такої інформації та систем даних і про передання резервних копій інформації користувачу; 4) дані про несанкціоновані дії, спрямовані на доступ до інформації, яка зберігається у хмарному сховищі або центрі обробки даних (існування зовнішніх і внутрішніх загроз, кібератаки та інциденти кібербезпеки); 5) дані про знищення інформації та її резервних копій;

– запропоновано доповнити КПК України ст. 88^2 під назвою «Допустимість доказів, отриманих із відкритих джерел» та викласти її у такій редакції: «Докази, отримані із відкритих джерел можуть бути визнані допустимими виключно за умови підтвердження джерела їх походження та якщо відповідні відомості підтверджуються іншими доказами, які визнані допустимими за правилами цього Кодексу»;

– запропоновано доповнити ч.2 ст. 237 КПК України абз. третім такого змісту: «Під час огляду житла чи іншого володіння особи виявлення та фіксація комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення огляду можлива лише за добровільною згодою володільця цього майна або якщо дозвіл на такий огляд був наданий в ухвалі слідчого судді»;

– запропоновано викласти абзац другий ч.6 ст. 236 КПК України у такій редакції: «Прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення обшуку виключно якщо дозвіл на такий пошук наданий в ухвалі слідчого судді». Водночас обґрунтовано, що чинна редакція абз. 2 ч.6 статті 236 КПК України

може бути застосовною в умовах воєнного стану, коли публічний інтерес розслідування злочинів проти основ національної безпеки превалює над приватним;

– запропоновано доповнити ч.4 ст. 163 КПК України нормою, відповідно до якої клопотання слідчого, прокурора про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо розглядається слідчим суддею у день його надходження;

удосконалено:

– класифікацію електронних (цифрових) доказів, зокрема з урахуванням її теоретичного та практичного значення та із застосуванням логічних правил поділу понять такі докази за критерієм їх форми запропоновано поділяти на наступні види: 1) електронні документи (текстові документи, аудіо- та відеозаписи, фотознімки та інші зображення); 2) електронні повідомлення (текстові, мультимедійні та голосові); 3) віртуальні активи; 4) логи, дані клієнтського середовища, контекстні дані, метадані та інші технічні дані; 5) інша інформація в електронній (цифровій) формі;

– науковий підхід до визначення поняття «кримінальне правопорушення, вчинене у кіберпросторі», під яким запропоновано розуміти передбачене законом України про кримінальну відповідальність суспільно небезпечне винне діяння, що вчиняється суб'єктом кримінального правопорушення у межах або з використанням кіберпростору як особливого соціально-технічного та інформаційного середовища, шляхом застосування інформаційно-комунікаційних технологій, комп'ютерних систем, мереж чи цифрових даних, та посягає на охоронювані кримінальним законом суспільні відносини;

– науковий підхід до виокремлення мінімальних гарантій захисту права на повагу до приватного та сімейного життя у кіберпросторі відповідно до

вимог статті 8 Конвенції та прецедентної практики ЄСПЛ. Зокрема, виокремлено такі гарантії як: 1) чітке законодавче визначення категорій осіб та даних, щодо яких можливе перехоплення; 2) наявність попереднього судового контролю або ефективного подальшого нагляду за спостереженням; 3) нормативне формулювання критеріїв, за якими ухвалюється рішення про ініціювання перехоплення; 4) обмеження строків зберігання даних та встановлення чіткого порядку їх знищення;

– поняття «спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі» під якими запропоновано розуміти сукупність наукових знань і практичних навичок у сфері інформаційних технологій, комп'ютерних систем і мереж, цифрової та комп'ютерно-технічної криміналістики, телекомунікацій, інформаційної безпеки, програмування, аналізу шкідливого програмного забезпечення та електронних фінансових технологій, здобутих у межах академічної підготовки й професійного досвіду, носіями яких є залучені до кримінального провадження за рішенням слідчого, прокурора, слідчого судді чи суду особи, що використовуються з метою вирішення питань, необхідних для повного, всебічного й об'єктивного встановлення фактичних обставин кримінального провадження;

набули подальшого розвитку:

– доктринальні положення щодо розуміння сутності електронних (цифрових) доказів, зокрема на підставі дослідження теоретичних підходів до її розкриття виокремлено процесуальний, технічний і криміналістичний аспекти її розуміння, вказано на взаємодоповнюваність і взаємозв'язок цих аспектів, визначено з їх урахуванням ознаки цих доказів і сформульовано авторську дефініцію їх поняття;

– доктринальні підходи до розуміння поняття та системи джерел електронних (цифрових) доказів, зокрема доведено, що в ході досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, ними є: 1) електронні пристрої, які містять значиму для кримінального провадження інформацію; 2) електронні комунікаційні системи, які використовувалися в

ході підготовки до кримінальних правопорушень у кіберпросторі, їх вчинення та приховування наслідків цих правопорушень; 3) сервери постачальників електронних комунікаційних послуг, хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів;

– наукові підходи до класифікації кримінальних правопорушень, вчинених у кіберпросторі, зокрема, запропоновано здійснювати таку класифікацію залежно від способу реалізації їх об'єктивної сторони;

– підходи до визначення міжнародних процедурних стандартів розслідування кіберзлочинів, які є спільними для усіх регіональних систем захисту прав людини;

– пропозиції щодо нормативного закріплення допустимості проведення зняття інформації з електронних комунікаційних мереж до постановлення ухвали слідчого судді на підставі постанови слідчого, прокурора у випадку, передбаченому ч.1 ст. 250 КПК України.

Практичне значення одержаних результатів полягає у тому, що сформульовані у дисертації висновки та пропозиції можуть бути використані у:

– науково-дослідній роботі – для розвитку подальших наукових досліджень проблематики кримінального процесуального доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– правотворчій діяльності – для удосконалення нормативної регламентації кримінального процесуального доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– правозастосовній діяльності – для забезпечення єдності застосування норм кримінального процесуального та суміжного законодавства, що регламентує питання доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

– навчальному процесі – при викладанні навчальних дисциплін «Кримінальний процес», «Сучасні проблеми кримінально-процесуального права», «Проведення слідчих (розшукових) дій», «Оперативно-розшукові заходи та негласні слідчі (розшукові) дії», «Забезпечення законності проведення оперативно-розшукових заходів та слідчих (розшукових) дій» (Акт впровадження в освітній процес Національного університету «Одеська юридична академія» від 19 січня 2026 року).

Особистий внесок здобувача. Дисертація становить самостійне дослідження, викладені у дисертації висновки і пропозиції становлять особистий здобуток автора.

Апробація результатів дослідження. Положення та висновки дисертаційного дослідження обговорювались під час засідання кафедри кримінального процесу Національного університету «Одеська юридична академія». Основні результати наукового дослідження були висвітлені у доповідях на наукових, науково-практичних конференціях, зокрема на: Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень» (м. Одеса, 19 травня 2023 р.), Міжнародній науково-практичній конференції «Актуальні питання розвитку юридичної науки в період воєнного стану» (м. Львів, 17 травня 2024 р.), Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.), Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: нові виміри у воєнний час» (м. Одеса, 16 травня 2025 р.).

Публікації. Основні положення дисертаційного дослідження відображені у дев’яти наукових публікаціях, у тому числі у п’ятьох статтях, опублікованих у наукових фахових виданнях, перелік яких затверджено МОН України, а також чотирьох тезах доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що включають 9 підрозділів, висновків, списку використаних джерел (205 найменувань) та 3 додатків. Загальний обсяг дисертації складає 201 сторінку, з них основний текст – 171 сторінка, додатки розміщені на 8 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ НАУКОВОГО ДОСЛІДЖЕННЯ ПРОБЛЕМ ДОКАЗУВАННЯ ПРИ ЗДІЙСНЕННІ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

1.1. Стан наукового дослідження проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі

Дослідження проблем розслідування кримінальних правопорушень, учинених у кіберпросторі, на сучасному етапі набуває особливої актуальності, оскільки цифрові технології остаточно інтегрувалися не лише у повсякденне життя людини, а й у функціонування економіки, суспільства та системи державного управління. Нині кіберпростір виступає не тільки засобом комунікації та обміну інформацією, а й специфічним середовищем вчинення окремих видів кримінальних правопорушень, зокрема шахрайств, крадіжок, незаконних операцій з платіжними засобами, розповсюдження порнографічної продукції, а також посягань на національну безпеку держави.

Кримінальним правопорушенням, що вчиняються у кіберпросторі, притаманні іманентні ознаки, серед яких високий рівень латентності, транскордонність та використання сучасних інформаційних технологій і телекомунікаційних мереж. Зазначені особливості істотно ускладнюють їх наукове осмислення, оскільки, поряд із традиційними криміналістичними знаннями, воно потребує використання спеціальних знань у сфері кібербезпеки, зокрема, щодо застосування технологій анонімізації, шифрування та інших інструментів захисту інформації. Вказаний чинник значно ускладнює й практичну діяльність органів досудового розслідування.

У цьому контексті наукові дослідження в означеній сфері сприяють формуванню ефективних методик розслідування кримінальних правопорушень, учинених у кіберпросторі, а також удосконаленню процесів збирання, фіксації та використання цифрових доказів. Наукові напрацювання з цієї проблематики у вітчизняній юридичній доктрині з'являлися поступово, по мірі розвитку та масового впровадження цифрових технологій у повсякденне життя громадян. Саме це зумовило зростання кількості кримінальних правопорушень, учинених у кіберпросторі, та актуалізувало питання щодо специфічних способів доказування, які істотно відрізняються від тих, що застосовуються при розслідуванні «традиційних» кримінальних правопорушень, вчинених у фізичному, а не віртуальному середовищі.

Однією із перших робіт, у якій комплексно розглянуто проблеми розслідування кримінальних правопорушень, вчинених у кіберпросторі є дисертаційне дослідження Д.В. Пашнєва «Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій» (м. Харків, 2007). Автором, зокрема, було вперше виокремлено структуру спеціальних знань обізнаних осіб, які залучаються до розслідування комп'ютерних злочинів, до якої включено: «1) основні спеціальні знання, до яких відносяться технічні знання в галузі комп'ютерних технологій і за якими здійснюється підготовка фахівців у вузах України – інформатика, комп'ютерні науки, комп'ютерна інженерія, програмна інженерія, системна інженерія, автоматизація та комп'ютерно-інтегровані технології, безпека інформаційних і комунікаційних систем, системи технічного захисту інформації, управління інформаційною безпекою; 2) додаткові юридичні знання – з криміналістики, кримінального процесу, нормативних актів, що регламентують діяльність в сфері використання комп'ютерних технологій» [77, с. 9].

Загалом, наукові дослідження, присвячені криміналістичним проблемам розслідування кримінальних правопорушень, вчинених у кіберпросторі натепер складають основний масив доктринального доробку у цій галузі.

Зокрема, цим питанням присвячено монографічні дослідження І.І. Васильковського, Б.Б. Теплицького, О.А. Самойленко, Я.В. Неділько.

У дисертаційному дослідженні І.І. Васильковського «Взаємодія правоохоронних органів при розслідуванні кіберзлочинів» (м. Київ, 2019) автором, серед іншого, було сформульовано сучасну класифікацію кримінальних правопорушень, вчинених у кіберпросторі: «1) за масштабністю (загальносвітові, на рівні країни, на рівні користувача, на рівні щоденного використання); 2) за ступенем соціальної небезпеки (високий ступінь їх розповсюдження; дуже високий рівень суспільної небезпеки (збитки від них часто не піддаються обчисленню); ступінь латентності (чи не найбільший порівняно з іншими видами злочинів); велика кількість професійної або «білокоміркової» злочинності; транснаціональний характер їх окремих видів); 3) згідно з класифікацією злочинів, впроваджених КК України (використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп’ютерних мереж і мереж електрозв'язку (у сферах платіжних систем); обігу інформації протиправного характеру із використанням електронно- обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж); 4) з урахуванням мотивації злочинців (кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних системи з метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам); інші злочини)» [11, с. 111].

Дисертаційне дослідження 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» (м. Київ, 2021) спрямоване на комплексний аналіз теоретичних і практичних засад техніко-криміналістичного забезпечення розслідування кримінальних правопорушень, пов'язаних із використанням електронно-обчислювальної техніки, комп'ютерних систем, мереж та мереж електрозв'язку. У межах роботи автор ґрунтовно досліджує особливості застосування техніко-криміналістичних засобів і методів у діяльності органів досудового розслідування під час виявлення, фіксації та дослідження слідів таких злочинів. Окрім цього, у дисертації запропоновано типізований перелік запитань, які доцільно ставити свідкам на подальших етапах розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем і мереж, що сприяє підвищенню ефективності доказування та оптимізації слідчої діяльності [122, с. 93-94].

У дисертаційному дослідженні Я. В. Неділько «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» (м. Київ, 2023) здійснено комплексний аналіз криміналістичних і процесуальних засад розслідування кримінальних правопорушень, пов'язаних із застосуванням інформаційних комп'ютерних технологій. Автор, зокрема, зосереджує увагу на дослідженні способів учинення таких правопорушень і характерних для них слідів, особливостей обстановки вчинення злочину та особи правопорушника. Значне місце в роботі відведено аналізу типових слідчих ситуацій, формуванню слідчих версій і плануванню досудового розслідування у відповідних кримінальних провадженнях. Окремо розглянуто специфіку проведення слідчих (розшукових) дій, застосування заходів забезпечення кримінального провадження, а також використання спеціальних знань, зокрема у формі судових експертиз, під час розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій [73].

Комплексному дослідженню методики розслідування злочинів, що вчиняються у кіберпросторі були присвячені монографічне дослідження О.А. Самойленко «Основи методики розслідування злочинів, вчинених у кіберпросторі» (м. Одеса, 2020) та дисертаційне дослідження О.Ю. Довженко «Основи методики розслідування кіберзлочинів» (м. Харків, 2021).

У монографії О.А. Самойленко авторка комплексно розробила методику розслідування відповідної категорії кримінальних правопорушень, зокрема, звернулася до питань щодо стану правового регулювання боротьби зі злочинами, що вчиняються у кіберпросторі, здійснила криміналістичну класифікацію злочинів, вчинених у кіберпросторі, виокремила структурні елементи криміналістичної характеристики злочинів, вчинених у кіберпросторі, предмети злочинного посягання у кіберпросторі, класифікувала типові способи вчинення злочинів у кіберпросторі, дослідила організаційні форми початку досудового розслідування відповідної категорії кримінальних правопорушень, звернулася до питань взаємодії слідчого із оперативними підрозділами, виокремила типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі, а також дослідила питання використання спеціальних знань при розслідуванні відповідної категорії кримінальних правопорушень тощо [111].

У дисертаційному дослідженні О.Ю. Довженка «Основи методики розслідування кіберзлочинів» (м. Харків, 2021) автор у ході свого наукового пошуку звертається до питання про специфіку слідчих (розшукових) дій, які проводяться при розслідуванні відповідної категорії кримінальних правопорушень та особливостей доказування окремих обставин, зазначаючи, що «вирішального значення набувають прийоми, способи та техніки роботи з інформацією та проведення відповідних слідчих дій з метою виявлення цієї інформації, яка дозволяє встановити характер злочинного діяння у кіберпросторі. Також слід брати до уваги складні причинно-наслідкові зв’язки між діями в реальному світі та результатом, що настає в кіберпросторі та через нього знов таки в реальному світі. Розслідування кіберзлочину переважно

повинно бути спрямоване на виявлення подій в кіберпросторі, що призвели до настання злочинного результату в реальному світі» [29, с. 194].

Слід також відзначити й наявність у доктрині наукових досліджень, присвячених розслідуванню окремих категорій кримінальних правопорушень, що вчиняються у кіберпросторі.

Однією із перших дисертацій, у яких досліджувалася проблематика розслідування аналізованої категорії кримінальних правопорушень була робота А.І. Анапольської «Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків» (м. Луганськ, 2011). У ході свого дослідження авторка сформулювала низку пропозицій, які стали істотним доктринальним підґрунтям для подальшого наукового осмислення проблематики розслідування відповідної категорії кримінальних правопорушень. Зокрема, нею було запропоновано поділити способи цих злочинів на дві групи: способи отримання конфіденційних даних про реквізити справжніх платіжних карток та способи використання отриманих реквізитів з метою вчинення розкрадання [3, с. 148].

Доволі детально у ході своєї роботи науковиця дослідила й питання соціально-демографічних та психологічних рис осіб, що вчиняють відповідні кримінальні правопорушення. Як зазначає дослідниця, слідчому зазвичай протистоять особи, які мають вищу освіту, високий інтелект, досконало володіють спеціальними знаннями та навичками. Сучасні злочинці, які вчиняють шахрайства у сфері функціонування електронних розрахунків, можуть бути класифіковані по двох великих групах: внутрішні користувачі та зовнішні користувачі.

Така класифікація правопорушників на внутрішніх і зовнішніх користувачів сприяє більш точному моделюванню слідчих ситуацій та забезпечує ефективність окремих слідчих (розшукових) дій на початковому етапі розслідуванні. Очевидно, що відповідний підхід не втратив актуальності й натепер.

Звертається авторка й до широкого кола питань, пов'язаних із особливостями проведення окремих слідчих (розшукових) дій при розслідуванні даного виду шахрайства, зокрема, особливостей проведення допиту, огляду, обшуку, а також експертиз.

У дисертаційному дослідженні А. В. Рейнгольда «Основи методики розслідування шахрайства в інтернет-комерції» (м. Дніпро, 2023) розроблено концептуальні засади методики розслідування шахрайства у сфері інтернет-комерції. Автор обґрунтовує підхід до дослідження даної методики через організацію та проведення тактичних операцій, на основі чого створено низку конкретних тактичних операцій із оптимізованим комплексом дій для кожної. Серед запропонованих операцій: «Фальшивий сайт», «Незаконна транзакція», «Встановлення IP-адреси», «Ідентифікація особи у віртуальному середовищі», «Встановлення умислу» та «Організація затримання шахрая, який діяв у мережі Інтернет» [104, с. 72].

У дотичному науковому напрямку здійснював наукові розвідки В.В. Сисолятін, підготувавши дисертаційне дослідження «Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» (м. Київ, 2024). Дослідником було одним із перших сформульовано у доктрині систему способів безпосереднього вчинення досліджуваної категорії кримінальних правопорушень: 1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг); 2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 4) розповсюдження шкідливих програмних чи технічних засобів або їхній збут з використанням мережі Інтернет; 5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах; 6) умисне масове розповсюдження повідомлень електрозв'язку,

здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін. [113, с. 175].

До цієї ж групи наукових праць слід віднести й дослідження С.В. Чучко «Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет» (м. Дніпро, 2021). Автором вперше на монографічному рівні було комплексно досліджено особливості розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет. У дослідженні автор виокремив типові способи здійснення шахрайських дій через мережу Інтернет, серед яких: «розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його вартості; розміщення фейкової інформації про продаж товару за умов накладної плати з подальшим отриманням частини його вартості на платіжну карту (передоплати); створення сайтів магазинів у мережі Інтернет або їх копій, що діють за принципом фірм-одноденок; кібер-втручання в обліковий запис сумлінного продавця, рівень довіри якого відповідає потребам споживачів, і здійснення шахрайських угод від його імені; отримання грошей за лот, виставлений на інтернет-аукціоні, від декількох покупців відразу; отримання грошей за фальсифікований чи заздалегідь зіпсований товар; отримання грошей за товар, що повинен складатися з великої кількості вузлів і комплектуючих без надання всієї складової (за умов, якщо це заздалегідь сплановано); шахрайські дії від імені несправжнього «покупця» шляхом отримання ним інформації про номер карткового рахунку, персональні дані та номер мобільного телефону продавця «під легендою» необхідності перерахування грошей із подальшим зняттям з рахунку всіх коштів; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати; підміна товару представником відділень поштового зв'язку» [159, с. 116].

У науковій праці, серед іншого, доволі детально розглянуто питання організації та здійсненні взаємодії слідчих, оперативних працівників при вирішенні проблемних конфліктних слідчих ситуацій у справах про шахрайство у мережі Інтернет, сформульовано типові слідчі ситуації

розслідування досліджуваного виду шахрайства, виокремлено групи обставин, що підлягають встановленню, під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет, визначено типові джерела доказів у кримінальних провадженнях про шахрайства даної категорії, а також названо основні фактори, що впливають на рівень вчинення шахрайств при купівлі-продажу через мережу Інтернет, серед яких нечіткість законодавчого регулювання умов створення інтернет-магазинів і порядку здійснення цивільно-правових угод купівлі-продажу у дистанційній формі. Такий висновок сприяє формуванню міжгалузевого наукового дискурсу та окреслює напрями подальших досліджень і вдосконалення правового регулювання.

Загалом, сформульовані науковцем положення мають істотне значення для розвитку криміналістичної та кримінальної процесуальної доктрини та правозастосовної практики, оскільки комплексно охоплюють як теоретичні, так і прикладні аспекти розслідування шахрайств, учинених у мережі Інтернет. Насамперед, детальний аналіз організації та здійснення взаємодії слідчих і оперативних працівників у проблемних та конфліктних слідчих ситуаціях сприяє поглибленню наукових уявлень про координацію суб'єктів кримінального провадження в умовах цифрового середовища, де швидкість обігу інформації та транснаціональний характер злочинної діяльності суттєво ускладнюють процес доказування.

У аналогічному напрямку здійснювала науковий пошук й Т.В. Коршикова, підготувавши дисертаційне дослідження «Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» (м. Київ, 2021). Дослідниця здійснила спробу класифікації способів вчинення шахрайств з використанням електронно-обчислюваної техніки, які умовно поділила залежно від: «а) періодичності вчинення кримінального правопорушення; б) сфери застосування; в) кількості задіяних до вчинення шахрайства осіб; г) предмета посягання; д) виду ЕОТ, яка використовувалась; е) інформаційної підтримки; є) характеру «стосунків», що виникають між потерпілим і злочинцем; ж) місця створення та місця реєстрації IP-адреси

ЕОТ; з) способів введення в оману або зловживання довірою; і) за характером подання відомостей; ї) використання мережі Інтернет» [53, с. 62].

Окремо заслуговує увагу дослідження авторкою трьох груп слідів, які залишаються внаслідок вчинення відповідних кримінальних правопорушень – матеріальних, цифрових та віртуальних. Зокрема, до матеріальних слідів дослідниця зараховує відображення, що залишаються на електронно-обчислювальній техніці та інших технічних засобах, які використовувалися під час учинення шахрайства (клавіатурі, дисководах, джерелах безперебійного живлення, принтерах тощо), а також на предметах, здобутих у результаті протиправних дій. До цифрових слідів, своєю чергою, віднесено відомості, що свідчать про зміни у файловій системі електронно-обчислювальної техніки, а також інформаційні сліди, які формуються в мережі Інтернет у процесі створення та адміністрування веб-сайтів, облікових записів і сторінок у соціальних мережах, комунікації злочинця з потерпілим та здійснення операцій з використанням банківських рахунків. Водночас носіями так званих віртуальних слідів авторка визначає осіб, які можуть бути очевидцями кримінального правопорушення, зокрема тих, хто був присутній під час створення веб-сайту чи облікового запису правопорушника, використання електронно-обчислювальної техніки з протиправною метою або вчинення інших незаконних дій із її застосуванням.

Пропонована класифікація слідів кримінального правопорушення дозволяє системно підходити до їх виявлення, фіксації та процесуального використання під час досудового розслідування. Чітке розмежування матеріальних, цифрових і «віртуальних» слідів орієнтує слідчих та прокурорів на комплексний збір доказів, запобігає втраті доказової інформації та сприяє правильному вибору слідчих (розшукових) дій і судових експертиз.

Достатньо велику увагу у роботі приділено використанню спеціальних знань під час розслідування шахрайства з використанням ЕОМ. Важливим внеском у доктрину слід вважати систематизацію науковицею тих видів експертних досліджень, які забезпечують повне та всебічне розслідування цих

кримінальних правопорушень, до яких віднесено: 1) експертизу комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза); 2) дактилоскопічну експертизу відбитків слідів рук осіб, які були вилучені з ЕОТ та інших предметів, а також у приміщенні, де здійснювалось використання ЕОТ з метою вчинення шахрайства; 3) експертизу матеріалів і засобів звукозапису, де об'єктом дослідження можуть бути записи дій та переговори осіб, причетних до шахрайства; 4) молекулярно-генетичну експертизу з метою дослідження біологічних зразків, відібраних у живих осіб, і слідів біологічного походження, вилучені під час проведення слідчих (розшукових) дій.

Така систематизація дозволяє слідчому, прокурору чітко орієнтуватися у видах спеціальних знань, необхідних для встановлення як цифрових, так і матеріальних та біологічних слідів кримінального правопорушення. Крім того, вона сприяє правильному визначенню об'єктів експертного дослідження та формулюванню релевантних питань перед експертами, що мінімізує ризик втрати відповідних доказів.

У межах поставленого завдання не можна оминути увагою й ті дослідження, які присвячені питанням, тісно пов'язаним із проблемою розслідування кримінальних правопорушень, вчинених у кіберпросторі. Зокрема, значну увагу привертає питання електронних та цифрових доказів, яке нині активно вивчається в кримінальній процесуальній доктрині. Йому присвячене дисертаційне дослідження А. В. Ратнової «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні» (м. Львів, 2021). Авторка виділяє характерні ознаки електронних документів як джерел доказів, зокрема наявність метаданих, електронну форму та необхідність візуалізації за допомогою спеціалізованих програм і пристроїв. Крім того, вона пропонує класифікацію електронних документів за стадіями виготовлення, комбінацією метаданих, доступом до метаданих, ступенем захисту, джерелом походження, місцем розташування та формою [102, с. 74].

В цьому ж ключі не можна не відзначити й дисертаційне дослідження А.В. Скрипника «Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні». Зокрема, саме у цій роботі автор визначив, що слід вважати цифровим доказом у кримінальному провадженні, а саме: а) цифрову інформацію, почерпнуту шляхом відтворення з використанням технічних засобів змісту файлу, збережуваного на носії цифрових даних (теоретичне визначення); б) цифрову інформацію, отриману у передбаченому КПК порядку, на підставі якої дізнавач, слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (нормативне визначення) [114, с. 10].

Висновки автора щодо визначення цифрового доказу мають особливе значення для розвитку кримінально-процесуальної доктрини. По-перше, вони дозволяють чітко окреслити межі та критерії віднесення інформації у цифровій формі до доказів, що забезпечує однозначність визначення її правової природи у кримінальному провадженні. По-друге, розмежування теоретичного та нормативного визначень цифрових доказів сприяє гармонізації наукових підходів і практичного застосування положень КПК України.

Важливого значення на сучасному етапі набувають також питання кримінологічного аналізу кіберзлочинності та розробки заходів протидії цьому явищу. Зокрема, дисертаційне дослідження П. П. Галушка «Кримінологічна характеристика та протидія кіберзлочинності в Україні в умовах війни» (м. Харків, 2025) було спрямоване на усунення цих прогалин у науковій доктрині. Науковець, серед іншого, запропонував кримінологічне визначення кіберзлочинності як «масового, багатофункціонального комунікативно-технологічного феномену, який реалізується через апаратне та програмне забезпечення в просторі комп’ютерних мереж та мереж електрозв’язку (кіберпросторі), із формами прояву, визначеними чинним кримінальним законодавством» [17, с. 112]. Вагому увагу у своєму

дослідженні автор приділив і кримінологічному аналізу російських кібератак проти України в умовах повномасштабної війни.

Окрему групу досліджень складають дослідження, присвячені міжнародному співробітництву у сфері боротьби із кіберзлочинністю. Комплексно відповідне питання було розглянуто у дисертації М.Ю. Яцишин «Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю» (м. Київ, 2019). Науковиця, серед іншого виокремлює основні ознаки кіберзлочинності як об'єкта міжнародно-правового регулювання, до яких відносить її інтелектуальний характер, анонімність та персоналізацію, високий рівень латентності, вартісність, дистанційність, автоматизованість, опосередкованість, віртуалізацію, а також транснаціональність. Достатньо вагому увагу у своїй роботі авторка приділила питання уніфікації норм кримінального процесуального права, що регламентують питання розслідування кримінальних правопорушень, вчинених у кіберпросторі та важливості міжнародного співробітництва у цій сфері. Вона зазначає, що «за допомогою співпраці з кримінально-процесуальних питань у сфері боротьби з кіберзлочинністю встановлюються загальні підходи до визначення юрисдикції у кіберпросторі, визнання і використання електронних доказів, виконання процесуальних дій, зокрема транскордонного доступу до інформації, а також визначаються канали зв'язку між державами. Проблема розподілу суверенних юрисдикцій держав у кіберпросторі вирішується за рахунок застосування критеріїв місцезнаходження інформаційної інфраструктури, локалізації злочинної дії та наслідків, які вона спричинила, а також громадянства злочинця і постраждалої сторони» [164, с. 177].

Крім того, у ході свого наукового дослідження дослідниця звертається до широкого кола питань, пов'язаних із розвитком інституту міжнародного співробітництва, реалізації принципу заборони використання сили у кіберпросторі, удосконалення норм матеріального права у контексті співробітництва у сфері боротьби зі злочинністю, інституційних основ

протидії кіберзлочинності в Україні, а також кібернетичної складової агресії росії проти України.

Зазначені напрями наукового пошуку мають виняткове значення як для теорії, так і для практики, оскільки формують цілісне бачення сучасних викликів у сфері протидії кіберзлочинності на міжнародному рівні. Аналіз розвитку інституту міжнародного співробітництва, принципу заборони застосування сили у кіберпросторі та матеріально-правових механізмів взаємодії держав дозволяє окреслити межі правомірної поведінки суб'єктів міжнародного права в цифровому середовищі. Дослідження інституційних основ протидії кіберзлочинності в Україні та кібернетичної складової агресії росії проти України створює науково обґрунтований базис для адаптації національного законодавства до міжнародних стандартів. Сукупно ці напрацювання закладають міцний фундамент для подальших комплексних досліджень міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю.

Як уже було зазначено, розслідування кримінальних правопорушень у кіберпросторі потребує не лише правових, а й технічних знань. У зв'язку з цим проблематика розслідування таких злочинів досліджується не лише в юридичній доктрині, а й у суміжних галузях знань, зокрема у сфері кібербезпеки. Так, В.А. Сусукайлом було підготовлене дисертаційне дослідження «Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем» (м. Львів, 2024), у якому автор проаналізував існуючі проблеми комплексних систем дослідження кіберзлочинів для інфраструктури інформаційних систем та розглянув сучасні методи побудови систем інформаційної безпеки з використанням підходів DevSecOps, ISMS-методології, технології Blockchain та моделей штучного інтелекту [118].

Отже, аналіз вітчизняного наукового доробку демонструє поетапне, але системне формування наукових підходів до вивчення проблематики розслідування кримінальних правопорушень у кіберпросторі. Початкові

роботи зосереджувалися переважно на питаннях залучення спеціалістів та використання спеціальних знань у сфері комп'ютерних технологій, тоді як подальший розвиток наукової думки спрямовувався на комплексне дослідження криміналістичних, кримінально-процесуальних, кримінологічних та міждисциплінарних аспектів кіберзлочинності.

У більшості досліджень приділено увагу криміналістичній характеристиці кіберзлочинів, методикам їх розслідування, техніко-криміналістичному забезпеченню та використанню спеціальних знань. Водночас, сучасні наукові роботи фокусуються на деталізації методик розслідування конкретних категорій кіберзлочинів, таких як шахрайство в інтернет-комерції, злочини у сфері інтернет-банкінгу та протиправні посягання на інформаційні та платіжні системи. Такий підхід свідчить про усвідомлення необхідності врахування специфіки способів вчинення злочинів, слідової картини та характеристик правопорушника у віртуальному середовищі [148, с. 144].

Натепер основними напрямками дослідження проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі є: 1) наукові дослідження, присвячені криміналістичним проблемам розслідування кримінальних правопорушень, вчинених у кіберпросторі; 2) наукові дослідження, присвячені криміналістичним проблемам розслідування окремих категорій кримінальних правопорушень, вчинених у кіберпросторі; 3) наукові дослідження, які присвячені питанням використання електронних та цифрових доказів у кримінальному процесуальному доказуванні; 4) наукові дослідження, які присвячені питанням використання спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі; 5) наукові дослідження, присвячені питанням кримінологічного аналізу кіберзлочинності та розробки заходів протидії цьому явищу; 6) наукові дослідження, присвячені питанням міжнародно-правового співробітництва у сфері боротьби зі злочинністю; 7) міждисциплінарні дослідження проблем

протидії кіберзлочинності та дослідження протидії кіберзлочинності у межах інших галузей науки.

1.2. Поняття кіберпростору та кримінальних правопорушень, вчинених у кіберпросторі

Характер і контекст нашого дослідження вимагає звернення до питання щодо визначення понять кіберпростору та кримінальних правопорушень, вчинених у кіберпросторі.

Офіційно вважається, що поняття «кіберпростір» уперше було використано Вільямом Ґібсоном у 1982 році в оповіданні «Burning Chrome», а концептуального та міждисциплінарного значення воно набуло після публікації роману Neuromancer у 1984 році. Саме після цього воно було запозичене американською правовою доктриною для позначення особливого соціально-технічного середовища, яке потребує специфічного правового регулювання.

Слід відзначити, що єдиного поняття кіберпростору в американській юридичній доктрині немає і його змістовне наповнення залежить здебільшого від кола наукових інтересів авторів та аспекту, у якому здійснюється дослідження.

Деякі дослідники вважають, що кіберпростір являє собою окреме «місце» або «простір» соціальної та економічної взаємодії. Такий підхід певною мірою спирався на аналогію із фізичним світом, і дозволяв переносити на цифрове середовище категорії територіальності, юрисдикції та кордонів. У такому контексті кіберпростір досліджувався Д. Джонсоном та Д. Постом. У своїй статті «Law and Borders - The Rise of Law in Cyberspace», вони обґрунтовували тезу про принципову відмінність кіберпростору від фізичного світу та необхідність формування автономних правових механізмів його регулювання. Як зазначали дослідники, «межі, що відокремлюють осіб і речі

у віртуальному світі функціонують інакше, однак залишаються юридично значущими. Повідомлення, опубліковані під одним іменем, не впливатимуть на репутацію іншої електронної адреси, навіть якщо обидва повідомлення створені тією самою фізичною особою» [186, с. 1402]. У підсумку, вони доходять висновку, що право як базова цінність збережеться для відносин, що виникають у кіберпросторі, але воно не може бути таким самим правом, яке застосовується до фізичних та географічно окреслених територій.

Подальший розвиток цієї ідеї простежується у наукових працях Л. Лессіґа, у яких кіберпростір розглядається як специфічний простір реалізації конституційних прав і свобод. Дослідник підкреслює, що цифрове середовище формує нові «просторові» умови для здійснення свободи вираження поглядів, права на приватність та інших базових прав людини [200, с. 1408].

Інша американська дослідниця Дж. Коуен зазначає, що кіберпростір не можна зводити виключно до «місця», однак просторове мислення продовжує суттєво впливати на правове регулювання. Кіберпростір, на її думку, є одночасно і простором, і соціально-технічною конструкцією, що формується через практики використання та архітектуру технологій. У своїх роботах вона підкреслює необхідність визнання факту виникнення нового простору, яке сама вона називає мережевим і зазначає, що цей простір проникає у фізичний світ, який є чітко окресленим. Головною проблемою, на думку авторки є те, наскільки цей процес конкретизує і порушує звичну географію влади [197, с. 254].

Інші автори розуміють кіберпростір не як певний альтернативний простір, а як динамічну сукупність протоколів і потоків даних.

У такому ключі здійснював дослідження Дж. Райденберґ, який у статті «Governing Networks and Rule-Making in Cyberspace» аналізував процеси формування правил у мережевому середовищі і дійшов висновку, що регулювання в кіберпросторі здійснюється не лише державами, а й через взаємодію приватних суб’єктів, технічних стандартів та інституцій управління мережею. Зокрема, автор вказує, що «Глобальні мережі структурно

трансформують процеси ухвалення регуляторних рішень. Національні кордони та секторальні межі значною мірою втрачають свою релевантність, натомість, посилюється значення мережевих кордонів і мережевих спільнот. Базове регуляторне формування політики, чи то в межах антиетатистського американського підходу, чи всеохопного європейського підходу, є недостатньо придатним для умов кіберпростору. Натомість має сформуватися нова «парадигма мережевого врядування», покликана визнавати складність центрів регуляторної влади, використовувати нові інструменти політики, зокрема технічну стандартизацію, для досягнення регуляторних цілей, надавати мережам статус напівсуверенних утворень, а також зміщувати роль держави в бік створення системи стимулів для саморегулювання мереж» [193, с. 930].

Схожий підхід простежується й у роботі Д. Поста «Governing Cyberspace», де кіберпростір описується як децентралізована мережа, у якій традиційні ієрархічні моделі влади поступаються горизонтальним механізмам координації та саморегуляції [185, с. 155].

У подальшому, розвиток доктрини кіберпростору пов’язувався із усвідомленням визначальної ролі технічної архітектури у його формуванні. В межах цього підходу кіберпростір розглядається як продукт програмного коду, протоколів і технічних рішень, які фактично виконують регулятивну функцію.

Водночас, деякі ідеї цієї концепції розвивалися і Л. Лессіґом у статті «The Zones of Cyberspace», у якій він запропонував концепцію так званих «зон» кіберпростору, які відрізняються за ступенем відкритості та можливостями контролю. Він доводить, що саме архітектура мережі визначає межі дозволеної поведінки користувачів, а отже, виконує роль «регулятора» не меншою мірою, ніж право [200, с. 1410].

Цей підхід міститься і у праці Дж. Райденберґа «Lex Informatica», де автор вводить поняття «інформаційного права», сформованого через технології. За цією концепцією, правила поведінки в кіберпросторі

встановлюються не лише законами, а й програмним кодом, який визначає можливе і неможливе [194, с. 553].

В межах окремого напрямку американської доктрини кіберпростір розглядається як автономне та самоврядне середовище, де правила поведінки визначають користувачі та окремі актори.

Наприклад, Г. Перрітт у статті «Cyberspace Self-Government» аналізує можливість демократичного самоврядування в кіберпросторі та ставить питання про співвідношення державного регулювання й автономії мережевих спільнот. У роботі, він, зокрема, зазначає, що «інтернет-спільноти повинні розробити принципи, кодекси належної практики або навіть жорсткіші форми правил, сформувати їх за допомогою традиційних договірних механізмів і реально застосовувати через певні форми арбітражу» [190, с. 477]. Власне таку модель функціонування кіберпростору, засновану на договірній моделі автор вважає найбільш прийнятною.

Інший американський дослідник Т. Гарді також обґрунтовує необхідність особливого правового режиму для кіберпростору як нового соціального середовища. Водночас, автор наголошує як на можливості законодавчого регулювання кіберпростору, так і укладення договорів та формуванні звичаїв [191, с.1054].

Слід зауважити, що сьогодні визначення поняття кіберпростору дедалі частіше має нормативне закріплення у різного роду нормативних актах.

Наприклад, у стратегічному документі ЄС «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace» кіберпростір розглядається як «віртуальний простір, в якому «циркулюють» електронні дані світових інформаційно-комунікаційних технологічних мереж» [195].

Поняття кіберпростору є нормативно визначеним і на рівні національного законодавства. У п.11 ч.1 ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України» кіберпростір визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті

функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [97].

Водночас, поняття кіберпростору доволі активно досліджується і у вітчизняній доктрині у наукових працях, присвячених релевантним питанням.

Наприклад, В.А. Фурашев визначає кіберпростір як «форму співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією» [156, с. 164].

У контексті криміналістичного дослідження методики розслідування кримінальних правопорушень, вчинених у кіберпростір О.А. Самойленко визначає кіберпростір як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача [111, с. 23].

В цьому ж ключі, О.Ю. Довженко розглядає кіберпростір як «особливий простір, що створюється за допомогою комп'ютерної техніки та комп'ютерних мереж, який є середовищем, в якому або за допомогою якого здійснюються кіберзлочини, а також відбувається спілкування кіберзлочинців» [29, с. 19].

На підставі наведених доктринальних підходів можна виокремити низку визначальних ознак кіберпростору: 1) кіберпростір є особливою формою співіснування матеріальних і нематеріальних об'єктів та процесів, пов'язаних зі створенням, обробкою та обміном інформацією; 2) він становить інформаційний простір соціальної взаємодії між людьми, що реалізується за допомогою електронних інформаційних технологій; 3) кіберпростір має інфраструктурну основу, яка охоплює Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та цифрові пристрої; 4) функціонування

кіберпростору забезпечується єдиною системою технічних стандартів і протоколів, що уможливлюють перетворення інформації на інформаційний продукт для іншого користувача; 5) кіберпростір виступає специфічним середовищем вчинення та забезпечення кіберзлочинної діяльності, а також комунікації між її учасниками, що має принципове значення для криміналістичного аналізу та методики розслідування кримінальних правопорушень.

Окремо у межах нашого дослідження необхідно звернутись до питання щодо поняття «кримінального правопорушення, вчиненого у кіберпросторі». Безумовно, термінологічної єдності у найменуванні даної категорії кримінальних правопорушень, натепер не існує. На цьому наголошується і у літературі. Зокрема, М.Ю. Яцишин зазначає, що «понятійний апарат, що використовується у процесі міжнародно-правового регулювання протидії кіберзлочинам, постійно розширюється і конкретизується. За рахунок цього як у практиці, так і в доктрині міжнародного права використовуються різноманітні терміни, серед яких, крім поняття «кіберзлочин», поширені такі, як: «комп'ютерні злочини», «інформаційні злочини», «високотехнологічні злочини», «Інтернет-злочини», «злочини у сфері комп'ютерної інформації», «злочини в сфері інформаційних технологій», «кібератака», «кібербезпека», «інформаційна безпека» тощо» [164, с. 22].

Як і поняття кіберпростору, поняття кіберзлочинності на початковому етапі знайшло свій розвиток у американській правовій доктрині.

В юридичній науці США поняття кіберзлочинності розглядається на міждисциплінарному рівні, на перетині кримінального права, теорії інформаційних технологій, а також міжнародного права. Втім, аналіз праць американських учених свідчить про відсутність уніфікованого визначення кіберзлочинності та наявності певного плюралізму концептуальних підходів до її розуміння.

У межах першого підходу кіберзлочинність розглядається як якісно нова форма злочинності, що виникла внаслідок трансформації соціальних відносин

у цифровому середовищі. Представники цього напряму наголошують, що використання комп'ютерних технологій змінює не лише спосіб учинення злочину, а й саму природу кримінально-правового посягання, що ставить під сумнів можливість механічного застосування традиційних норм кримінального права. Прихильником такого підходу є, зокрема, американський вчений Ніл Катял. Він зазначає, що стратегії боротьби як із традиційною злочинністю, так і з кіберзлочинністю може відбуватися за допомогою одних і тих самих стратегій, але водночас, висловлює думку, що правоохоронна система має застосовувати непропорційно суворі санкції до тих, хто вчиняє «соціальний безлад» у кіберпросторі. На його думку, такий підхід дозволить уникнути деяких побічних проблем, зокрема, масового наслідування таких правопорушень, що зумовлене легкодоступністю хакерських інструментів [202, с. 113].

Інші дослідники пов'язують кіберзлочинність із категорією несанкціонованого доступу до комп'ютерних систем і цифрових даних. У межах цього напряму кіберзлочини інтерпретуються як різновид цифрового вторгнення, а ключовим елементом складу злочину визнається порушення меж дозволеного доступу. Такий підхід суттєво вплинув на формування судової практики у США, зокрема щодо тлумачення понять «authorization» та «exceeding authorized access». Так, наприклад, Дж. Голдфут і А. Бамзай пропонують концепцію кіберзлочинності як цифрового аналога кримінального правопорушення проти володіння. Вони доводять, що хакінг слід розглядати як різновид незаконного проникнення, де комп'ютерна система виконує роль «цифрового простору», а порушення технічних бар'єрів - роль фізичного вторгнення [196, с.1498].

Схожого підходу дотримується і О. Керр. На його думку, ключовим елементом більшості кіберзлочинів є порушення меж дозволеного доступу, а не сам факт використання комп'ютерних технологій [203, с. 1666].

Так само, Л. Сачарофф розвиває ідею застосування концепції criminal trespass (незаконне втручання) до комп'ютерних злочинів, але водночас

застерігає від автоматичного перенесення будь-яких фізичних аналогій у цифрове середовище. Він зазначає, що кіберпростір не має чітких меж, а тому й межі криміналізації мають визначатися з урахуванням функціональних, а не територіальних критеріїв [199, с. 645].

Представники іншого наукового напрямку акцентують увагу на транснаціональному характері кіберзлочинності, що зумовлює труднощі у визначенні юрисдикції, збиранні доказів і притягненні винних до відповідальності. У цьому контексті кіберзлочинність розглядається як глобальне явище, яке не підпорядковується класичним територіально-просторовим межам кримінального права. Зокрема, С. Бреннер і Дж. Шверга зазначали, що здобуття цифрових доказів лише у межах національних юрисдикцій залишатиметься складним завданням протягом тривалого часу, а міжнародна співпраця має стати елементом будь-якої стратегії, спрямованої на подолання проблеми кіберзлочинності [205, с. 395].

В межах четвертого підходу кіберзлочинність розглядається як соціально-технічний феномен, де традиційні кримінально-правові заборони доповнюються регуляторними, технічними та організаційними засобами стримування. У цьому контексті важливу роль відіграють інтернет-провайдери та оператори телекомунікацій. Наприклад, А. Кесарі розглядає кіберзлочинність як феномен, який може бути ефективно стриманий не тільки через кримінальне переслідування злочинців, але й активну роль інтернет-провайдерів, платформ і хостинг-компаній у їх запобіганні [198, с. 1131].

Отже, як бачимо, у американській доктрині виробилося чотири ключових підходи до визначення сутності та змісту кіберзлочинності як явища: 1) кіберзлочинність як якісно нова форма злочинності, що виникла внаслідок трансформації соціальних відносин у цифровому середовищ; 2) кіберзлочинність як різновид кримінальних правопорушень, пов’язаних із несанкціонованим доступом до комп’ютерних систем і даних; 3) кіберзлочини як злочини транснаціонального характеру; 4) кіберзлочинність як соціально-технічний феномен, в межах якого традиційні кримінально-правові заборони

доповнюються регуляторними, технічними та організаційними засобами стримування.

Поняття кіберзлочину активно досліджується і розвивається у вітчизняній юридичній доктрині. Зокрема, О.Ю. Довженко визначає кіберзлочин як «особливу форму протиправної поведінки, що, що посягає на охоронювані кримінальним законом суспільні інтереси, та скоюється у кіберпросторі або з використанням можливостей кіберпростору» [29, с. 18].

Ю. Бельський надає наступню дефініцію кіберзлочину – це «злочини, які вчиняються в процесі автоматизованої обробки інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації та інші суспільних відносин, у яких комп'ютер виступає кваліфікуючою ознакою вчинення злочину (наприклад, комп'ютерне шахрайство, або кібертероризм)» [7, с. 417].

На думку М.Ю. Яцишин під кіберзлочином слід розуміти протиправне суспільно небезпечне діяння, здійснене за допомогою інформаційно-комунікаційних технологій проти прав і законних інтересів учасників кіберпростору (фізичних, юридичних осіб, держав та їх об'єднань), що охороняються нормами національного та міжнародного права [164, с. 39].

Незважаючи на широку варіативність визначень кіберзлочину у юридичній доктрині, окремі із них мають недоліки, пов'язані із тим, що вони не включають в себе ознаки кримінального правопорушення, визначені законом України про кримінальну відповідальність. На наше переконання, саме воно має бути першоосновою для формулювання будь-яких дефініцій у цьому контексті.

Зважаючи на це, вважаємо, що під ***кримінальним правопорушенням, вчиненим у кіберпросторі***, слід розуміти *передбачене законом України про кримінальну відповідальність суспільно небезпечне винне діяння, що вчиняється суб'єктом кримінального правопорушення у межах або з використанням кіберпростору як особливого соціально-технічного та*

інформаційного середовища, шляхом застосування інформаційно-комунікаційних технологій, комп'ютерних систем, мереж чи цифрових даних, та посягає на охоронювані кримінальним законом суспільні відносини.

Окремої уваги заслуговує й питання щодо класифікації «кіберзлочинів». Тривалий час основною для правових досліджень була та класифікація, яка закладена у Конвенції про кіберзлочинність, положеннями якої виокремлено: «1) правопорушення проти конфіденційності (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання в систему, зловживання пристроями); 2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство, пов'язане із комп'ютерами); 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією); 4) правопорушення, пов'язані з порушенням авторських та суміжних прав» [50].

Утім, згодом ряд підходів до класифікації кіберзлочинів було сформульовано і у вітчизняній кримінально-процесуальні та криміналістичній доктрині.

О.А. Самойленко пропонує таку класифікацію злочинів, вчинених у кіберпросторі: «1) злочини, вчинені з корисливих мотивів, що пов'язані із фінансово-економічними відносинами у кіберпросторі; 2) злочини, вчинені з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі; 3) злочини, вчинені з політичних мотивів суб'єктів у кіберпросторі; 4) злочини, вчинені з ідейних мотивів» [111, с. 316-317].

О.Ю. Довженко пропонує в межах свого дослідження класифікацію, яка грунтуються на об'єкті / предметі злочину, однак автор визнає, що вона вимагає адаптації до класифікації злочинів за КК України. За такого підходу дослідник пропонує наступну класифікацію кіберзлочинів «1) злочини проти конституційних прав і свобод людини і громадянина (порушення права на особисте та сімейне життя, порушення таємниці листування, порушення авторських і суміжних прав, що скоюються за допомогою комп'ютерних технологій чи мережі Інтернет); 2) злочини проти життя та здоров'я населення,

(використання мережі Інтернет для розповсюдження заборонених чи обмежених у обігу речовин, таких як наркотики, психотропні речовини, ліки); 3) злочини проти честі та гідності особи. (використання комп'ютерних технологій та мережі Інтернет для розповсюдження відомостей, що порочать честь та гідність особи); 4) злочини проти власності (викрадення грошових коштів з банківських рахунків, шахрайство та інші корисливі злочини, що ставлять на меті заволодіти власністю іншої особи з використанням комп'ютерних технологій і мережі Інтернет); 5) злочини в сфері комп'ютерної інформації, (неправомірний доступ до інформації, а також створення та використання шкідливих комп'ютерних програм); 6) злочини проти суспільної моралі (виготовлення, зберігання й поширення порнографії, в тому числі дитячої); 7) злочини проти безпеки держави; 8) злочини терористичного характеру, зокрема заклики до тероризму, фінансування тероризму та безпосередньо акти кібертероризму» [27, с. 22].

Розгалужену систему класифікації кіберзлочинів пропонує І.І. Васильковський, пропонуючи здійснювати її за такими критеріями як масштабність; ступінь соціальної небезпеки; класифікація злочинів, зазначених у КК України; мотивація злочинців; сфера посягання; вид кібератаки; загроза суспільству та державі [11, с. 111-112].

Загалом, у літературі існують й інші підходи до класифікації правопорушень, вчинених у кіберпросторі і цей перелік цих підходів можна було б продовжувати, але й наведені приклади свідчать, що авторські пропозиції здебільшого залежать від предмету наукового пошуку.

Практика останніх років, зокрема, після повномасштабного вторгнення рф демонструє, що чимало правопорушень, можуть вчинятися як у кіберпросторі, та і у традиційному фізичному середовищі. До них належать зокрема й ті діяння, що були криміналізовані законодавцем у відповідь виклики, які виникли у зв'язку із агресією. Прикладом такого кримінального правопорушення може бути правопорушення, передбачене ст. 436^2 КК

України «Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників».

Для цілей нашого дослідження ми пропонуємо класифікацію кримінальних правопорушень, вчинених у кіберпросторі залежно від способу реалізації їх об'єктивної сторони.

До першої групи слід віднести *виключно кіберпросторові кримінальні правопорушення*, об'єктивна сторона яких може бути реалізована виключно в кіберпросторі, серед яких: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК); 2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК); 3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2 КК); 4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК); 5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК).

Кримінальні правопорушення другої групи слід умовно назвати *варіативно-кіберпросторовими*, адже їх об'єктивна сторона може бути реалізована як у фізичному середовищі, так і у кіберпросторі. До таких правопорушень слід віднести: 1) шахрайство (ст. 190 КК України); 2) порушення недоторканності приватного життя (ст. 182 КК України); 3) погроза вбивством (ст. 129 КК України); 4) ввезення, виготовлення, збут і розповсюдження порнографічних предметів (у частині розповсюдження) (ст.

301 КК України); 5) легалізація (відмивання) доходів, одержаних злочинним шляхом (ст. 209 КК України); 6) дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України); 7) колабораційна діяльність (ст. 111^1 КК України); 8) виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436^2 КК України) тощо.

1.3. Забезпечення права особи на повагу до приватного життя у кіберпросторі у практиці Європейського суду з прав людини

Рішення ЄСПЛ мають ключове значення для розвитку та функціонування національної правової системи, оскільки виступають джерелом тлумачення положень Конвенції про захист прав людини і основоположних свобод. Правові позиції, викладені у цих рішеннях, надають конвенційним нормам практичний зміст, формують єдині стандарти захисту прав людини для держав-членів Ради Європи та слугують орієнтиром для національних судів у правозастосуванні.

Суд традиційно керується принципом динамічного тлумачення, що дозволяє адаптувати наявні підходи до змін, зумовлених зокрема науково-технічним прогресом. Це стосується й забезпечення права на повагу до приватного та сімейного життя у цифровому середовищі.

У класичному розумінні, право на повагу до приватного життя, житла та кореспонденції за статтею 8 Конвенції у кримінально-правовому вимірі захищає сферу таємниці спілкування, кореспонденції та недоторканності житла чи іншого володіння. Однак тотальна цифровізація суспільного життя дедалі частіше ставить питання про застосування цих основоположних стандартів у випадках порушень прав людини в онлайн-просторі.

Актуальним питання електронних доказів сьогодні є й для української правової системи. Докази, отримані за допомогою перехоплення повідомлень у месенджерах, електронній пошті у цифрову епоху дедалі частіше визнаються належними у кримінальних провадженнях. В умовах повномасштабного вторгнення та постійних гібридних загроз національній безпеці цей аспект набуває особливого значення. ККС ВС у Постанові від 12 червня 2024 року по справі 569/1908/23 зазначив, що «електронні (цифрові) докази, до яких належать матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), що містяться у відкритих (інтернет, різноманітні засоби масової інформації, соціальні мережі) чи закритих мережах (приватні месенджери та телеграм- канали, особисте листування з використанням комп'ютерної техніки і мобільних телефонів, флешнакопичувачі, карти пам'яті тощо), у яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог процесуального законодавства, є основними доказами у кримінальних провадженнях щодо злочинів проти основ національної безпеки України» [82].

Суд послідовно підкреслює, що будь-яке втручання у цифрову сферу приватного життя повинно відповідати вимогам законності, переслідувати легітимну мету та бути необхідним у демократичному суспільстві, а національне законодавство має передбачати чіткі, передбачувані та ефективні гарантії від зловживань. Водночас, очевидно, що цифрова сфера має власні специфічні особливості. Це визначає потребу детально проаналізувати правові позиції Суду в цьому контексті задля того, щоб адаптувати національне законодавство та практику його застосування до стандартів, закріплених у статті 8 Конвенції.

В межах окресленої проблематики передусім, слід поговорити й про визначення поняття приватного життя. Так, наприклад, В.О. Серьогін визначає право на недоторканність приватного життя (прайвесі) як «соціально зумовлену й гарантовану міру можливої поведінки особи, визначену нормами

об'єктивного права (як національного, так і міжнародного), що полягає в її можливості утримувати під повним контролем (фізичним, психологічним, інформаційним тощо) сферу свого приватного життя. Це право має на меті забезпечити автономію людини у сфері приватного життя для задоволення її власних потреб та інтересів щодо усамітнення та приватного спілкування» [112, с. 97].

З наведеним визначенням слід цілком погодитися, оскільки воно адекватно відображає багатовимірний характер права на приватність, зокрема, його інформаційну складову. В умовах цифровізації саме контроль особи над обігом, збиранням і використанням її персональної та комунікаційної інформації стає ключовим елементом автономії приватного життя. Сучасні цифрові технології істотно розширили можливості втручання у цю сферу, що ще більше підсилює значення приватності як гарантії самовизначення та захисту особистої інформаційної сфери людини.

І.В. Михайленко на підставі проведених наукових досліджень визнає, що поняттю приватного життя доволі складно дати точне та вичерпне тлумачення, оскільки, «по-перше, кожен вміщує в нього власний, індивідуальний зміст, по-друге, неможливо охопити всі сфери його прояву з огляду на сучасний стан і розвиток суспільних відносин. Тому узагальнено приватне життя можна визначити як фізичну й духовну царину, яка формується й контролюється самою людиною, яка є вільною від зовнішнього втручання. Дослідження категорії «приватне життя», змісту, ознак і суб’єктів права на недоторканність приватного життя дозволило зробити висновок, що будь-яка його «рамкова» дефініція буде неповною, можливо, навіть спірною. Це можна пояснити тим, що саме право на приватність не містить чітко сформованого ядра, а об’єднує в собі невизначене коло інтересів, які важко описати одним поняттям» [69, с. 15]. Саме з таких міркувань авторка доходить висновку про те, що давати йому вичерпного визначення й суворо окреслювати його межі недоцільно.

Таке твердження заслуговує на підтримку, принаймні у тому контексті, що приватне життя не має уніфікованого, і чітко формально визначеного змісту. Індивідуалізований характер права на повагу до приватного життя випливає із природи цього права: воно покликане захищати автономію особи, її свободу формувати власну ідентичність, соціальні зв'язки, спосіб життя, комунікацію та інформаційний простір. У цьому сенсі висновок про неможливість охопити всі сфери прояву приватного життя є цілком обґрунтованим, особливо в умовах динамічного розвитку цифрових технологій, коли межі між публічним і приватним доволі сильно перетинаються.

Загалом і практика ЄСПЛ засвідчує наявність випадків, коли Суд визнавав наявність порушення в аспектах, що непрямо випливають зі змісту ст. 8 Конвенції. Наприклад, у справі Sidabras and Džiautas v. Lithuania ЄСПЛ визнав, що заборона займатися певними видами професійною діяльністю вплинула на їх здатність працевлаштуватися та, як наслідок становила порушила їх права на повагу до приватного життя. Мотивуючи своє рішення, Суд зазначив, що «з огляду на тривалий проміжок часу, що минув між розпадом Радянського Союзу (із подальшими політичними трансформаціями в Литві) та набранням чинності у 1999 році оспорюваним Законом, обґрунтовано припустити, що заявники не могли передбачити наслідків, які матиме для них робота в органах державної безпеки. У будь-якому разі ця справа має для заявників значно ширше значення, ніж просто захист їхньої доброї репутації. В очах громадськості вони постають як особи, які в минулому були пов'язані з репресивним режимом. Відтак Суд вважає, беручи до уваги також широкий спектр обмежень у сфері трудової діяльності, яким були піддані заявники, що потенційна шкода для їхнього нормального приватного життя має розглядатися як істотний чинник при вирішенні питання про те, чи підпадають оскаржувані ними обставини під сферу застосування статті 8 Конвенції» [180].

Суд розглядав також можливість охоплення сферою ст. 8 Конвенції такі питання як професійна діяльність вченого [176], зберігання біологічних даних [179], посягання на професійну репутацію судді [174], відеоспостереження в університетській аудиторії [167] тощо.

Передусім, варто зазначити, що пересилання повідомлень електронною поштою у практиці Суду зазвичай підпадає під захист, передбачений статтею 8 Конвенції про захист прав людини та основоположних свобод. У ключовій справі «Барбулеску проти Румунії» ЄСПЛ наголошував, що «не можна вважати, ніби відправляючи електронні листи, заявник автоматично відмовився від свого права на конфіденційність лише через гіпотетичну можливість того, що ці листи можуть бути переслані третім особам або отримані владою. Натомість він мав обґрунтоване очікування того, що конфіденційність його комунікацій буде поважатися та захищатися» [169].

Однією з перших справ, у яких було порушено питання забезпечення права на приватне життя в умовах цифрових технологій та кіберпростору, стала справа «Роман Захаров проти Росії» (Zakharov v. Russia). Заявник стверджував, що російське законодавство про оперативно-розшукову діяльність дозволяло таємне перехоплення його телефонних та електронних комунікацій без належних правових гарантій. Він не стверджував, що саме його комунікації були прослухані, але підкреслював, що сама наявність правового режиму масового перехоплення створює постійну загрозу втручання у приватне життя.

Ключовим питанням у цій справі було відповідність системи SORM, яка надавала російським органам безпеки прямий технічний доступ до мереж операторів зв’язку, вимогам статті 8 Конвенції. Судові дозволи на перехоплення не забезпечували ефективного контролю, оскільки оператори не могли перевірити законність доступу, а особа не інформувалася про втручання навіть постфактум.

ЄСПЛ встановив порушення статті 8, зазначивши, що система перехоплення електронних комунікацій у Росії не відповідала вимогам якості

закону, передбачуваності, пропорційності та ефективного судового контролю. Ця справа стала важливим прецедентом для захисту права на приватність у цифровому середовищі [178].

Одним із ключових рішень у цьому контексті є також справа «Сабо та Віссі проти Угорщини» (Szabó and Vissy v. Hungary). Заявники оскаржували законодавство, яке дозволяло таємне стеження, зокрема доступ до цифрових даних та перехоплення електронних комунікацій, на предмет відповідності стандартам статті 8 Конвенції.

ЄСПЛ підкреслив, що для звернення до Суду не обов'язково доводити факт реального стеження, якщо закон створює реальну загрозу втручання у приватне життя. Суд констатував порушення статті 8, оскільки закон дозволяв перехоплення без індивідуалізації особи та без необхідного зв'язку з реальною загрозою національній безпеці, що фактично відкривало шлях до масового й невибіркового цифрового спостереження. Дозвіл на таємне стеження надавався посадовою особою виконавчої влади, тоді як судового контролю до початку втручання не існувало, що встановило важливий прецедент щодо необхідності незалежного судового санкціонування у цифровій сфері.

Суд також зазначив про порушення щодо необмежених строків перехоплення та відсутності чітких правил зберігання, використання та знищення електронних даних. Загалом, угорська система не забезпечувала належного рівня захисту від свавільного втручання у приватне життя користувачів [181].

Питання відповідності стандартам статті 8 Конвенції у сфері перехоплення електронних комунікацій також розглядалося ЄСПЛ у справі «Centrum för Rättvisa v. Sweden». У цій справі шведська правозахисна організація оскаржувала законність системи масового перехоплення комунікацій, що здійснювала Національна радіотехнічна установа Швеції. Заявники стверджували, що національне законодавство не відповідає вимогам якості закону щодо процедур перехоплення кабельних електронних комунікацій (інтернет-трафік, електронна пошта тощо), збору та

автоматизованої обробки метаданих, а також зберігання й аналізу великих масивів цифрової інформації у сфері національної безпеки та зовнішньої розвідки.

Суд зазначив, що шведське законодавство передбачає певні гарантії від можливих зловживань з боку органів влади. Зокрема, закон забороняє обробку персональних даних на основі раси чи етнічного походження, політичних, релігійних чи філософських переконань, членства у профспілках, стану здоров'я або сексуальної орієнтації. Водночас Суд відзначив, що закон не вимагав враховувати інтереси конфіденційності конкретної особи під час прийняття рішення про обмін інформацією, що становить серйозну прогалину у законодавчому режимі перехоплення комунікацій та є важливим чинником для оцінки його сумісності зі статтею 8 Конвенції (п. 330).

Крім того, Суд підкреслив, що механізм подальшого контролю не був ефективним: зацікавлені особи не мали права отримувати відповіді на свої скарги щодо перехоплення, що могло створювати у них обґрунтоване побоювання свавільного обмеження їхніх прав.

У підсумку ЄСПЛ дійшов висновку, що основні характеристики шведського режиму масового перехоплення відповідали вимогам Конвенції щодо якості закону, і в більшості аспектів цей режим залишався в межах «необхідного у демократичному суспільстві». Проте, наявні недоліки не були належним чином компенсовані існуючими гарантіями, що призвело до того, що режим масового перехоплення виходив за межі дискреційних повноважень держави-відповідача [173].

Безперечно, одним із ключових рішень ЄСПЛ у сфері масового цифрового спостереження є справа «Big Brother Watch and Others v. United Kingdom» [171]. У цій справі заявники оскаржували відповідність Конвенції трьох взаємопов'язаних режимів спостереження у Великій Британії: 1) масового перехоплення електронних комунікацій; 2) отримання комунікаційних даних від провайдерів; 3) обміну розвідувальною інформацією з іноземними спецслужбами.

Як і в попередніх рішеннях, Суд визнав порушення статті 8 Конвенції через відсутність ефективного попереднього судового контролю та недостатньо чіткі правила щодо відбору інтернет-трафіку, застосування пошукових селекторів, зберігання і знищення цифрових даних. Особливо ЄСПЛ звернув увагу на те, що метадані можуть так само відтворювати приватне життя особи, як і сам контент комунікацій, тому до них мають застосовуватися ті самі гарантії захисту приватності.

Водночас, на відміну від попередніх справ, Суд у цій справі вперше розглянув питання виконання процедур обміну інформацією з іноземними спецслужбами. Суд визнав, що такий обмін загалом може відповідати Конвенції, але лише за умови існування адекватних правил перевірки та контролю, яких у британському законодавстві було передбачено недостатньо. Через це, попри загальну можливу сумісність обміну даними, ЄСПЛ констатував порушення статті 8 Конвенції у зв'язку з фактичною відсутністю ефективних гарантій захисту приватності.

У контексті оцінки якості законодавства, що регулює втручання держави у сферу цифрового спілкування, ЄСПЛ неодноразово підкреслював необхідність існування дієвих і достатніх гарантій від свавільного втручання органів влади. Ця проблематика була детально розглянута, зокрема, у справі «Екімджієв та інші проти Болгарії» [175].

У цьому рішенні Суд встановив порушення статті 8 Конвенції, зазначивши, що хоча законодавство Болгарії щодо збереження телекомунікаційних даних та доступу до них було суттєво вдосконалено після рішення Конституційного суду 2015 року та з урахуванням позиції Суду ЄС у справі Digital Rights Ireland, на практиці воно не забезпечує мінімальних гарантій, необхідних для запобігання свавільним діям та зловживанням.

Зокрема, ЄСПЛ вказав на такі недоліки: 1) процедура надання дозволу на доступ до даних не гарантує, що втручання здійснюється виключно за умови його необхідності у демократичному суспільстві; 2) законодавство не визначає чіткі строки зберігання та обов'язкового знищення даних після їх

використання у кримінальних провадженнях; 3) відсутні публічно доступні та зрозумілі правила щодо зберігання, доступу, аналізу, використання, передачі та знищення телекомунікаційних даних органами влади; 4) механізм нагляду не забезпечує ефективної та незалежної перевірки можливих зловживань; 5) процедура повідомлення осіб про втручання у приватне життя є надмірно обмеженою; 6) національне законодавство не гарантує наявності ефективних засобів правового захисту для постраждалих осіб.

Таким чином, Суд констатував, що сукупність зазначених недоліків свідчить про невідповідність болгарської моделі доступу до даних зв'язку вимогам статті 8 Конвенції щодо передбачуваності правового регулювання та належного захисту від свавільного втручання.

ЄСПЛ послідовно наголошує на тому, що судовий контроль має бути основною гарантією від незаконного втручання в приватне електронне спілкування. Водночас така гарантія повинна бути реальною та ефективною [147, с. 359].

У справі «Азер Ахмадов проти Азербайджану» Суд зазначив, що таємне спостереження становить серйозне втручання у право особи на повагу до приватного життя, тому судовий дозвіл, на підставі якого воно здійснюється, не може бути сформульований у розпливчастих або нечітких термінах, що залишають простір для спекуляцій щодо його змісту та, головне, щодо особи, на яку спрямований захід. У цій справі, через відсутність чіткості щодо конкретного номера телефону або чисел, які підлягають спостереженню, а також щодо зв'язку цих номерів із реально підозрюваною особою, використання слова «контакти» у рішенні від 14 березня 2008 року і формулювання всього дозволу в цілому виявилися надто широкими та неточними, що не забезпечувало належного захисту приватності [168].

У контексті належного контролю за доступом до особистих даних користувачів важливе значення мають також висновки ЄСПЛ у справі «Бенедік проти Словенії» [170]. Заявник використовував мережі файлообміну (peer-to-peer, зокрема Razorback) для завантаження та поширення файлів, у

тому числі вмісту, що містив дитячу порнографію, про що було повідомлено швейцарськими правоохоронними органами. Ці органи ідентифікували динамічну IP-адресу, пов'язану з такою діяльністю, і передали цю інформацію словенській поліції.

У серпні 2006 року словенська поліція, не отримавши попереднього судового дозволу, звернулася до місцевого інтернет-провайдера з вимогою надати дані про абонента, пов'язаного з певною динамічною IP-адресою. Провайдер передав ці дані, що дозволило встановити особу заявника, Ігора Бенедіка. Лише після цього поліція, вже на підставі судового дозволу, отримала додаткові трафік-дані та розпочала кримінальне провадження.

Заявник стверджував, що його право на повагу до приватного життя та конфіденційність інтернет-спілкування було порушено через незаконний доступ поліції до інформації про абонента без попереднього судового дозволу. Він також наголошував, що національне законодавство, яке застосовувалося для отримання таких даних, не відповідало вимозі «у відповідності до закону» у розумінні статті 8 Конвенції, а також не забезпечувало достатніх гарантій від свавільного втручання чи надмірного доступу до персональних даних.

Словенський уряд визнавав, що поліція отримувала інформацію для розслідування тяжких злочинів і стверджував, що законодавство дозволяло правоохоронцям запитувати у провайдера дані про абонента. Уряд також наполягав, що такі дії були необхідними для розкриття правопорушень, зокрема, поширення дитячої порнографії.

ЄСПЛ, здійснюючи оцінку, чи було втручання здійснено відповідно до закону, підкреслив, що це передбачає чіткі та передбачувані правові підстави, зрозумілі для особи, яка піддається втручанню. Суд встановив, що норма Кримінального процесуального кодексу Словенії, якою користувалася поліція для отримання даних без судового дозволу, не відповідала цим критеріям: вона не забезпечувала чіткої прив'язки між динамічною IP-адресою та даними абонента, фактично не містила гарантій проти свавільного втручання та не передбачала ефективного незалежного контролю.

Суд також зазначив, що навіть якщо динамічна IP-адреса була доступна іншим користувачам, для ідентифікації конкретного абонента необхідна додаткова інформація від провайдера, і така діяльність за своєю природою має високий рівень анонімності, який підпадає під захист приватного життя.

У підсумку ЄСПЛ дійшов висновку, що дії словенських правоохоронців не відповідали вимозі «відповідно до закону», а держава не забезпечила належних гарантій від свавільного втручання.

Висновки, до яких дійшов Суд у цій справі вкотре наголошують на необхідності удосконалення національних процедур доступу до даних користувачів інтернет-послуг, особливо в кримінальних провадженнях, а також забезпечення ефективного судового нагляду та пропорційності втручання. Практично воно закріплює принцип, що доступ до персональних даних без належних гарантій порушує право на приватне життя, навіть якщо втручання спрямоване на розкриття тяжких злочинів, і слугує орієнтиром для законодавців та судів у цифрову епоху. Слід зауважити, що вітчизняне законодавство цьому стандарту відповідає, зокрема, відповідно до п.7 ч.1 ст. 162 КПК України інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв’язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо відноситься до охоронюваної законом таємниці, що передбачає доступ до неї виключно на підставі ухвали про тимчасовий доступ до речей і документів.

В цілому, ці висновки Суду формують достатньо чіткий орієнтир для національних правових систем: релевантне законодавство має гарантувати баланс між національною безпекою і правом на приватність, передбачати пропорційні обмеження і ефективні механізми контролю, щоб не підривати саму сутність права на приватне життя у цифровому середовищі.

Натомість, у справі «Брейєр проти Німеччини» заявники оскаржували положення німецького законодавства, згідно з яким оператори телекомунікацій зобов’язані збирати та зберігати персональні дані

користувачів передплачених (pre-paid) SIM-карток - включно з іменем, адресою проживання та номером телефону, навіть якщо ці дані не були необхідні для виставлення рахунків чи інших договірних цілей [172].

Заявники стверджували, що зберігання та можливе надання таких даних державним органам становило втручання у їхнє право на повагу до приватного життя та кореспонденції, гарантоване статтею 8 Конвенції.

Здійснюючи оцінку того, чи було втручання здійснено відповідно до закону, Суд встановлює, що зберігання персональних даних заявників під час придбання SIM-карт мобільного зв'язку здійснювалося на підставі § 111 Закону про телекомунікації, який у частині обсягу збережених даних був достатньо чітким і передбачуваним. Крім того, строк зберігання був чітко врегульований, а технічні аспекти зберігання - принаймні після видання відповідного регламенту й технічної директиви - достатньо конкретизовані.

Уряд держави-відповідача стверджував, що втручання переслідувало легітимні цілі громадської безпеки, запобігання заворушенням чи злочинам та захисту прав і свобод інших осіб. ЄСПЛ також звернув увагу на пояснення Федерального конституційного суду про те, що доступ до збереженої інформації здійснюється «з метою відвернення небезпек, переслідування кримінальних правопорушень чи адміністративних проступків та виконання завдань розвідувальних органів». Ці цілі також відображені у Законі про телекомунікації.

Суд погодився із тим, що обов'язкова реєстрація абонентів значно полегшує розслідування та сприяє запобіганню злочинам, і що можливість обходу таких правил не нівелює їх загальної користі. З огляду на відсутність консенсусу між державами-членами, Німеччина мала певну межу розсуду. Водночас, ЄСПЛ відзначив, що обсяг втручання був обмеженим: зберігалися лише базові ідентифікаційні дані, без інформації про дзвінки, місцезнаходження чи побудову профілів особи, тому втручання було відносно незначним. Окремо було звернено увагу на те, що строки зберігання, технічні гарантії, обмеження доступу, вимога наявності правової підстави (концепція

«подвійних дверей») та критерій необхідності забезпечують належний рівень захисту від зловживань, а система контролю, включно з наглядом органів із захисту даних та можливістю судового оскарження, забезпечила ефективний незалежний перегляд законності доступу до даних.

Зрештою Суд дійшов висновку, що зберігання персональних даних заявників відповідно до § 111 Закону про телекомунікації було пропорційним і «необхідним у демократичному суспільстві», а державою не було перевищено меж допустимого втручання. Відтак, було констатовано відсутність порушення ст. 8 Конвенції.

Із рішення у справі «Breyer v. Germany» випливає низка важливих для національної правової системи та правозастосування висновків. Насамперед Суд чітко підтвердив, що навіть зберігання базових ідентифікаційних даних абонентів телекомунікацій становить втручання у приватне життя, а отже потребує виправдання за статтею 8 Конвенції. Це означає, що законодавець не може розглядати такий масив даних як «технічно нейтральний» або незначущий. Водночас рішення демонструє, що загальне зобов'язання з ідентифікації користувачів може відповідати Конвенції, якщо воно ґрунтується на чіткій, доступній і передбачуваній нормі закону та супроводжується достатньою системою гарантій.

Важливе значення для сучасного розуміння забезпечення права на повагу до приватного життя у цифровому середовищі мають висновки ЄСПЛ у справі «Подчасов проти росії» [177]. У ній, заявник, Владислав Подчасов, був адміністратором та власником месенджер-сервісу Telegram Passport (у межах екосистеми Telegram), у якого російські органи безпеки вимагали надати криптографічні ключі, які дозволяли б розшифровувати приватні повідомлення користувачів месенджера.

Ця вимога ґрунтувалася на положеннях так званого «пакета Ярової» – змін до російського законодавства, які зобов'язували постачальників електронних комунікацій: зберігати повідомлення, надавати ФСБ доступ до змісту комунікацій, передавати ключі дешифрування.

Заявник відмовився надавати таку інформацію, стверджуючи, що: технічно неможливо надати ключі для end-to-end шифрування, вимога зруйнувала б систему захисту всіх користувачів.

У контексті зберігання ІСО інтернет-комунікацій та пов'язаних з ними даних Суд зазначив, що саме зберігання даних, які стосуються приватного життя особи, вже є втручанням у значенні статті 8 Конвенції. Подальше використання збереженої інформації не впливає на цей висновок. Проте при визначенні, чи зачіпає збережена персональна інформація різні аспекти приватного життя, Суд враховує конкретний контекст збору та зберігання інформації, характер записів, спосіб їх використання та обробки, а також можливі наслідки. На підставі цього Суд дійшов висновку, що безперервне зберігання інтернет-комунікацій та пов'язаних даних, потенційний доступ органів влади до цих даних та обов'язок розшифровувати їх, якщо вони зашифровані, за законом про інформацію та відповідними нормативами, становлять втручання у права заявника за статтею 8.

Національне законодавство передбачало безперервне автоматичне зберігання всіх інтернет-комунікацій протягом 6 місяців та пов'язаних даних протягом 1 року. Це стосувалося всіх користувачів і не вимагало наявності підозри у вчиненні кримінального правопорушення. Суд вважає таке втручання надзвичайно широким та серйозним.

Крім того, вимога надавати доступ без перевірки та авторизації створює високий ризик зловживань. Закон не передбачає необхідності показати дозволи суду постачальнику послуг, що суперечить стандартам таємного спостереження. Стосовно обов'язку розшифровувати повідомлення, Суд зазначив, що розшифровка end-to-end шифрованих повідомлень призвела би до послаблення шифрування для всіх користувачів, що є непропорційним легітимним цілям, натомість повинні розглядатися альтернативні методи без ослаблення шифрування.

У підсумку, Суд дійшов висновку, що законодавство про зберігання всіх інтернет-комунікацій, прямий доступ служб безпеки без гарантій та обов'язок

розшифровки end-to-end повідомлень не є необхідними у демократичному суспільстві. Воно підриває саму сутність права на приватне життя і перевищує допустиму межу втручання.

Висновки ЄСПЛ у справі «Подчасов проти Росії» мають принципове значення для національних правових систем і правозастосування у цифрову епоху. Вони підкреслюють, що будь-яке автоматичне зберігання даних про інтернет-комунікації вже є втручанням у право на приватне життя незалежно від того, чи використовуються ці дані. Це означає, що національне законодавство, що регулює зберігання персональних даних, повинно чітко визначати обсяг, строки та умови доступу до таких даних.

Крім того, Суд звернув увагу на необхідність ефективних та пропорційних гарантій проти зловживань, включно з судовим контролем доступу до даних та обмеженням використання. У національних правових системах повинні бути передбачені прозорі процедури, незалежний контроль та можливість оскарження дій органів влади, щоб не допустити свавільного втручання.

І насамкінець, рішення підкреслює важливість збереження технічних засобів захисту, таких як end-to-end шифрування, та заборону непропорційного ослаблення безпеки користувачів. Для національного законодавства це означає, що зобов’язання постачальників послуг щодо розшифровки комунікацій повинні бути технічно обґрунтовані та обмежені конкретними особами, а не застосовуватися масово.

Аналіз практики ЄСПЛ свідчить про формування цілісної та послідовної системи стандартів захисту права на повагу до приватного життя у кіберпросторі, яка базується на положеннях статті 8 Конвенції та принципі верховенства права. Суд, застосовуючи динамічне тлумачення Конвенції, адаптує класичні підходи до оцінки втручання у приватне життя до умов цифровізації, визнаючи, що електронні комунікації, метадані та інші цифрові сліди особи можуть розкривати різні аспекти її приватного та сімейного життя не меншою мірою, ніж традиційні форми кореспонденції.

У розглянутих рішеннях ЄСПЛ послідовно наголошується, що сама наявність законодавчого режиму, який допускає таємне або масове втручання у цифрове спілкування, може розцінюватися як втручання у право на повагу до приватного життя. Важливим є не лише формальне існування правового регулювання, а його «якість», що передбачає достатню чіткість, передбачуваність і наявність ефективних гарантій від свавілля [154, с. 634].

Зокрема, узагальнений аналіз практики дозволяє виділити мінімальні гарантії захисту права на повагу до приватного та сімейного життя у кіберпросторі відповідно до вимог статті 8 Конвенції: 1) чітке законодавче визначення категорій осіб та даних, щодо яких можливе перехоплення; 2) наявність попереднього судового контролю або ефективного подальшого нагляду за спостереженням; 3) нормативне формулювання критеріїв, за якими ухвалюється рішення про ініціювання перехоплення; 4) обмеження строків зберігання даних та встановлення чіткого порядку їх знищення.

1.4. Міжнародні стандарти та зарубіжний досвід регламентації розслідування кримінальних правопорушень, вчинених у кіберпросторі

У сучасних умовах стрімкої цифровізації всіх сфер суспільного життя міжнародні стандарти розслідування кримінальних правопорушень, учинених у кіберпросторі, набувають визначального значення для забезпечення ефективної протидії таким діянням.

У кримінально-процесуальній, криміналістичній і кримінологічній доктрині майже загальновизнаною є така іманентна ознака кіберзлочинів як їх транскордонний характер. Сервери, потерпілі, а також особи, підозрювані чи обвинувачені у вчиненні таких правопорушень, можуть перебувати в різних державах, що робить виключно національні правові механізми кримінального переслідування недостатніми. У зв’язку з цим узгодження правової політики

щодо розслідування цієї категорії злочинів на основі міжнародних стандартів є необхідною умовою подолання конфліктів юрисдикцій і формування спільних підходів до здійснення кримінального переслідування.

Більшість міжнародних стандартів у цій сфері спрямована на уніфікацію кримінально-правових підходів. Зокрема, міжнародні документи закріплюють поняття кіберзлочинів, визначають мінімальні вимоги до їх криміналізації та основні підходи до кваліфікації відповідних діянь. Водночас кримінально-процесуальні аспекти розслідування злочинів у кіберпросторі також мають суттєве нормативне підґрунтя, оскільки транскордонний характер таких правопорушень зумовлює потребу у використанні механізмів міжнародної правової допомоги, обміну інформацією та отримання доступу до даних, що перебувають у розпорядженні іноземних провайдерів.

За останні двадцять років було ухвалено низку міжнародно-правових документів, спрямованих на розвиток міждержавного співробітництва у сфері протидії кіберзлочинності. Як зазначає М. Ю. Яцишин, «для сучасного етапу формування інституту міжнародно-правового співробітництва у цій галузі характерними є його регіоналізація та посилення процесів уніфікації національних правових систем» [164, с. 41]. Такий висновок, зокрема, обґрунтовується відсутністю універсальних міжнародних договорів, що комплексно регулювали б відповідну сферу.

У межах Ради Європи ключовим міжнародним актом, який встановлює основи взаємодії держав у боротьбі з кіберзлочинністю, є Конвенція Ради Європи про кіберзлочинність від 21 листопада 2001 року (Будапештська конвенція) та Додатковий протокол до неї від 28 січня 2003 року.

Друга частина розділу II Будапештської конвенції, поіменована «Процедурне право», закріплює мінімальні стандарти щодо законодавчих та інших заходів, необхідних для здійснення конкретних кримінальних розслідувань і кримінального переслідування. Згідно з підпунктом «с» пункту 2 статті 14 Конвенції, «встановлені правила і процедури поширюються,

зокрема, на збирання доказів у електронній формі у межах кримінального провадження» [50].

Серед процесуальних заходів, які держави-учасниці можуть застосовувати з метою забезпечення ефективного розслідування кіберзлочинів, Конвенція передбачає: «термінове збереження збережених комп'ютерних даних (ст. 16); термінове збереження та часткове розкриття даних про рух інформації (ст. 17); обшук і вилучення збережених комп'ютерних даних (ст. 19); збір даних про рух інформації в режимі реального часу (ст. 20), а також перехоплення даних змісту повідомлень (ст. 21)». Окрім цього, Будапештська конвенція встановлює загальні засади міжнародного співробітництва, зокрема механізми взаємної правової допомоги під час розслідування кримінальних правопорушень у кіберпросторі.

Не менш важливе значення у контексті міжнародного співробітництва має також Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи стосуються криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [30]. У документі, серед іншого визначено поняття дій «расистського або ксенофобного характеру» як «будь-якого письмового матеріалу, будь-якого зображення чи будь-якого іншого представлення ідей або теорій, які захищають, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій».

У статті 4 Додаткового протоколу встановлено, що кожна Сторона зобов'язується вжити таких законодавчих та інших заходів, які є необхідними для того, щоб у її національному праві визнавалися кримінальними правопорушеннями, за умови умисного вчинення без належних на те підстав, такі дії, як погроза, здійснена за допомогою комп'ютерної системи, вчинення

тяжкого злочину, визначеного національним законодавством, спрямована проти: 1) окремих осіб з огляду на їх належність до групи, що відрізняється за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, коли ці ознаки використовуються як привід для таких дій; 2) групи осіб, яка характеризується будь-якою з перелічених ознак.

Будапештська конвенція про кіберзлочинність і її Додаткові протоколи мають фундаментальне значення для національної правової системи, оскільки формують універсальну правову рамку реагування на злочини, що вчиняються у цифровому середовищі. Вона не лише уніфікує підходи до криміналізації основних видів кіберзлочинів, а й регламентує сучасні процесуальні механізми збирання, збереження та використання електронних доказів. Для національного кримінального процесу це відкриває можливість адаптації традиційних засобів доказування до специфіки цифрових даних, які є нестійкими, легко змінюваними та часто перебувають за межами державної юрисдикції. Особливо важливою є роль Конвенції у забезпеченні міжнародного співробітництва, адже більшість кіберзлочинів має транскордонний характер. Завдяки встановленим стандартам взаємної правової допомоги та термінового збереження даних держава отримує реальні інструменти для забезпечення ефективного розслідування кримінальних правопорушень, вчинених у кіберпросторі. Водночас Конвенція закладає баланс між інтересами кримінального переслідування та захистом прав людини, зокрема права на приватність.

На рівні права ЄС міжнародне співробітництво у сфері розслідування кримінальних правопорушень, учинених у кіберпросторі, врегульовується передусім двома ключовими нормативними актами: 1) Директивою (ЄС) 2022/2555 Європейського парламенту та Ради від 14 грудня 2022 року про заходи із забезпечення високого спільного рівня кібербезпеки в межах Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 і скасування Директиви (ЄС) 2016/1148 (так звана Директива NIS 2) (далі – Директива (ЄС) 2022/2555) [187]; 2) Регламентом (ЄС) 2023/1543

Європейського парламенту та Ради від 12 липня 2023 року «Про Європейські накази про подання та збереження електронних доказів у кримінальному провадженні та для виконання покарань у вигляді позбавлення волі після завершення кримінального провадження» (далі – Регламент (ЄС) 2023/1543) [204].

Директива (ЄС) 2022/2555 містить розділ VI «Обмін інформацією», у якому визначено засади співпраці у сфері кібербезпеки. Зокрема, стаття 29 встановлює обов'язок держав-членів забезпечити можливість для суб'єктів, що підпадають під дію цієї Директиви, а також, за потреби, інших заінтересованих осіб добровільно здійснювати взаємний обмін релевантною інформацією з питань кібербезпеки. Такий обмін може охоплювати відомості про кіберзагрози, уразливості та недоліки систем, застосовувані методи й процедури, дані про суб'єктів загроз, попередження щодо кіберінцидентів, а також рекомендації з налаштування інструментів кіберзахисту для виявлення атак.

Відповідно до Директиви, обмін інформацією має здійснюватися за умови, що він: а) спрямований на запобігання інцидентам, їх виявлення, реагування або відновлення після них чи на мінімізацію їх наслідків; б) сприяє підвищенню загального рівня кібербезпеки, зокрема шляхом зростання обізнаності щодо загроз, обмеження або унеможливлення їх поширення, підтримки оборонних спроможностей, виявлення та усунення вразливостей, удосконалення методів виявлення, стримування і запобігання атакам, розроблення стратегій пом'якшення наслідків та процедур реагування і відновлення, а також через заохочення спільних досліджень кіберзагроз між державними та приватними суб'єктами.

Найбільш дотичним до кримінального процесу є Регламент (ЄС) 2023/1543. У пункті 23 цього акта зазначено, що, оскільки процедури взаємної правової допомоги в державах-членах можуть розглядатися як різновид кримінального провадження за їхнім національним правом, необхідно чітко розмежувати ці механізми. Зокрема, Європейський наказ про надання

електронних доказів або Європейський наказ про збереження не можуть використовуватися для надання взаємної правової допомоги іншій державі-члену чи третій країні. У таких ситуаціях запит має адресуватися відповідній державі, яка надає правову допомогу відповідно до власного національного законодавства. Водночас, у межах власне кримінального провадження зазначені європейські накази можуть видаватися лише щодо конкретного кримінального провадження і конкретного вже вчиненого кримінального правопорушення, за умови проведення в кожній справі індивідуальної оцінки їх необхідності та пропорційності з урахуванням прав підозрюваного або обвинуваченого (п. 24 Регламенту).

Регламент також приділяє значну увагу стандартам захисту приватного життя у процесі розслідування кіберзлочинів. Так, у пункті 33 встановлено, що коли IP-адреси, ідентифікатори доступу та пов'язана з ними інформація запитуються не лише з метою встановлення особи користувача у конкретному кримінальному провадженні, а для ширших цілей, зазвичай повинні витребовуватися і більш чутливі відомості, зокрема дані про контакти та місцезнаходження користувача. Такі відомості дають змогу сформувати детальний профіль особи, хоча їх технічно простіше обробляти та аналізувати, ніж дані про зміст повідомлень, оскільки вони мають структурований і стандартизований характер. Саме тому Регламент вимагає, щоб у подібних випадках IP-адреси, номери доступу та пов'язані з ними дані, які не використовуються виключно для ідентифікації користувача в межах конкретного розслідування, кваліфікувалися як дані про трафік і запитувалися за тим самим правовим режимом, що й дані про зміст.

Регламент також охоплює ситуації, у яких запитувані дані перебувають під захистом імунітетів або привілеїв, передбачених правом окремих держав-членів. Згідно з пунктом 48, якщо орган, що має намір видати Європейський наказ, запитує дані про трафік і має обґрунтовані підстави вважати, що такі відомості охороняються імунітетами чи привілеями за правом держави-виконавця або підпадають під її правила щодо свободи преси чи свободи

вираження поглядів у медіа, він повинен мати можливість попередньо звернутися за роз'ясненнями перед видачею наказу. Такі консультації можуть здійснюватися з компетентними органами держави-виконавця безпосередньо або за посередництва Євроюсту чи Європейської судової мережі.

У системі актів права ЄС, що регулюють розслідування кримінальних правопорушень у кіберпросторі, окреме значення має також Резолюція Європейського парламенту від 3 жовтня 2017 року «Про боротьбу з кіберзлочинністю» (2017/2068(INI)) (2018/C 346/04). У цьому документі наголошується на потребі вироблення спільних процесуальних стандартів, які враховували б територіальний вимір кіберзлочинності та визначали б слідчі заходи, що можуть застосовуватися незалежно від державних кордонів [189].

Зазначимо, що окремі документи у сфері протидії кіберзлочинності були прийняті в межах інших регіональних систем захисту прав людини. Однією із них є Конвенція Ліги арабських держав про боротьбу зі злочинами у сфері інформаційних технологій (Arab Convention on Combating Information Technology Offences) [166] - регіональний міжнародний договір, прийнятий у грудні 2010 р. у Каїрі в межах Ліги арабських держав та спрямований на узгодження кримінальної політики держав-учасниць у сфері боротьби з кіберзлочинністю, посилення співробітництва та захисту суспільної безпеки від загроз, пов'язаних із інформаційними технологіями.

Конвенція встановлює загальні зобов'язання держав-учасниць щодо попередження, розслідування та переслідування злочинних діянь у сфері інформаційних технологій (незаконний доступ, перехоплення або зміна даних, знищення інформації тощо), включно з тими, що мають транснаціональний характер.

Основною метою документу є, передусім, гармонізація кримінально-правової політики у сфері боротьби із кіберзлочинами. Конвенція спрямована на узгодження визначень злочинів та підходів до їхнього розслідування серед арабських держав для уніфікації правових стандартів у регіоні і зобов'язує Держави учасниці внести до національного законодавства норми, що

визнають перелік кіберзлочинів як правопорушення з відповідними санкціями.

Однак, водночас, Конвенція містить положення про співробітництво щодо збирання доказів і кримінального переслідування. Передусім, мова йде про розширення юрисдикції. За Конвенцією Держави зобов'язуються адаптувати компетенцію національних органів для охоплення транскордонних злочинів та забезпечити можливість здійснення кримінального переслідування, коли правопорушник чи наслідки злочину охоплюють кілька держав-учасниць.

Крім того, у Конвенції закріплені механізми видачі осіб, які вчинили кіберзлочини, навіть за відсутності двостороннього договору, якщо ці діяння караються позбавленням волі не менше року в обох державах; Конвенція може виступати як правова основа для видачі.

Основними механізмами взаємної юридичної допомоги за Конвенцією є передача запитів між центральними органами, обмін інформацією, доказами, документами, матеріальними та цифровими даними, без вимоги подвійної криміналізації, якщо це передбачено Конвенцією. Водночас, документ забезпечує можливість дотримання конфіденційності запитаної інформації та її використання виключно в межах кримінального розслідування.

Таким чином, Конвенція Ліги арабських держав про боротьбу зі злочинами у сфері інформаційних технологій є ключовим регіональним документом, що забезпечує гармонізацію кримінально-правової політики держав-учасниць у сфері кіберзлочинності. Вона встановлює єдині стандарти визначення кіберзлочинів, зобов'язує адаптувати національне законодавство, а також сприяє ефективному міжнародному співробітництву щодо збирання доказів та кримінального переслідування. Конвенція розширює юрисдикцію на транснаціональні злочини, передбачає механізми видачі осіб і обмін цифровими та матеріальними даними, встановлюючи при цьому гарантії забезпечення конфіденційності інформації.

Ще одним документом регіонального характеру у сфері боротьби із кіберзлочинністю є Конвенція Африканського Союзу про кібербезпеку і захист персональних даних (African Union Convention on Cyber Security and Personal Data Protection) [165], також відома як Малабоська конвенція.

Основною метою Конвенції проголошено створення правового та безпекового середовища для розвитку цифрового суспільства в Африці, яке забезпечує повагу фундаментальних прав людини, у тому числі права на приватність, водночас сприяючи поширенню інформаційно-комунікаційних технологій та електронної комерції. У Документі наголошується на необхідності гармонізації національних законодавств відповідно до найкращих міжнародних практик.

Значна частина Конвенції присвячена криміналізації дій, пов'язаних з інформаційно-комунікаційними технологіями, зокрема, несанкціонованого доступу до систем, перешкоджання функціонуванню комп'ютерних систем, цифрових порушень даних та розповсюдження шкідливого контенту, такого як дитяча порнографія. Конвенція зобов'язує держави закріпити у національному законодавстві ці правопорушення та передбачити ефективні санкції.

Доволі суттєвою особливістю цього міжнародного документу є вимога адаптації національного законодавства у частині криміналізації «традиційних» злочинів до цифрового середовища. Іншими словами, Конвенція вимагає, щоб окремі норми кримінального права, які встановлюють відповідальність за деякі традиційні злочини (наприклад, шахрайство, розкрадання, відмивання грошей) враховували можливість використання інформаційно-комунікаційних технологій як спосіб вчинення злочину.

Конвенція містить й низку стандартів процесуального характеру. Зокрема, її положення встановлюють, що держави-члени повинні забезпечити правову основу для отримання доступу до інформації, яка зберігається в електронних системах, включно з: 1) обліковими записами користувачів у сервісах електронної пошти та соціальних мережах; 2) даними про трафік та

метаданими; 3) інформацією, що зберігається на серверах, хмарних платформах та мобільних пристроях.

Важливим є те, що Конвенція передбачає чіткі стандарти для будь-яких процесуальних дій із цифровими доказами. Зокрема, за Конвенцією правоохоронні органи можуть проводити пошук та вилучення даних лише у межах конкретного кримінального провадження; копіювання інформації має здійснюватися без зміни оригінальних даних, щоб забезпечити цілісність доказів, а також передбачена необхідність документування процедур вилучення, задля забезпечення можливості оскарження дій.

Що цікаво, Малабоська Конвенція чи не єдиний міжнародний документ у сфері боротьби із кіберзлочинністю, який містить положення щодо попереднього санкціонування дій зі збирання цифрових доказів. Зокрема, у п.4 ст. 10 Конвенції наголошено, що виключно після отримання дозволу національного органу із захисту даних можуть бути здійснені такі дії як: 1) обробка персональних даних, що включає генетичну інформацію та дані, пов'язані із дослідженнями у сфері охорони здоров'я; 2) обробка персональних даних, що включає інформацію про правопорушення, судимості або заходи безпеки; 3) обробка персональних даних з метою взаємоз'єднання (інтерконекції) файлів, а також обробка даних що включає ідентифікаційний номер або будь-який інший ідентифікатор того самого типу; 4) обробку персональних даних, що включає біометричні дані; 5) обробка персональних даних, що становлять суспільний інтерес, зокрема, для історичних, статистичних або наукових цілей.

У ст. 16 Конвенції також наголошено на тому, що при обміні даними з іншими державами, конвенція зобов'язує забезпечувати збереження конфіденційності та цілісності переданих даних, використовуючи за потреби шифрування та суворі умови доступу, і обмежувати їхнє застосування виключно у межах цілей кримінального переслідування чи розслідування.

У цьому контексті Малабоська Конвенція Африканського Союзу є вдалим прикладом дотримання балансу між захистом фундаментальних прав людини, зокрема права на приватність, із протидією кіберзлочинності.

Отже аналіз регіональних міжнародних документів у сфері боротьби із кіберзлочинністю дозволяє стверджувати, що у переважній більшості відповідні акти містять норми як матеріально-, так і процесуально-правового характеру. Серед процедурних стандартів розслідування кіберзлочинів, які є спільними для усіх регіональних систем захисту прав людини слід виокремити наступні: 1) обов'язок держав запровадити чітку правову основу для отримання доступу до інформації, яка зберігається в електронних системах; 2) зобов'язання держав адаптувати компетенцію національних органів і включити до неї переслідування транскордонних злочинів, а також забезпечити можливість здійснення кримінального переслідування, коли правопорушник чи наслідки злочину охоплюють кілька держав-учасниць; 3) здійснення правоохоронними органами пошуку та вилучення виключно у межах конкретного кримінального провадження із забезпеченням оригінальності вилучених даних, цілісності доказів, а також обов'язковим документуванням відповідних правових процедур; 4) забезпечення можливості екстрадиції осіб, які вчинили кіберзлочини; 5) визначення основних видів міжнародно-правової допомоги при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі, серед яких: передача запитів між центральними органами, обмін інформацією, доказами, документами, матеріальними та цифровими даними, у т.ч. без вимоги подвійної криміналізації; 6) забезпечення конфіденційності інформації, отриманої у межах міжнародно-правової допомоги; 7) необхідність санкціонування компетентним органом процесуальних дій, які передбачають втручання у приватне життя осіб.

Окремо в межах нашого дослідження слід розглянути питання регламентації розслідування кіберзлочинів у межах національних юрисдикцій.

У США діє низка нормативних актів, які визначають федеральні правила та процедури доступу до електронних доказів. Одним із базових у цій сфері є закон 18 U.S.C. § 1030 - Computer Fraud and Abuse Act (CFAA) [182], який передбачає кримінальну й цивільну відповідальність за несанкціонований доступ до комп'ютерів та пов'язані з цим зловживання. У ньому закріплено перелік конкретних діянь, що визнаються кримінальними правопорушеннями у сфері незаконного доступу до інформаційних систем, зокрема незаконне отримання інформації, комп'ютерне шахрайство, заподіяння шкоди комп'ютерним системам, торгівля засобами доступу (паролями, кодами), а також вимагання, пов'язане з комп'ютерною шкодою. Закон також містить правило екстериторіальної дії, за яким він застосовується, зокрема, у випадках, коли шкода завдана комп'ютеру, що знаходиться у США, незалежно від місця перебування особи, яка вчинила правопорушення.

Іншим важливим федеральним актом, який модернізував регулювання приватності електронних комунікацій в умовах цифровізації, є Electronic Communications Privacy Act (ECPA) 1986 року [188]. Цей закон закріплює загальний принцип судового контролю за доступом до комунікацій та встановлює різні правові режими отримання правоохоронними органами абонентських і комунікаційних даних.

У Великій Британії також існує низка спеціальних законів, що регламентують розслідування злочинів у кіберпросторі. Ключовим серед них є Computer Misuse Act 1990 [183], який криміналізує такі діяння, як несанкціонований доступ до комп'ютерних систем і даних, незаконне знищення, пошкодження чи перешкоджання роботі комп'ютерів, а також створення або використання інструментів для вчинення таких правопорушень.

Водночас основним актом, що визначає процесуальні засади доступу до цифрових даних у межах розслідувань, є Investigatory Powers Act 2016 (IPA) [192], який формує правову основу для втручання у цифрові системи та запроваджує судовий контроль за наданням відповідних дозволів.

Відповідно до положень IPA у Великій Британії впроваджено посадову особу Державного секретаря, який наділений повноваженнями вимагати від оператора телекомунікацій зберегти певні дані, якщо вважає, що така вимога є необхідною та пропорційною для однієї або кількох цілей визначених законом. Зокрема, таке «повідомлення про збереження» може: 1) стосуватися конкретного оператора або будь-якої категорії операторів; 2) вимагати зберігання усіх даних або певної категорії даних; 3) визначати строк або строки, протягом яких дані мають зберігатися; 4) містити інші вимоги або обмеження щодо зберігання даних; 5) передбачати різні положення для різних цілей; 6) стосуватися даних незалежно від того, чи існували на момент надання повідомлення або набрання ним чинності.

Однак закон містить низку обмежень щодо меж, у яких може бути затребувано збереження даних. Зокрема, повідомлення про зберігання не може вимагати від оператора, який контролює або надає телекомунікаційна послуги зберігати дані, які стосуються використання телекомунікаційної послуги, наданої іншим оператором телекомунікацій.

Водночас, релевантне законодавство містить низку гарантій ід свавілля у контексті надання наказів про збереження. Зокрема, ст. 90 Закону IPA передбачає, що перед наданням повідомлення про збереження даних, Державний секретар зобов’язаний враховувати низку факторів та обставин, серед яких: 1) ймовірна користь такого повідомлення; 2) ймовірна кількість користувачів (якщо вона відома) будь-якої телекомунікаційної послуги, на яку поширюється повідомлення; 3) технічна можливість виконання вимог, встановлених у повідомленні; 4) ймовірні витрати, пов’язані із виконанням повідомлення; 5) будь-який інший вплив такого повідомлення на оператора телекомунікацій (або категорію операторів), на якого воно поширюється.

Крім того, закон вимагає від Державного секретаря зобов’язати вжити розумних заходів для проведення консультацій з будь-яким оператором, на якого воно поширюється.

Слід також зауважити, рішення Державного Секретаря не є остаточним, його має перевірити та затвердити Судовий комісар. У ст. 89 Закону IPA визначено, що під час вирішення питання про затвердження рішення щодо надання повідомлення про зберігання даних, Судовий комісар зобов'язаний перевірити висновки Державного секретаря стосовно того, чи є вимога, що передбачається відповідним повідомленням і полягає у зобов'язанні зберігати релевантні дані електронних комунікацій, необхідною та пропорційною для досягнення однієї або кількох цілей, передбачених законом.

Окремі аспекти доступу правоохоронних органів до цифрової інформації врегульовані також у Data Protection Act 2018 (DPA 2018) [184]. Цей акт встановлює спеціальний режим обробки електронних даних компетентними органами, зокрема, вимагає чіткого визначення мети такої обробки та дотримання принципу релевантності й недопущення надмірності даних щодо потреб конкретного розслідування (п. 37).

Data Protection Act 2018 (DPA 2018) є основоположним актом законодавства Великої Британії, що комплексно регулює питання захисту персональних даних та встановлює правові рамки їх обробки як у публічному, так і в приватному секторах. Закон був ухвалений з метою імплементації положень Загального регламенту про захист даних (GDPR) та Директиви (ЄС) 2016/680, а також забезпечення балансу між правом особи на приватність і потребами держави у сфері безпеки та кримінального правосуддя.

Зміст DPA 2018 побудований за диференційованим підходом до режимів обробки персональних даних. Закон розмежовує загальний режим обробки даних, який застосовується до цивільного та комерційного обігу інформації, і спеціальний режим, що регулює обробку персональних даних з метою запобігання, розслідування та розкриття кримінальних правопорушень, а також виконання кримінальних покарань. У межах правоохоронного режиму закон закріплює принципи законності, необхідності та пропорційності обробки даних, вимагаючи, щоб втручання у приватне життя особи було обґрунтованим і мінімально достатнім для досягнення легітимної мети.

Особливу увагу DPA 2018 приділяє обробці чутливих категорій персональних даних, таких як дані про здоров'я, біометричні та генетичні дані, політичні чи релігійні переконання. Їх обробка допускається виключно за умов суворої необхідності та за наявності спеціальних гарантій захисту. Закон також визначає обсяг прав суб'єктів персональних даних, водночас, допускаючи можливість їх обмеження у випадках, коли реалізація таких прав може зашкодити кримінальному провадженню або інтересам національної безпеки. Таким чином, DPA 2018 формує сучасну правову модель захисту персональних даних, адаптовану до умов цифровізації та використання інформаційних технологій у діяльності правоохоронних органів.

Дещо схожий за своєю природою нормативно-правовий акт наявний і у французькому законодавстві. У Франції чинним натепер є Закон Loi informatique et libertés 1978 року [201], який передбачає низку заходів щодо захисту персональних даних при здійсненні кримінального провадження. Закон передбачає, що усі правила щодо обробки персональних даних поширюються, у тому числі, на сферу кримінального провадження та запобігання кримінальних правопорушень. У ст. 90 Закону зазначається, що розкриття даних, які стосуються расового або етнічного походження, політичних поглядів, релігійних або філософських переконань, членства в профспілці фізичної особи, обробки генетичних даних, біометричних даних з метою унікальної ідентифікації фізичної особи, даних, що стосуються здоров'я, сексуального життя або сексуальної орієнтації фізичної особи дозволяється включно за умови, що це суворо необхідно для кримінального провадження.

Закон покладає, зокрема, і на органи досудового розслідування обов'язок забезпечити технічну безпеку, конфіденційність та захист від несанкціонованого втручання у випадках, якщо під час кримінального провадження використовується відповідна інформація.

Серед інших базових принципів обробки та розкриття персональних даних, що містяться у електронних інформаційних системах і випливають із

Закону 1978 року можна виокремити, зокрема такі: 1) законність та пропорційність визначеній законом меті; 2) суворе обмеження мети розкриття; 3) мінімізація даних, що передбачає допустимість розкриття лише ти даних, які є мінімально необхідними для досягнення завдань кримінального провадження; 4) обмеження строків зберігання такої інформації; 5) забезпечення конфіденційності даних.

Таким чином, Закон Loi informatique et libertés 1978 року відіграє ключову роль у формуванні балансу між потребами кримінального переслідування та захистом фундаментальних прав особи у цифровому середовищі. Його значення для кримінального провадження полягає в тому, що він поширює стандарти захисту персональних даних на діяльність правоохоронних органів, запобігаючи свавільному збиранню й використанню чутливої інформації. При цьому, вимога суворої необхідності при обробці спеціальних категорій даних забезпечує пропорційність втручання у приватне життя, а обов'язок гарантувати технічну безпеку та конфіденційність забезпечує достовірність таких цифрових доказів.

Отже, аналіз міжнародних стандартів і зарубіжного законодавства у сфері розслідування кримінальних правопорушень, учинених у кіберпросторі, свідчить про поступове формування багаторівневої моделі правового регулювання, спрямованої на ефективну протидію кіберзлочинності з урахуванням її транскордонної природи. Визначальну роль у цьому процесі відіграють міжнародні стандарти, які забезпечують узгодження національних правових підходів, зменшення ризиків юрисдикційних конфліктів і створення спільних механізмів отримання та використання електронних доказів.

Будапештська конвенція Ради Європи закладає основоположні процесуальні інструменти для розслідування кіберзлочинів і визначає базові засади міжнародного співробітництва у цій сфері. Водночас право Європейського Союзу демонструє тенденцію до подальшої деталізації й уніфікації процедур доступу до електронних доказів, що особливо наочно проявляється в Регламенті (ЄС) 2023/1543, який запроваджує прямі механізми

взаємодії з постачальниками цифрових послуг за умови дотримання принципів необхідності, пропорційності та захисту приватності.

Законодавство США та Великої Британії виступає яскравим прикладом поєднання жорсткої криміналізації несанкціонованого втручання в інформаційні системи з розвинутими процедурами судового контролю за доступом держави до електронних комунікацій. У цих правопорядках особливий акцент робиться на забезпеченні балансу між інтересами ефективного кримінального переслідування і гарантіями прав людини, передусім права на повагу до приватного життя та захист персональних даних [150, с. 662].

У підсумку, міжнародні стандарти й позитивний зарубіжний досвід підтверджують потребу подальшої імплементації в українське законодавство сучасних процесуальних механізмів доступу до цифрових доказів, поглиблення міжнародного співробітництва та розширення судового контролю. Це є необхідною умовою адаптації кримінального процесу до викликів цифрової доби й підвищення ефективності розслідування злочинів, учинених у кіберпросторі.

РОЗДІЛ 2. ДОКАЗИ ТА ДЖЕРЕЛА ДОКАЗІВ ПРИ ЗДІЙСНЕННІ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

2.1. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх класифікація

Здійснення досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, спрямоване на з'ясування фактів та обставин предмета доказування у кримінальному провадженні. Їх встановлення забезпечується за допомогою доказів, якими законодавець визнає отримані в передбаченому кримінальним процесуальним законом порядку фактичні дані, придатні за своїм змістом прямо або непрямо підтверджувати чи спростовувати значимі для кримінального провадження факти та обставини або свідчити про достовірність/недостовірність інших доказів чи можливість/неможливість їх використання в доказуванні (ч. 1 ст. 84, ст. 85, ч. 1 ст. 86 КПК України. Із урахуванням специфіки кримінальних правопорушень, вчинених у кіберпросторі, вагоме значення для встановлення фактів та обставин предмета доказування у кримінальних провадженнях щодо них відіграють електронні (цифрові) докази.

У кримінальному процесуальному законі, на відміну від ГПК України, КАС України і ЦПК України, поняття електронних (цифрових) доказів законодавцем не закріплене. Водночас, комплексний підхід у реформуванні процесуального законодавства зумовив розробку та внесення на розгляд Верховної Ради України проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» від 01.09.2020 р. (реєстраційний № 4004), присвяченого визначенню

поняття та видів електронних доказів і детальному регулюванню порядку їх збирання, зберігання та вирішення питання про них.

Зазначеним законопроєктом запропоновано доповнити КПК України статтею 100-1 «Електронні докази», відповідно до ч. 1 якої «електронним доказом є інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [94]. Хоча наведене визначення за рахунок використання терміносполучення «інформація з відомостями» не є досконалим і потребує уточнення, оскільки відомості про значимі для кримінального провадження факти та обставини є інформацією, проте у ньому міститься підхід, закладений законодавцем в інших процесуальних кодексах. Згідно з цим підходом, електронними доказами визнаються відомості в електронній формі, тобто саме електронна форма є основоположною ознакою, що дозволяє відрізнити їх від інших доказів. Так, відповідно до ч. 1 ст. ст. 96 ГПК України [201], ч. 1 ст. 99 КАС України [45] і ч. 1 ст. 100 ЦПК України [157], «електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі». При цьому наведене визначення, за рахунок відображення в ньому примірного переліку видів електронних доказів є більш широким, ніж дефініція, пропонована в законопроєкті від 01.09.2020 р. № 4004. Проте, незважаючи на потребу правового регулювання електронних (цифрових) доказів у кримінальному процесуальному праві, зазначений законопроєкт був знятий з розгляду на підставі Постанови Верховної Ради України «Про порядок денний чотирнадцятої сесії Верховної Ради України дев’ятого скликання» від 03.09.2025 р. № 4586-IX [98].

Наведений підхід знайшов застосування в судовій практиці та відображений у судових рішеннях, постановлених за результатами розгляду

кримінальних проваджень. Так, ККС ВС у Постанові від 06 лютого 2024 р. вказує, що «електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі» [84].

Натомість, законодавець у контексті закріплення документа як процесуального джерела доказів і способів їх збирання у кримінальному процесуальному законі оперує терміном «комп'ютерні дані» (п. 1 ч. 2 і ч. 4 ст. 99, п. 3 ч. 3 ст. 104, п. 4 ч. 2 ст. 105, ч. 6 ст. 236, частини 1 і 2 ст. 237 КПК України). Такий підхід ґрунтується на положеннях Конвенції про кіберзлочинність від 23.11.2001 р., ратифікованої із застереженнями і заявами Законом України від 07.09.2005 р. № 2824-IV, в якій вказаний термін знайшов широке використання. У п. b ст. 1 зазначеної Конвенції вказується, що «комп'ютерні дані означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою» [50]. Водночас, термін «комп'ютерні дані» використовується вченими, зазвичай, у контексті дослідження порядку їх огляду та фіксації в ході проведення слідчих (розшукових) дій [10, с. 970; 37, с. 215], хоча окремі науковці звертаються до визначення поняття комп'ютерних даних, розглядаючи їх як будь-яку інформацію, що була створена, оброблена чи збережена з використанням комп'ютера або іншого електронного пристрою [48, с. 127].

У науці кримінального процесу для позначення досліджуваної категорії використовуються терміни «електронні докази» [51, с. 192; 116, с. 74], «цифрові докази» [36, с. 133; 81, с. 611], «електронні (цифрові) докази» [38, с. 108; 155, с. 210], «цифрові (електронні) докази» [61, с. 99], «докази електронної форми» [34, с. 89], «докази в електронній формі» [145, с. 99]. При

цьому значна кількість вчених, обґрунтовуючи доцільність використання для потреб здійснюваних ними наукових розвідок одного з наведених термінів, звертається до його відмежування від інших і наводить відповідну аргументацію на підтвердження правильності авторського підходу [116, с. 50; 155, с. 218]. Найбільш повно такий підхід застосовує І.Г. Каланча, яка звертається до розмежування понять «електронний доказ», «цифровий доказ» і «доказ електронної форми» з урахуванням їх технічного та правового змісту і відзначає, що «перше з них характеризує технічний спосіб реалізації доказу в електронному середовищі та його збереження на електронних носіях чи в інформаційних системах незалежно від того, чи характеризується його зміст цифровою структурою, друге відображає зміст доказу – значиму для кримінального провадження інформацію, яка існує у виді цифрового (бінарного) коду і підлягає збереженню, обробці та переданню із використанням інформаційних технологій, а третє відповідає процесуальній формі доказу та є узагальнюючим кримінальним процесуальним поняттям, що застосовується для позначення доказу в електронному форматі, збереження або подання якого здійснено без зміни цього джерела чи його процесуальної природи» [34, с. 89].

Звернення до аналізу цього підходу свідчить про використання термінів «електронний доказ», «цифровий доказ» і «доказ електронної форми» («доказ в електронній формі») для позначення одного й того самого правового явища – доказів, які існують в електронній формі, що забезпечує його поглиблене теоретичне розуміння за рахунок відображення різних аспектів їх змісту та форми. Водночас, із точки зору термінознавства, термін відображає точне найменування певного поняття спеціальної галузі знань, яке підлягає точному науковому визначенню [65, с. 36]. Відповідно, для позначення будь-якого правового явища повинен використовуватися один термін, що сприяє забезпеченню точності термінології, використовуваної у відповідній галузі знань. У цьому контексті А.В. Коваленко слушно наголошує, що «за сучасних умов категорії «електронні» та «цифрові» стосовно доказів і слідів є

рівнозначними та мають однакове змістовне навантаження, на підставі чого пропонує до закріплення нормативних дефініцій досліджуваних понять у чинному кримінальному процесуальному законі використовувати термін «електронні (цифрові) докази/сліди» [38, с. 107]. Аналогічну позицію відстоюють Н.В. Глинська та Д.І. Клепка, які вказують на відсутність принципових розбіжностей найменуванні таких доказів електронними, цифровими чи комп'ютерними [18, с. 51], та О.О. Торбас, котрий з огляду на відсутність відповідної термінології у кримінальному процесуальному законодавстві вказує на обґрунтованість доктринального використання термінів «електронні докази» і «цифрові докази» як синонімів [125, с. 104]. Термін «доказ електронної форми» («доказ в електронній формі») використовується вченими виключно для характеристики форми, в якій існує відповідний доказ, внаслідок чого не дозволяє повно охарактеризувати його поняття. Із урахуванням наведеного, для позначення доказів, які існують у електронній формі, доцільно використовувати термін «електронні (цифрові) докази».

Поняття електронних (цифрових) доказів у вітчизняній науці кримінального процесу не знайшло однозначного розуміння. Звертаючись до визначення поняття таких доказів, вчені акцентують увагу на одному з таких аспектів: процесуальному, технічному або криміналістичному.

У процесуальному аспекті електронні (цифрові) докази характеризуються науковцями як фактичні дані (відомості про факти, інформація) в електронній формі, значимі для встановлення фактів та обставин кримінального провадження. Так, Г. Авдєєва та Е. Живуцька-Козловська розглядають електронні (цифрові) докази як «фактичні дані у виді бінарного (двійкового) коду, що містять інформацію, значиму для об'єктивного вирішення кримінального провадження» [1, с. 131]. У процесуальному аспекті О.О. Рачинський і Т.Г. Фоміна визначають електронні (цифрові) докази як цифрову інформацію, яка відображена на електронних носіях і відповідає вимогам, передбаченим ст. 84 КПК України [155, с. 210]. Схожу дефініцію

електронних (цифрових) доказів наводить А.В. Маркіна, на думку якої вони за своєю сутністю є фактичними даними (відомостями про факти), що знайшли відображення в цифровій формі на відповідному матеріальному носії [67, с. 392]. Таким чином, визначаючи поняття електронних (цифрових) доказів у процесуальному аспекті, вчені основну увагу зосереджують на їх змісті, яким, на думку С.О. Ковальчука, є фактичні дані, що існують в електронній формі та можуть бути використані для встановлення значимих для кримінального провадження фактів та обставин [42, с. 121].

Поряд із наведеними дефініціями досліджуваного поняття, низка вчених визначає його з урахуванням вказівки на технічний аспект, але не розкриває зміст останнього. Зокрема, Н.В. Глинська розглядає електронні (цифрові) докази як «отримані у встановленому КПК України порядку фактичні дані, що існують в електронній формі, відображені на електронних (цифрових) носіях і використовуються задля з'ясування фактів та обставин, що підлягають доказуванню» [51, с. 195-196]. Із цих позицій В.М. Фігурський характеризує електронні (цифрові) докази як «створену, збережену, оброблену чи передану з використанням аналогових або цифрових сигналів інформацію, значиму для кримінального провадження» [145, с. 99].

Поділяючи такий підхід, окремі вчені у визначенні поняття електронних (цифрових) доказів констатують значення технічного аспекту. Так, І.І. Липкан визначає електронні (цифрові) докази як «інформацію в електронній формі, що збережена чи передана з використанням електронних засобів, є релевантною для встановлення фактів та обставин кримінального провадження та характеризується специфічною технічною природою, яка забезпечує автентичність цієї інформації та можливість її дослідження» [61, с. 99]. Схожу позицію відстоює І.А. Смаль, на думку котрої електронні (цифрові) докази є «інформацією в електронному виді, яка містить значимі для кримінального провадження відомості про його факти та обставини, створена, збережена чи передана з використанням електронних систем, мереж або

пристроїв та існує у формі, яка забезпечує її цілісність, автентичність і придатність для дослідження» [116, с. 74].

Із точки зору технічного аспекту електронні (цифрові) докази характеризуються науковцями шляхом розкриття їх технічних особливостей. Зокрема, В.С. Сезонов і М.Г. Щербаковський вказують, що «електронна (цифрова) інформація за своєю сутністю є двійковим кодом, що записаний за допомогою використання нулів та одиниць і призначений для зчитування, обробки та передавання шляхом використання інформаційних технологій, у зв'язку з чим така інформація в первинному вигляді є непридатною для людського сприйняття» [162, с. 14]. Поділяючи таку позицію, Д.М. Цехан визначає електронні (цифрові) докази як «фактичні дані, що існують у цифровій (дискретній) формі, відображені на носії будь-якого типу та стають доступними для сприйняття виключно після їх обробки за допомогою електронно-обчислювальної техніки» [36, с. 133]. Прихильниками такого розуміння електронних (цифрових) доказів є Д.О. Алєксєєва-Процюк та О.М. Брисковська, на думку котрих ними є «збережені в електронному виді в будь-яких електронних засобах чи на будь-яких електронних носіях фактичні дані, які стають доступними для сприйняття після обробки за допомогою програмного забезпечення або спеціальних технічних засобів» [2, с. 250].

Окремі вчені наводять дефініції електронних (цифрових) доказів одночасно у двох наведених аспектах: процесуальному та технічному. Так, на основі інформаційного підходу до розуміння доказів як єдності фактичних даних (відомостей про факти), що становлять їх зміст, і носія цих даних (відомостей), яким є джерело доказів), А.В. Скрипник пропонує два визначення поняття електронних (цифрових) доказів: 21) теоретичне, відповідно до якого ними є електронна (цифрова) інформація, отримана за допомогою здійсненого з використанням технічних засобів відтворення змісту файлу, що зберігається на носії цифрових даних; 2) нормативне, згідно з яким такими доказами є отримана у встановленому КПК України порядку електронна (цифрова) інформація, на підставі якої дізнавачем, слідчим,

прокурором, слідчим суддею, судом встановлюються значимі для кримінального провадження факти та обставини» [114, с. 21].

У криміналістичному аспекті електронні (цифрові) докази характеризуються в контексті криміналістичного пізнання обставин вчиненого кримінального правопорушення. Так, О.Г. Козицька вказує, що «електронні (цифрові) докази за своєю сутністю є цифровим об'єктом, який був засобом чи знаряддям вчинення кримінального правопорушення, зберіг електронно-цифрові сліди кримінального правопорушення, був предметом або об'єктом вчинення кримінального правопорушення або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [46, с. 420]. У цьому аспекті електронні (цифрові) докази розглядаються з точки зору їх зв'язку з подією кримінального правопорушення.

Аналізуючи наведені підходи до розуміння електронних (цифрових) доказів у процесуальному, технічному та криміналістичному аспектах, потрібно відзначити їх взаємодоповнюваність і, як наслідок, потребу у визначенні поняття таких доказів у взаємозв'язку цих аспектів. У ході визначення поняття електронних (цифрових) доказів необхідно звернути увагу на декілька моментів, сукупне врахування яких дозволить сформулювати науково обґрунтовану дефініцію.

По-перше, у процесуальному аспекті електронні (цифрові) докази визначаються вченими як «фактичні дані», «відомості про факти» та «інформація про факти». Розглядаючи вказані терміни як синоніми, С.О. Ковальчук зазначає, що зміст доказів становлять фактичні дані, під якими пропонує розуміти відомості (інформацію) про значимі для кримінального провадження факти та обставини [42, с. 149]. Такий підхід у цілому підлягає поширенню й на електронні (цифрові) докази, але з урахуванням притаманності їм більш складної внутрішньої структури, зумовленої специфікою таких доказів. Як слушно вказує І.Г. Каланча, «внутрішня структура електронних (цифрових) доказів є чотирирівневою і містить: 1)

контент, що являє собою інформаційне ядро, яке становить змістовну частину доказу – значимі для кримінального провадження фактичні дані (інформація в текстовій і графічній формі, аудіо- та відеоінформація, відомості журналів активності тощо); 2) метадані, які забезпечують технічну ідентифікацію цифрового об'єкта – дозволяють відтворити його історію, ідентифікувати джерело походження, виявити спроби втручання та модифікації, а в окремих випадках характеризуються в доказуванні самостійним значенням (дані про дату та час створення об'єкта, його модифікації та доступу до нього, авторство, розмір і формат об'єкта, місце його зберігання та інші характеристики контенту); 3) системна оболонка, що являє собою службову інформацію відповідної операційної системи (програмного середовища), в якій цей цифровий об'єкт існує, слугує контекстом для інтерпретації контенту та метаданих і відіграє вагому роль у ході підтвердження цілісності доказу (структура директорій, атрибути файлів, тимчасові файли, системні журнали та інші компоненти, які автоматично створюються програмним середовищем); 4) носій інформації, яким є матеріальний об'єкт, що забезпечує фізичне існування електронного (цифрового) доказу та його зберігання» [34, с. 139].

По-друге, звертаючись до наведених визначень електронних (цифрових) доказів у технічному аспекті, потрібно констатувати, що вони не враховують один з основних елементів їх дефініції в аспекті процесуальному – їх значимість для встановлення фактів та обставин кримінального провадження. Поряд із цим, недостатньо констатувати існування фактичних даних (відомостей про факти) в електронній формі, оскільки доказом вони стати лише після їх отримання у процесуальному порядку. На це звертають увагу Н.В. Глинська та Д.І. Клепка, котрі за способом вираження поділяють цифрову інформацію на два види: представлену за допомогою використання двійкової форми та інтерпретовану з використанням програмного забезпечення у зображення, звук, текст тощо, на підставі чого вказують на можливість безпосереднього дослідження в суді виключно другого з наведених видів

інформації (зокрема, дослідження матеріальних носіїв електронної інформації, інтернет-сторінок тощо) [18, с. 55].

По-третє, поняття «електронні (цифрові) докази» у криміналістичному аспекті потрібно відмежовувати від поняття «електронні (цифрові) сліди кримінального правопорушення». Під останнім із них переважна більшість вчених розуміє результат здійсненого в ході доступу до електронної інформації впливу на неї, що знаходить свій прояв у будь-яких змінах цієї інформації, пов'язаних з подією кримінального правопорушення (її копіювання, модифікація, знищення, блокування доступу тощо) [5, с. 221]. Поділяючи такий підхід, А.В. Коваленко електронні (цифрові) сліди кримінального правопорушення пропонує розуміти як «комп'ютерні дані, що утворилися в запам'ятовувальних пристроях відповідної електронно-обчислювальної техніки чи зазнали змін у цих пристроях у результаті дій користувачів, безпосередньо пов'язаних із вчиненням кримінального правопорушення» [40, с. 230]. Відповідно, електронні (цифрові) сліди кримінального правопорушення є одним із видів електронних (цифрових) доказів. Встановлюючи їх співвідношення, І.А. Колеснікова вказує, що «електронні (цифрові) докази є інформацією, яка зафіксована на будь-якому електронному носії в електронній формі, а електронні (цифрові) сліди кримінального правопорушення є метаданими – інформацією про дату та час створення електронної інформації, місце її створення, внесені до неї зміни, її переміщення тощо, що супроводжує цю електронну інформацію» [47, с. 195].

По-четверте, невід'ємною передумовою визначення поняття електронних (цифрових) доказів є виокремлення притаманних їм ознак. Як слушно наголошує О.В. Капліна, визначення будь-якого терміну має відображати основні, найбільш суттєві ознаки поняття, що позначається ним, які є необхідними та у своїй сукупності достатніми для ідентифікації цього терміну та його відмежування від інших термінів [35, с. 176]. Це зумовлює необхідність звернення до дослідження ознак, притаманних електронним (цифровим) доказам у кримінальному провадженні.

У науці кримінального процесу виокремленню ознак електронних (цифрових) доказів, як і визначенню їх поняття, присвячена істотна увага вчених, серед яких спостерігається плюралізм думок як стосовно кількісного вираження цих ознак, так і їх змісту.

Одна група вчених визначає ознаки електронних (цифрових) доказів шляхом наведення їх переліку, основну увагу в якому надають їх технічним характеристикам. Так, звертаючись до виокремлення характерних властивостей електронних (цифрових) доказів, І.О. Крицька до їх числа відносить: 1) притаманність неречового характеру, про який свідчить відсутність нерозривного зв'язку з матеріальним носієм електронної інформації; 2) неможливість безпосереднього сприйняття електронної інформації та її подальшого дослідження поза інтерпретацією та перекодуванням з використанням програмного забезпечення і спеціальних технічних засобів; 3) можливість внесення змін до електронної інформації та її знищення дистанційно; 4) здійснення збирання електронних (цифрових) доказів, їх перевірки та оцінки із дотриманням специфічного порядку [57, с. 304]. Акцентуючи увагу на поєднанні ознак електронних (цифрових) доказів, які ґрунтуються на процесуальному та технічному аспектах їх розуміння, С.Є. Абламський і В.В. Романюк вважають, що до них належать такі: 1) такими доказами є інформація в електронній (цифровій) формі; 2) ця інформація відображена на електронному носії; 3) релевантність таких доказів до конкретного кримінального провадження та її значимість для встановлення його фактів та обставин; 4) їх специфічна природа, яка полягає в тому, що вони є фактичними даними у цифровій (дискретній) формі [107, с. 143]. Дещо ширше коло ознак електронних (цифрових) доказів наводить В.М. Фігурський, котрий до них включає такі: 1) їх створення людиною або комп'ютерною системою; 2) притаманність нематеріального вираження, що зумовлює можливість їх зберігання на одному або декількох матеріальних носіях поза нероздільним зв'язком з ними чи існування у цифровому середовищі поза таким носієм; 3) можливість сприйняття в результаті використання

програмного забезпечення або спеціальних технічних засобів; 4) можливість тривалого зберігання без змін, копіювання та пересилання поза коригуванням змісту, необмеженість у кількості операцій з використання; 5) піддатливість до маніпуляцій та знищення; 6) можливість визнання копій деяких електронних (цифрових) доказів (зокрема, документів) за наявності обов'язкових реквізитів оригіналами та їх одночасного використання в декількох кримінальних провадженнях [145, с. 100]. Схожу позицію висловлюють Д.О. Алєксєєва-Процюк та О.М. Брисковська, котрі, водночас, визначають більш широке коло ознак електронних (цифрових) доказів: 1) існування в нематеріальному виді; 2) можливість створення людиною або виникнення внаслідок функціонування інформаційної системи; 3) неможливість існування поза межами матеріального носія інформації чи каналу зв'язку; 4) відсутність нерозривного зв'язку з матеріальним носієм інформації; 5) вільне переміщення в електронній мережі без матеріального носія; 6) неможливість безпосереднього сприйняття і дослідження поза використанням програмного забезпечення та спеціальних технічних засобів; 7) дотримання специфічного порядку збирання електронних (цифрових) доказів, їх перевірки та оцінки; 8) здатність до дубляжу, що полягає в копіюванні інформації чи її переміщенні на інший носій, внаслідок якого вона не втрачає притаманних їй характеристик; 9) можливість внесення змін до інформації та її знищення дистанційно [2, с. 252].

Інша група вчених виокремлює ознаки електронних (цифрових) доказів шляхом узагальненої характеристики кожної з них та подальшого пояснення її змісту. Зокрема, І.І. Липкан вказує, що «електронні (цифрові) докази характеризуються такими ознаками: 1) цифрова (електронна) форма (ця ознака полягає в існуванні інформації у форматі, який підлягає збереженню, обробленню та переданню виключно з використанням інформаційно-комунікаційних технологій); 2) наявність специфічного електронного носія (наведена ознака вказує на зберігання інформації або можливість доступу до неї на відповідному електронному носії (як фізичному, так і віртуальному), що

забезпечує автентичність цієї інформації); 3) релевантність (ця ознака свідчить про значимість інформації для конкретного кримінального провадження, тобто безпосередній зв'язок цієї інформації з його фактами та обставинами); 4) специфічна природа (вказана ознака відображає технічні особливості, якими повинна характеризуватися інформація – наявність метаданих, можливість копіювання та відновлення поза зміною її первинного змісту, залежність доступу від наявності програмного забезпечення або апаратних засобів)» [61, с. 89]. Поділяючи таку позицію в цілому, більш розгалужене коло ознак електронних (цифрових) доказів наводить І.А. Смаль, на думку котрої до їх числа належать: «1) відтворюваність (ця ознака свідчить про можливість здійснення їх копіювання поза втратою первинного змісту); 2) нематеріальність (відповідно до наведеної ознаки, вони існують у виді цифрових даних, які закодовані за допомогою бінарних чи інших електронних сигналів та підлягають відображенню виключно з використанням спеціальних технічних пристроїв); 3) динамічність (зазначена ознака вказує на їх придатність до змін і знищення під впливом користувацьких дій або програмного забезпечення); 4) залежність від технічних носіїв (ця ознака передбачає можливість їх збереження, дослідження та перевірки лише за допомогою відповідного технічного обладнання або спеціального програмного забезпечення); 5) відсутність жорсткого зв'язку з матеріальним носієм (наведена ознака вказує на можливість одночасного існування однієї й тієї самої інформації на декількох непов'язаних між собою матеріальних носіях); 6) наявність метаданих (ця ознака передбачає існування даних, що не становлять основний зміст файлу, проте дозволяють встановити його автентичність, авторство, час створення, редагування тощо)» [116, с. 62-63].

За допомогою більш широкого кола ознак електронні (цифрові) докази характеризує А.В. Скрипник, котрий обґрунтовує доцільність здійснення класифікації цих ознак і поділяє їх на такі групи: 1) ознаки, які ґрунтуються на сутності цифрової інформації: а) електронне (цифрове) середовище існування; б) характерні риси, притаманні інформації: позбавленість суб'єктивності;

закодованість; можливість існування в декількох формах; мобільність; мінливість інформації; тиражованість; в) характерні риси, притаманні носію інформації: опосередкованість через машинний (фізичний) носій; відсутність жорсткої позиційної прив'язки як до тієї чи іншої ділянки машинного носія, так і до певного носія в цілому; мультиплікативність; можливість багаторазового запису на машинні носії; 2) ознаки цифрової інформації, які знаходять безпосередній прояв у доказуванні (власне ознаки таких доказів): – комплексність доказу; наявність апаратних і програмних засобів як джерела доказу; специфічність порядку збирання електронних (цифрових) доказів, їх перевірки та оцінки [114, с. 87-94].

Невдаючись до поглибленого аналізу кожної із наведених вченими властивостей електронних (цифрових) доказів, які виокремлюються ними як характерні ознаки таких доказів, потрібно звернути увагу на декілька аспектів розуміння їх кола.

По-перше, надмірне виокремлення ознак будь-якого правового явища перенасичує його поняття, внаслідок чого не відповідає вимогам до правових дефініцій. Зокрема, як одну з основних вимог, яким повинно відповідати правове визначення будь-якого терміну, В.М. Косович виокремлює відображення ним лише суттєвих ознак, притаманних узагальненим явищам, що мають правове значення [54, с. 48]. Із цих позицій, кількість виокремлюваних ознак електронних (цифрових) доказів повинна бути достатньою для визначення їх поняття.

По-друге, з огляду на предмет дослідження, основу для визначення поняття електронних (цифрових) доказів повинні становити ознаки, що ґрунтуються на процесуальному аспекті їх розуміння. Відповідно, ті ознаки, що ґрунтуються на технічному аспекті розуміння електронних (цифрових) доказів, мають відображатися в узагальненому вигляді та не містити детального переліку особливостей існування таких доказів і процесуальної діяльності щодо їх збирання, дослідження, зберігання, перевірки та оцінки у кримінальному провадженні.

Із урахуванням наведеного, електронні (цифрові) докази у кримінальному провадженні підлягають характеристиці за допомогою виокремлення таких ознак: 1) вони є фактичними даними (відомостями про факти), які отримані в передбаченому КПК України порядку; 2) вони існують в електронній формі на відповідному електронному носії – як фізичному, так і віртуальному; 3) вони характеризуються цілісністю, автентичністю та придатністю для дослідження; 4) вони мають значення для встановлення щодо фактів та обставин, які мають значення для кримінального провадження. Наведені ознаки підлягають відображенню у дефініції електронних (цифрових) доказів зі слушним уточненням, висловленим С.Є. Абламським і В.В. Романюком, котрі, з огляду на те, що інформація на електронних носіях є саме електронною, констатують недоцільність паралельної вказівки у визначенні на електронний характер інформації та її відображення на електронному носію [107, с. 147]. На підставі зазначених ознак та враховуючи наведене уточнення, електронні (цифрові) докази доцільно визначити як фактичні дані в електронній формі, які отримані в передбаченому КПК України порядку, характеризуються цілісністю, автентичністю та придатністю для дослідження та мають значення для встановлення фактів та обставин кримінального провадження.

За своєю сутністю електронні (цифрові) докази, як зазначає О.Г. Козицька, є цифровими об’єктами, які: «1) були засобом вчинення кримінального правопорушення чи його знаряддям (використані для несанкціонованого доступу до інформації вірусні програми, створені для збуту наркотичних засобів телеграм-канали тощо); 2) зберегли в електронно-цифровій формі сліди кримінального правопорушення (відеозаписи з камер відеоспостереження, містять зображення підозрюваного, інформація про здійснений в електронній формі переказ коштів, наданих як неправомірна вигода, метадані, що відображають час входу в автоматизовану систему ідентифікованого користувача тощо); 3) були предметом кримінального правопорушення (веб-сайт, використаний для розміщення матеріалів

порнографічного характеру); 4) були об’єктом кримінально протиправних дій (незаконно поширений у мережі інтернет об’єкт авторського права, викрадена криптовалюта тощо); 5) містять будь-які інші відомості, придатні для використання як докази фактів та обставин, встановлюваних у кримінальному провадженні (розміщена на сторінці соціальної мережі інформація, що характеризує особу підозрюваного) [46, с. 419-420]. Натомість, електронна форма інформації, як вказує В.М. Фігурський, відтворює всі елементи інформації в матеріальній формі та становить нематеріальну версію інформації, яка існує в іншій формі (графічній, письмовій, аудіовізуальній) чи в поєднанні зазначених форм» [145, с. 99].

У науці кримінального процесу дискусійним є питання стосовно процесуального статусу електронних (цифрових) доказів. Узагальнюючи висловлені вченими підходи, М.І. Демура, Д.І. Клепка та І.О. Крицька виокремлюють чотири підходи щодо нього: 1) віднесення електронних (цифрових) доказів до числа документів як джерела доказів; 2) можливість їх визнання речовими доказами; 3) можливість віднесення електронних (цифрових) доказів як до документів, так і до речових доказів; 4) доцільність їх визнання самостійним джерелом доказів [26, с. 40]. Значною мірою такий плюралізм підходів зумовлений тривалим пошуком шляхів наукового обґрунтування механізму формування електронних (цифрових) доказів та їх використання в доказуванні. Водночас, на сьогодні існують всі передумови для їх виокремлення як самостійного джерела доказів, що зумовлено притаманністю їм специфічної процесуальної природи. Як зазначає А.В. Коваленко, процесуальною формою закріплення таких доказів (їх процесуальним джерелом) є електронний документ, джерелом відомостей, які мають доказове значення, є комп’ютерні дані як електронні (цифрові) сліди вчиненого кримінального правопорушення в їх широкому розумінні, а їх носієм – матеріальний носій комп’ютерних даних, що свідчить про поєднання електронними (цифровими) доказами ознак слідів у широкому криміналістичному значенні (як результату причинно пов’язаних із подією

кримінального правопорушення змін комп'ютерних даних) і документів (що містять відомості про факти у зашифрованій формі) [38, с. 108]. При цьому у практичній площині матеріальні носії комп'ютерних даних, що є носіями електронних (цифрових) доказів, визнаються речовими доказами. Проте, як вказує І.Г. Каланча, набуття статусу речового доказу ґрунтується не на процесуальній природі електронних (цифрових) доказів, а є рішенням, направленим на забезпечення їх збереження стороною обвинувачення (зокрема, задля дотримання норм КПК України у частині накладення арешту на майно, яке було тимчасово вилучене під час огляду, обшуку) [34, с. 120].

Види електронних (цифрових) доказів, як і їх поняття, нормами кримінального процесуального закону не визначаються. Водночас, спроба їх нормативного закріплення була здійснена у законопроєкті від 01.09.2020 р. (реєстраційний № 4004), яким пропонувалося доповнити КПК України ст. 100-1 «Електронні докази», згідно з ч. 2 якої «до електронних доказів можуть належати: 1) електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо); 2) віртуальні активи; 3) веб-сайти, веб-сторінки; 4) текстові, мультимедійні та голосові повідомлення; 5) метадані; 6) бази даних; 7) інша інформація в електронній (цифровій) формі» [94]. Проєкт наведеної норми відображає підхід законодавця, закладений у нормах інших процесуальних кодексів, в яких наведений перелік видів електронних (цифрових) доказів, за винятком віртуальних активів, включений ним до визначення їх поняття (ч. 1 ст. 96 ГПК України [21], ч. 1 ст. 99 КАС України [45] і ч. 1 ст. 100 ЦПК України [157]). Такий перелік електронних доказів наводиться й у судовій практиці ККС ВС (Постанова ККС ВС від 06.02.2024 р. у справі № 645/6247/16-к) [84].

Із урахуванням широкого кола видів електронних (цифрових) доказів, у науці кримінального процесу запропоновано здійснювати їх класифікацію за декількома критеріями. Узагальнюючи пропоновані вченими підходи, В.В. Петрик класифікує електронні (цифрові) докази за трьома критеріями: «1) за джерелом походження: а) дані з комп'ютерних систем (файли, що

зберігаються в комп'ютерних мережах, серверних сховищах, на жорстких дисках і резервних носіях: бази даних, документи, графіки, таблиці, а також програмне забезпечення, що відображає інформацію стосовно користувацьких дій, програмних збоїв тощо); б) дані з мобільних пристроїв (текстові повідомлення, фотографії, відеозаписи, записи дзвінків, електронні листи, місцезнаходження (геолокація), дані про інстальовані додатки тощо); в) дані з мережі Інтернет (повідомлення в соціальних мережах, листування у месенджерах, блоги, чати, коментарі на форумах тощо); г) відеозаписи та аудіофайли (записи з камер відеоспостереження та інших цифрових джерел, аудіофайли, отримані з різних джерел, тощо); 2) за способом отримання: а) вилучені в ході слідчих (розшукових) і негласних слідчих (розшукових) дій; б) добровільно надані учасниками кримінального провадження або витребувані за запитом сторони обвинувачення; 3) за характеристиками інформації: а) структуровані дані (ними є дані, для зберігання яких використовується певний формат, що полегшує їх аналіз і використання в доказуванні: бази даних, таблиці тощо); б) неструктуровані дані (їх становлять дані, які не мають чітко визначеної структури або потребують додаткового аналізу, спрямованого на відновлення змісту: електронні листи, повідомлення, текстові файли тощо)» [79, с. 326].

Більш розгалужену класифікацію електронних (цифрових) доказів за способом їх отримання наводить І.І. Липкан, котрий за цим критерієм виокремлює такі види: «1) електронні (цифрові) документи та інші електронні (цифрові) докази, надані державними органами чи іншими офіційними установами або отримані в результаті доступу до інформації, що міститься на сервері; 2) електронні (цифрові) докази, одержані автономних систем (ними є записи, отримані з камер відеоспостереження, реєстраторів тощо); 3) електронні (цифрові) докази, одержані в результаті проведення слідчих (розшукових) і негласних слідчих (розшукових) дій; 4) електронні (цифрові) докази, отримані внаслідок застосування заходів забезпечення кримінального провадження; 5) електронні (цифрові) докази, одержані з використанням

технічних засобів (фотознімки, відеозаписи тощо); 6) електронні (цифрові) докази, отримані внаслідок тимчасового вилучення майна в порядку ст. 168 КПК України» [61, с. 115].

Поряд із класифікацією електронних (цифрових) доказів у цілому, вчені звертаються до класифікації електронних документів. Так, А.В. Гутник та А.Я. Хитра класифікують їх за такими критеріями: 1) із точки зору використання як доказу: юридичні та технічні; 2) за місцем знаходження: смартфон, відеокамера, планшет, комп'ютер, інтернет-сервер, «розумна» побутова техніка, тощо; 3) за формою: електронні повідомлення, аудіозаписи, відеозаписи, веб-сайти, інформація в електронній формі; 4) за джерелом походження: створені користувачем та сформовані комп'ютерною системою; 5) за стадією виготовлення: оригінали електронних документів, копії та витяги; 6) за ступенем захисту: відкриті та закриті; 7) залежно від можливості доступу до метаданих: з відкритими метаданими і прихованими; 8) за комбінацією метаданих електронного документа: одно-, дво-, три-, чотири- та п'ятирангові [24, с. 58].

Класифікація електронних документів за стадіями виготовлення ґрунтується на нормах кримінального процесуального закону, які передбачають можливість використання як їх оригіналів, так і копій і витягів з них. Із урахуванням ч. 3 ст. 99 КПК України, оригіналом електронного документа визнається його відображення, яке має таке саме значення, як і сам документ. Застосовуючи наведену норму, ОП ККС ВС звертає увагу, що «характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. У випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той же електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені або

повноважною особою, яка його створила (обчисленням контрольної суми файлу або каталогу з файлами (CRC-суми, hash-суми) чи накладенням цифрового підпису), або, за наявності підстав, шляхом проведення спеціальних судових досліджень» (Постанова від 25.09.2023 р. у справі № 208/2160/18) [93].

Звертаючись до аналізу висловлених вченими підходів до класифікації електронних (цифрових) доказів, необхідно вказати на прийнятність її здійснення за тими критеріями, яким притаманне теоретичне та практичне значення. Теоретичне значення класифікації електронних (цифрових) доказів забезпечує поглиблене дослідження та формування на його основі детального розуміння сутності кожного з виокремлених видів таких доказів із урахуванням його особливостей і відмінностей від інших їх видів за цим критерієм. Практичне значення класифікації електронних (цифрових) доказів полягає в її спрямованості на підвищення ефективності процесуальної діяльності зі збирання, перевірки, оцінки і використання у таких доказів кримінальному процесуальному доказуванні, виходячи зі специфіки, притаманної конкретним їх видам.

Поряд із цим, здійснюючи класифікацію електронних (цифрових) доказів, потрібно дотримуватися логічних правил поділу понять. Відповідно до цих правил, їх поділ має відбуватися за однією основою, яка характеризується виразністю, бути співмірним і безперервним (поступовим), а виокремлювані внаслідок його здійснення групи повинні виключати одна одну та не мати спільних елементів [62, с. 51-52]. Із урахуванням наведеного, найбільш прийнятною класифікацією електронних (цифрових) доказів, що дозволяє розкрити притаманні їм особливості, є їх поділ за формою на такі види: 1) електронні документи (текстові документи, аудіо- та відеозаписи, фотознімки та інші зображення); 2) електронні повідомлення (текстові, мультимедійні та голосові повідомлення); 3) віртуальні активи; 4) логи, дані клієнтського середовища, контекстні дані, метадані та інші технічні дані; 5) інша інформація в електронній (цифровій) формі.

Підсумовуючи викладене, потрібно відзначити, що застосування інформаційної концепції до розуміння електронних (цифрових) доказів дозволяє розглядати їх як єдність фактичних даних (зміст доказів) та носія цих даних (джерела доказів). Електронні (цифрові) докази є фактичними даними в електронній формі, які отримані в передбаченому КПК України порядку, характеризуються цілісністю, автентичністю та придатністю для дослідження та мають значення для встановлення фактів та обставин кримінального провадження. З огляду на їх існування в електронній формі, електронні (цифрові) докази відображаються на відповідному електронному носії – як фізичному, так і віртуальному.

Класифікацію електронних (цифрових) доказів доцільно здійснювати за їх формою, на основі якої виокремлювати електронні документи, електронні повідомлення, віртуальні активи, технічні дані та іншу інформацію в електронній (цифровій) формі.

Задля вдосконалення механізму формування та використання електронних (цифрових) доказів у кримінальному процесуальному доказуванні КПК України необхідно доповнити статтею 99-1 у такій редакції:

«Стаття 99-1. Електронні (цифрові) докази

1. Електронними (цифровими) доказами є фактичні дані в електронній формі, які отримані в передбаченому цим Кодексом порядку, характеризуються цілісністю, автентичністю та придатністю для дослідження та мають значення для встановлення фактів та обставин кримінального провадження.

2. До електронних (цифрових) доказів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати:

1) електронні документи та інші носії інформації в електронній формі, передбачені пунктами 1, 3 частини другої статті 99 цього Кодексу;

2) електронні повідомлення;

3) віртуальні активи;

4) логи, дані клієнтського середовища, контекстні дані, метадані та інші технічні дані;

5) інша інформація в електронній (цифровій) формі».

2.2. Джерела електронних (цифрових) доказів у кримінальному провадженні

Питома вага електронних (цифрових) доказів у системі доказової бази у провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі, зумовлює спрямованість процесуальної діяльності слідчого та уповноважених ним співробітників оперативних підрозділів на виявлення джерел таких доказів. Правильне визначення джерел електронних (цифрових) доказів є запорукою їх отримання та подальшого використання для встановлення обставин кримінальних правопорушень, вчинених у кіберпросторі. Досліджуючи проблематику збирання електронних (цифрових) доказів, вчені відзначають важливість точного встановлення їх джерел. Так, І.І. Липкан вказує, що «точне визначення джерела електронних (цифрових) доказів відіграє ключове значення в ході забезпечення правомірності здійснення кримінального провадження та його ефективності, оскільки дозволяє: 1) обрати правильні процесуальні процедури із виявлення, вилучення та фіксації цих доказів і релевантні засоби (їх відповідність правилам, передбаченим КПК України, становить необхідну умову визнання одержаних фактичних даних допустимими доказами); 2) забезпечити збереження інформації (в ході фіксації та вилучення таких доказів потрібно запобігати їх втраті, модифікації та пошкодженню, оскільки наслідком навіть незначних змін у них може бути втрата ними доказового значення); 3) гарантувати належний рівень компетенції (фіксація та вилучення цих доказів із залученням спеціалістів у сфері інформаційної безпеки та інформаційних технологій дозволить провести відповідні процесуальні дії з урахуванням встановлених стандартів та

запобігти процесуальним помилкам, які можуть призвести до визнання судом цих доказів недопустимими або недостовірними)» [61, с. 103].

Визначенню поняття джерел електронних (цифрових) доказів, на відміну від поняття цих доказів, у теорії кримінального процесу присвячено недостатньо уваги. Звернення до дослідження позицій вчених і практичних працівників, присвячених дослідженню електронних (цифрових) доказів дозволяє виокремити два підходи до їх розуміння.

Представники першого підходу джерелом електронних (цифрових) доказів визнають виключно електронні (цифрові) об'єкти. Так, С.Є. Абламський, А.С. Крижановський і В.В. Романюк вважають, що «джерелом таких доказів є електронний (цифровий) об'єкт, використаний для створення, фіксації та передання доказової інформації» [107, с. 147; 56, с. 1027]. У контексті дослідження електронних документів Ю.Ю. Орлов і С.С. Чернявський пояснюють наведений підхід тим, вони існують в інформаційній мережі, відповідно до специфіки хмарних технологій можуть неодноразово перезаписуватися з одного на інший матеріальний носій та внаслідок відсутності прив'язки до такого носія являють собою інформацію «в чистому вигляді» [75, с. 14].

Представники другого підходу джерело електронних (цифрових) доказів пов'язують з його матеріальним носієм (відображенням на такому носії). Зокрема, звертаючись до розкриття сутності електронних документів, В.С. Сезонов і М.Г. Щербаковський вказують, що «їх поняття є невіддільним від носія цих документів – матеріального об'єкта або середовища, придатних за своєю структурою для зберігання внесеної інформації» [162, с. 15]. Наведеного підходу притримуються розробники методичних рекомендацій і практичних посібників із формування та використання електронних (цифрових) доказів, адресованих слідчим, прокурорам, співробітникам оперативних підрозділів, суддям. На їх думку, джерелами таких доказів можуть бути будь-які електронні (цифрові) пристрої [72, с. 699]. У межах цього підходу низка вчених визначає джерело електронних (цифрових) доказів

через їх відображення на відповідному матеріальному носію. Так, досліджуючи джерела електронних документів, Я.В. Жидовцев та Я.В. Мілімко зазначають, що будь-яка форма їх відображення фактично є джерелом доказів [70, с. 306].

Аналізуючи наведені підходи, потрібно вказати, що електронні (цифрові) докази, незважаючи на своє існування в електронній формі, відображаються на відповідному електронному носії – як фізичному, так і віртуальному. У цьому аспекті слушною є позиція О.А. Кульбашної, котра у структурі електронного документа виокремлює два елемента: «1) внутрішню структуру, яку становить його змістовна частина; 2) зовнішню структуру, яку складає структура того середовища, в якому електронний документ існує (носій електронної інформації, формат файлу тощо)» [58, с. 380]. Поділяючи таку позицію, її доцільно поширити й на структуру будь-яких інших видів електронних (цифрових) доказів, оскільки для встановлення обставин кримінального провадження значення може мати не лише зміст електронного (цифрового) доказу, але й місце його створення, зберігання, оброблення та виявлення, що є відображенням середовища існування цього доказу. При цьому такий носій необхідно відрізняти від матеріального носія електронних (цифрових) доказів, який отримується внаслідок їх процесуального формування відповідно до норм КПК України, на що звертають увагу вчені у контексті розмежування джерел доказів та їх матеріальних носіїв. Так, Ю.А. Комісарчук зазначає, що «зміст доказів складають отримані з належних джерел фактичні дані, а матеріальну основу становить штучно створений процесуальний носій, а не джерело» [31, с. 41].

У кримінальному процесуальному законі перелік джерел електронних (цифрових) доказів не наводиться, водночас, з аналізу його норм, присвячених проведенню слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій, спрямованих на виявлення та вилучення комп’ютерних даних та їх копій, можна дійти висновку, що законодавець такими джерелами охоплює електронні інформаційні системи, електронні комунікаційні системи,

комп'ютерні системи та їх частини, мобільні термінали систем зв'язку (ч. 4 ст. 99, ч. 1 ст. 159, ч. 2 ст. 168, ч. 3 ст. 170, ч. 6 ст. 236, ч. 2 ст. 237 КПК України). В інших процесуальних кодексах, на відміну від кримінального процесуального закону, законодавець наводить примірний перелік джерел електронних (цифрових) доказів. Так, відповідно до ч. 1 ст. 96 ГПК України, ч. 1 ст. 99 КАС України і ч. 1 ст. 100 ЦПК України, такі докази «можуть зберігатися, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет)».

До визначення переліку джерел електронних (цифрових) доказів у своїй практиці неодноразово звертається ККС ВС. При цьому в одних випадках ним наводиться перелік джерел таких доказів, який в повному обсязі відповідає їх переліку, визначеному ч. 1 ст. 96 ГПК України, ч. 1 ст. 99 КАС України і ч. 1 ст. 100 ЦПК України. Зокрема, в у Постанові від 06.02.2024 р. у справі № 645/6247/16-к ККС ВС вказує на те, що дані, які становлять зміст електронних (цифрових) доказів, «можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет)» [84]. В інших випадках ККС ВС наводить перелік джерел електронних (цифрових) доказів залежно від їх характеру мережі, в якій вони існують: закритою чи відкритою є така мережа. Так, у Постанові ККС ВС від 12.06.2024 р. у справі № 569/1908/23 він зазначає, що до електронних (цифрових) доказів «належать: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), що містяться у відкритих (інтернет; різноманітні засоби масової інформації; соціальні мережі) чи закритих мережах (приватні месенджери та телеграм-канали; особисте листування з використанням комп'ютерної техніки і мобільних телефонів, флеш-носії, карти пам'яті тощо)» [82].

У науці кримінального процесу не сформовано однозначного підходу до виокремлення переліку джерел електронних (цифрових) доказів.

Переважна більшість вчених, звертаючись до визначення видів джерел електронних (цифрових) доказів, наводить їх примірний перелік. Так, І.О. Крицька вважає, що «джерелом таких доказів та, відповідно, формою їх існування є засоби цифрової техніки, якими виступають машинні носії: постійні та оперативні запам'ятовуючі пристрої; переносні машинні носії (флеш-карти, оптичні носії); накопичувачі на жорстких магнітних дисках (дискети, вінчестери); NAS-системи тощо» [57, с. 302] . Більш широкий перелік джерел електронних (цифрових) доказів пропонують виокремлювати Я.В. Жидовцев та Я.В. Мілімко, на думку яких «найбільш поширеними серед них є сайти в комп'ютерній мережі, файли та групи файлів, електронні бази даних, сервери, електронні пошти, чати, записи з відеореєстраторів, камер відеоспостереження та іншого програмного забезпечення, застосунки, встановлені користувачем на планшетах, мобільних телефонах та інших електронних пристроях, тощо» [70, с. 306]. Розробники методичних рекомендацій і практичних посібників, адресованих слідчим, прокурорам, співробітникам оперативних підрозділів, суддям, до джерел електронних (цифрових) доказів відносять різноманітні носії інформації, мобільні пристрої (планшетні комп'ютери, мобільні телефони), цифрові камери, моноблоки, роутери, маршрутизатори, глобальну мережу Інтернет, комп'ютерні мережі, звуко- та відеозаписи тощо [12, с. 7; 72, с. 699]. Заслуговує на увагу проведене низкою вчених і практичних працівників дослідження електронних (цифрових) доказів, які на основі узагальнення матеріалів кримінальних проваджень вказують, що «в ході досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, такі докази містяться: в пам'яті електронно-обчислювальної техніки, планшетів – 98 %; у пам'яті мобільного телефону (історія телефонних з'єднань, голосових і текстових повідомлень, IMEI-код, програмне забезпечення для здійснення за допомогою телефона банківських операцій тощо) – 84 %; в електронній поштовій скриньці – 77 %; на флеш-карті (папки, файли тощо) – 75 %; у відображеній в електронному виді інформації про суми грошових коштів, переказаних за допомогою тієї або

іншої системи електронних платежів («Qiwi-гаманець», «ПриватБанк», Western Union, MoneyGram, Perfect Money тощо) – 59 %; на сервері мобільного оператора – 56 %; у відображеній в профілі у соціальних мережах або розміщеній на сайтах інформації – 43 %; у пам'яті сім-карти – 32 %; на сервері інтернет-провайдера (сервер баз даних, сервер зберігання білінгової інформації та flow-статистики тощо) – 21 %» [161. с. 64].

Низка вчених звертається до класифікації джерел електронних (цифрових) доказів, здійснюючи їх поділ за різними критеріями. Зокрема, В.С. Сезонов і М.Г. Щербаковський, беручи до уваги правову природу джерел електронних (цифрових) доказів, із позицій доказування поділяють їх на дві групи: «1) речові – об'єкти, які у формі файлів містять криміналістично значиму інформацію: використовувані в комп'ютерах об'єкти для зберігання цифрових даних (гнучкі, жорсткі, оптичні, магнітооптичні диски; електронні пристрої зі схожими функціями); персональні електронні прилади (PEDs), персональні цифрові помічники (PDAs), мобільні телефони, карти пам'яті; цифрові фото- та відеокамери (зокрема, CCTV); стандартні комп'ютери з мережевими з'єднаннями; мобільні навігаційні системи; мережі, засновані на цифрових протоколах (TCP/IP та інших), а також прилади з подібними функціями; 2) електронні – електронне середовище, в якому криміналістично значима інформація міститься у формі електронних документів (документів, поєднані з конкретним матеріальним носієм, який вилучено за певних обставин у конкретної особи або у встановленому місці як доказ факту або обставин кримінального провадження, але які володіють доказовим значенням безвідносно до матеріального носія): локальні та глобальні мережі; хмарні сховища; електронні реєстри (зброї, іпотек, речових прав на нерухоме майно тощо)» [162, с. 15]. Схожий підхід висловлюють Ю.Ю. Орлов і С.С. Чернявський, котрі на підставі дослідження слідчої практики наводять види джерел електронних (цифрових) доказів залежно від місця виявлення таких доказів: «1) виявлені в оглянутому або обшукуваному приміщенні чи на місцевості: на автономному електронному носії (автономний електронний

накопичувач, флешка), на спеціалізованому пристрої (смартфон, цифровий фотоапарат, диктофон тощо) чи на пристрої пам'яті ноутбука або стаціонарного комп'ютера; 2) виявлені в мережі Інтернет поза межами оглянутого або обшукуваного приміщення чи місцевості (розташовані на віддаленому сервері, доступ до якого здійснюється з ноутбука або стаціонарного комп'ютера)» [75, с. 18]. За цим критерієм В.В. Романюк і Т.Г. Фоміна виокремлюють три групи джерел електронних (цифрових) доказів: «1) які містяться у відкритих мережах: засоби масової інформації; інтернет; соціальні мережі (зокрема, сторінки у соціальних мережах і веб-сайти, відкриті телеграм-канали, різноманітні медіа); 2) які містяться в закритих мережах; 3) які наявні в осіб: флеш-носії; карти-пам'яті; приватні месенджери; здійснюване з використанням комп'ютерної техніки і мобільних телефонів особисте листування» [108, с. 346-347].

Розгалужену класифікацію джерел електронних (цифрових) доказів наводить І.Г. Каланча, котра з урахуванням особливостей цифрового середовища поділяє їх за декількома критеріями: «1) за доступністю: а) локальні носії (фізично доступні для огляду та, за потреби, вилучення): смартфони, ноутбуки, зовнішні диски тощо; б) віддалені носії (фізично розташовані поза межами контролю суб'єкта, але з наявністю логічного доступу за допомогою мережевих протоколів): поштові сервери, хмарні сховища, облікові записи тощо; в) динамічні носії (генеруються в ході активної мережевої взаємодії та характеризуються тимчасовістю існування): IP-з'єднання, здійснювані в реальному часі сесії обміну повідомленнями, інтерактивні потоки даних тощо; 2) за середовищем зберігання: а) фізичні (матеріальні пристрої з елементами пам'яті): жорсткі диски, маршрутизатори, флеш-накопичувачі тощо; б) віртуальні (існують у хмарних чи ізольованих віртуальних середовищах, фізично розташовані поза межами досяжності суб'єкта, але містять значимі для кримінального провадження дані): віртуальні машини, контейнери, сервери в дата-центрах; 3) за типом пам'яті: а) постійна (дозволяє зберегти інформацію після вимкнення пристрою): HDD, SSD тощо;

б) тимчасова (забезпечує високу швидкість доступу, але внаслідок завершення роботи пристрою або сесії втрачає вміст): RAM, кеш; в) розподілена (функціонує в децентралізованих системах, в яких у результаті реплікації інформації на множині вузлів ускладненим є її вилучення та автентифікація): блокчейн-платформи, P2P-мережі» [34, с. 141-142]. Поряд із наведеною класифікацію, вчена звертається до поділу електронних носіїв інформації з урахуванням їх технічної конструкції та здійснює його за такими критеріями: «1) за ступенем інтеграції електронного носія з інформаційною системою: а) відокремлені від інформаційної системи (знімні носії, які доступні для суб'єкта як окремі пристрої для зберігання електронної інформації та дослідження яких може здійснюватися після безпосереднього підключення до комп'ютера, ноутбука): карти пам'яті, дискети, оптичні диски, USB флеш-накопичувачі, твердотілі накопичувачі, накопичувачі на жорстких магнітних дисках, стрічкові картриджі тощо; б) вбудовані в інформаційну систему (носії існують у складі мобільного телефона, комп'ютера чи іншої інформаційної системи), які поділяються на носії, які можуть від'єднуватися (відокремлюватися) від цієї системи без втрати властивостей, та носії, від'єднання (відокремлення) яких від інформаційної системи є можливим шляхом фізичного знищення структурних елементів і, відповідно, порушення цілісності цієї системи; 2) за типом запам'ятовуючого пристрою: а) оперативний, яким є енергозалежна пам'ять (зберігає електронну інформацію в обмеженій кількості протягом сеансу роботи інформаційної системи до її вимкнення); б) енергонезалежний (non-volatile storage), який становить енергонезалежна пам'ять (зберігає електронну інформацію після завершення сеансу роботи інформаційної системи та її вимкнення, тобто за відсутності живлення)» [34, с. 142-144].

Аналіз наведених підходів, дозволяє стверджувати, що система джерел електронних (цифрових) доказів не обмежується виключно матеріальними (фізичними) носіями електронної інформації, оскільки вона може відображатися на відповідних віртуальних носіях. Визначення електронного

середовища як одного з джерел електронних (цифрових) доказів також не є коректним з огляду на відображення цих доказів у конкретній інформаційній системі, електронній комунікаційній системі, хмарному сховищі тощо. Відповідно, система джерел електронних (цифрових) доказів повинна включати як матеріальні (фізичні), так і віртуальні носії електронної інформації. Це створює передумови для здійснення класифікації джерел електронних (цифрових) доказів і свідчить про її обґрунтованість та практичну значимість здійснення за критерієм місця їх відображення: 1) матеріальні (фізичні) джерела, якими є будь-які електронні пристрої, придатні для відображення електронної інформації; 2) віртуальні джерела, які відображають інформацію, що існує у хмарних сховищах або інших віртуальних середовищах.

У ході досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, джерелами електронних (цифрових) доказів є:

1. Електронні пристрої, які містять значиму для кримінального провадження інформацію. Ними можуть виступати будь-які технічні засоби, в основу роботи яких покладені електронні компоненти та електричні сигнали і які за своїм функціональним призначенням спрямовані на зберігання, оброблення або передання інформації чи виконання певних дій за заданим алгоритмом: комп’ютери, ноутбуки, планшети, смартфони, цифрові фотоапарати і відеокамери, персональні електронні прилади і персональні помічники, мобільні навігаційні системи, гнучкі, жорсткі, оптичні, магнітооптичні диски, карти пам’яті, зовнішні диски, роутери, маршрутизатори тощо. Розробники методичних рекомендацій із використання електронних носіїв інформації як джерел доказів усі електронні носії інформації поділяють на декілька видів, зумовлених фізичними засадами здійснюваного запису інформації на них та її подальшого зчитування: 1) магнітні (дискети, жорсткі диски, стримери); 2) оптичні (CD-ROM; DVD-ROM); 3) магнітно-оптичні; 4) напівпровідникові – твердотільні на основі використання Flash-пам’яті (SSD), USB Flash Drive (флешка) [13, с. 15].

У разі, якщо електронний пристрій керується за допомогою програми або здійснює оброблення інформації за заданим алгоритмом, його робота здійснюється з використанням програмного забезпечення, що складається з відповідних програм, які надають йому інструкції. Для позначення електронних пристроїв, які здійснюють автоматичне оброблення даних, у Конвенції про кіберзлочинність від 23.11.2001 р., ратифікована із застереженнями і заявами Законом України від 07.09.2005 р. № 2824-IV використовується термін «комп'ютерна система». Так, згідно з п. «а» ст. 1 цієї Конвенції, ««комп'ютерна система означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних» [50].

Як вказує Д.О. Московчук, «значний спектр використовуваного на комп'ютерах, планшетах, ноутбуках і мобільних телефонах програмного забезпечення, включаючи програми, надають користувачу можливість створювати бази даних і текстові документи, готувати електронні таблиці та презентації, надсилати повідомлення, робити цифрові фотографії, створювати мультимедіа тощо, а файли, які міститимуть бази даних, електронні тексти і таблиці, презентації, повідомлення, фотографії, мультимедіа самі по собі можуть виступати електронними доказами» [71, с. 33]. Поряд з існуванням у пам'яті вказаного носія, вони можуть бути збережені на знімному носії інформації (карті пам'яті, зовнішньому диску, оптичному диску тощо).

2. Електронні комунікаційні системи, які використовувалися в ході підготовки до кримінальних правопорушень у кіберпросторі, їх вчинення та приховування наслідків цих правопорушень. Відповідно до п. 28 ч. 1 ст. 2 Закону України «Про електронні комунікації» від 16.12.2020 р. № 1089-IX, «електронна комунікація (телекомунікація, електрозв'язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій» [95]. Поняття електронних комунікаційних систем міститься в Законі України «Про основні засади забезпечення кібербезпеки України» від

05.10.2017 р. № 2163-VIII, згідно з п. 21 ч. 1 ст. 1 якого «системи електронних комунікацій – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-комунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних» [97].

До числа таких електронних комунікаційних систем, які є джерелом електронних (цифрових) доказів у провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі, належать: електронна пошта, месенджери і соціальні мережі. Доступ до електронних комунікаційних систем забезпечує ознайомлення зі змістом повідомлень, які передаються ними, і дозволяє ідентифікувати користувача. Як вказує В.В. Луцик, «у комп'ютерних мережах повідомлення можна відстежити за допомогою: а) IP-адреси, присвоєною у відповідній комп'ютерній мережі конкретному комп'ютеру; б) MAC-адреси – ідентифікаційної адреси комп'ютерного обладнання; в) адреси електронної поштової скриньки; г) даних, відображених в облікових записах користувачів соціальних мереж, чатів, форумів, блогів; д) ідентифікаційного номеру UIN, який надається користувачам ICQ» [36, с. 169]. Ідентифікаційними ознаками, на основі яких можна унікально ідентифікувати користувача, як зазначають із посиланням на положення Закону України «Про електронні комунікації» від 16.12.2020 р. № 1089-IX і підзаконних нормативно-правових актів С.О. Ковальчук і Г.Р. Крет, є: 1) у разі зняття інформації з мережі Інтернет – її адреса, тобто визначений чинними в мережі Інтернет міжнародними стандартами символьний та/або цифровий ідентифікатор; 2) у разі зняття інформації з інших мереж зв'язку –

абонентський номер чи інший мережевий ідентифікатор, тобто індивідуальний набір цифрових знаків або інших символів для позначення (ідентифікації) абонента в електронній комунікаційній мережі [43, с. 140].

3. Сервери постачальників електронних комунікаційних послуг, хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів.

Із урахуванням пунктів 79-81, 87 ч. 1 ст. 2 Закону України «Про електронні комунікації» від 16.12.2020 р. № 1089-IX, постачальник електронних комунікаційних послуг на власних мережах чи мережах інших постачальників надає такі послуги: 1) голосової електронної комунікації, що полягає в «обміні інформацією голосом у реальному часі з використанням електронних комунікаційних мереж та номерів національного або міжнародного плану нумерації»; 2) доступу до мережі Інтернет, яка «забезпечує доступ до мережі Інтернет і можливість логічного з'єднання з кінцевими точками мережі Інтернет незалежно від технології, що застосовується в електронній комунікаційній мережі, і кінцевого (термінального) обладнання, що використовується»; 3) міжособистісної електронної комунікації, яка «дає змогу здійснювати прямий міжособистісний та інтерактивний обмін інформацією через електронні комунікаційні мережі між обмеженою кількістю осіб, за якого особи, які ініціюють або беруть участь у комунікації, визначають одержувача (одержувачів) інформації (крім послуг, що дають змогу міжособистісного та інтерактивного спілкування лише як незначну допоміжну функцію, невід'ємно пов'язану з іншою послугою)» [95].

Надання електронних комунікаційних послуг здійснюється їх постачальником із використанням серверів. Сервером є комп'ютер або спеціалізована програмна система, призначена для надання даних, ресурсів і послуг іншим користувачам шляхом зберігання інформації, оброблення запитів і повідомлень, керування доступом. Кожен сервер має унікальну IP-адресу (числову послідовність, яка є ідентифікатором девайсу для Інтернет-сервера), що дозволяє встановити місце його знаходження [41, с. 168]. Усі

запити і повідомлення користувача надходять на сервер, після чого за допомогою маршрутизатора направляються абонентам, а на сервері постачальника електронних комунікаційних послуг фіксуються та зберігаються дані про їх відправника [64, с. 501].

Як наголошує Д.О. Московчук, «джерела електронних (цифрових) доказів із серверів включають записи журналів, з яких можна отримати інформації про час підключення користувача до сервера, незалежно від того, завантажує він електронну пошту чи надає доступ до інтернету» [71, с. 38]. Така інформація, за слушним зауваженням О.О. Торбаса, «у кримінальному провадженні має більш істотне значення, ніж місце фактичного знаходження сервера, яке жодним чином не впливає на вчинене кримінальне правопорушення» [125, с. 109-110]. Натомість, на самому сервері постачальника електронних комунікаційних послуг, як вказує О.А. Самойленко, відбувається протоколювання у вигляді log-файлів (спеціальних файлів реєстрації) технічної інформації, яка відображає дані про бази даних і технічний обмін [111, с. 124]. Як зазначає О.Ю. Довженко, «log-файл являє собою журнал автоматичної реєстрації подій, фіксація яких здійснюється в ході використання програми; кожній події зазвичай відповідає один запис у log-файл, який вноситься одразу після неї та відображається у визначеному самою програмою файлі чи пересилається нею іншій програмі, призначеній для ведення log-файлів» [29, с. 141].

Поряд із серверами постачальників електронних комунікаційних послуг, джерелом електронних (цифрових) доказів у провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі, є хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів. Відповідно до норм ч. 1 ст. 2 Закону України «Про хмарні послуги» від 17.02.2022 р. № 2075-IX, надавач хмарних послуг надає хмарні послуги – послуги з надання, за допомогою використання технології хмарних обчислень, хмарних ресурсів, якими є «будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, доступ до яких

забезпечують технології хмарних обчислень, зокрема процесорний час (обчислювальна потужність), місце у сховищах даних, обчислювальні мережі, бази даних і комп'ютерні програми», а надавач послуг центру обробки даних – «послуги із зберігання та обробки даних, у тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди комунікаційних стійок, послуг хостингу» [99].

Хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів можуть бути джерелом електронних (цифрових) доказів, якими є: 1) дані, які зберігаються у хмарних ресурсах надавачів хмарних послуг і центрів обробки даних, що перебувають у володінні надавачів послуг таких центрів; 2) дані про доступ до цієї інформації користувача хмарних послуг або центру обробки даних; 3) дані про наявність резервних копій такої інформації та систем даних і про передання резервних копій інформації користувачу; 4) дані про несанкціоновані дії, спрямовані на доступ до інформації, яка зберігається у хмарному сховищі або центрі обробки даних (існування зовнішніх і внутрішніх загроз, кібератаки та інциденти кібербезпеки); 5) дані про знищення інформації та її резервних копій.

Наведені види джерел електронних (цифрових) доказів, із урахуванням бурхливого розвитку цифрових технологій, із плином часу можуть не відображати усієї багатоманітності їх системи. У зв'язку з цим у ході розробки і подальшого внесення доповнень до кримінального процесуального закону потрібно зважати на це і закріпити джерела електронних (цифрових) доказів шляхом наведення їх відкритого переліку.

Результати проведеного дослідження дозволяють стверджувати, що джерелами електронних (цифрових) доказів є будь-які електронні носії фактичних даних, які існують у фізичному або віртуальному виді. До джерел електронних (цифрових) доказів у ході досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, належать: 1) електронні пристрої, які містять значиму для кримінального провадження інформацію; 2) електронні комунікаційні системи, які використовувалися в

ході підготовки до кримінальних правопорушень у кіберпросторі, їх вчинення та приховування наслідків цих правопорушень; 3) сервери постачальників електронних комунікаційних послуг, хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів.

Із метою формування однозначного розуміння джерел електронних (цифрових) доказів до пропонованого в попередньому підрозділі проєкту ст. 99-1 КПК України «Електронні (цифрові) докази» необхідно включити ч. 3 у такій редакції:

«3. Електронні (цифрові) докази можуть бути отримані з електронних пристроїв, електронних комунікаційних систем, серверів, хмарних ресурсів, центрів обробки даних та з інших місць зберігання даних в електронній формі».

РОЗДІЛ 3. ОСОБЛИВОСТІ ЗБИРАННЯ ТА ПЕРЕВІРКИ ДОКАЗІВ ПРИ ЗДІЙСНЕННІ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

3.1. Слідчі (розшукові) дії при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі

Слідчі (розшукові) дії виступають основним способом збирання доказів у кримінальному провадженні. У ч.1 ст. 223 КПК України визначено, що слідчі (розшукові) дії є «діями, спрямованими на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні».

Їх проведення допускається лише за наявності достатніх відомостей, що вказують на можливість досягнення мети такої дії, що прямо випливає із положень ч.2 ст. 223 КПК України. Саме за допомогою слідчих (розшукових) дій здійснюється встановлення фактичних обставин кримінального провадження, передбачених ст. 91 КПК України, а також перевірка вже отриманих доказів.

Водночас, у контексті інституту слідчих (розшукових) дій важливе значення має й належна правова процедура, адже їх проведення так чи інакше пов’язане із обмеженням прав та свобод громадян. В цьому ключі виникає чи не найбільше проблем, адже кримінальне процесуальне законодавство не містить спеціальних норм щодо розслідування кримінальних правопорушень, вчинених у кіберпросторі. Фактично, у зв’язку із цим перед правозастосувачами постає непросте питання, пов’язане із адаптацією чинних норм, які регламентують порядок та способи збирання доказів у кримінальному провадженні до ситуацій, коли відповідні докази мають цифровий характер.

Саме тому, доцільність проведення тих чи інших слідчих (розшукових) дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі залежить переважно від криміналістичної методики розслідування того чи іншого кримінального правопорушення.

Так, наприклад, К.О. Чаплинський, А.В. Рейнгодьд та Н.В. Павлова, досліджуючи методику розслідування шахрайства у сфері інтернет-комерції, зазначають, що «при розслідуванні даної категорії кримінальних правопорушень здебільшого проводяться такі слідчі (розшукові) та негласні слідчі (розшукові) дії: допит; проведення допиту в режимі відео-конференції; пред'явлення особи для впізнання; пред'явлення особи для впізнання в режимі відео конференції; пред'явлення речей для впізнання; обшук; огляд; слідчий експеримент; проведення експертизи; отримання зразків для експертного дослідження» [68, с. 119].

Л.П. Гринько, досліджуючи питання фішингу як способу вчинення Інтернет-шахрайства називає «найбільш розповсюдженими слідчими (розшуковими) діями початкового етапу цього кримінального правопорушення : обшук, огляд предметів вилучених під час проведення обшуку за місцем проживанням підозрюваного, чи іншого помешкання де можуть бути предмети, за допомогою яких здійснювалось відповідне кримінальне правопорушення, допит потерпілого та підозрюваного, призначення судових експертиз» [22, с. 35].

Досліджуючи питання розслідування шахрайства у сфері використання банківських електронних платежів, І.О. Коваленко указує на такі найбільш поширені слідчі (розшукові дії) першочергового етапу розслідування цієї категорії кримінальних правопорушень: «1) огляд місця події (59 %); допит потерпілого або представника потерпілої сторони (100 %); 2) огляд ЕОТ, документів (85 %); 3) освідування (1 %); 4) допит свідка (14 %); 5) допит підозрюваного (87 %); обшук (58 %); призначення судових експертиз (100 %); слідчий експеримент (6 %); пред'явлення особи для впізнання (5 %); одночасний допит раніше допитаних осіб (18 %)» [41, с. 127].

Авторським колективом посібника «Теоретичні та праксеологічні засади розслідування кримінальних правопорушень у кіберпросторі» виокремлено такі слідчі (розшукові) дії, які зазвичай проводяться при розслідуванні відповідних кримінальних правопорушень: «1) допит підозрюваного (100 %); 2) допит потерпілого або представника потерпілої сторони (100 %); 3) огляд ЕОТ, документів (100 %); 3) призначення судових експертиз (100 %); 3) обшук (72 %); 4) огляд місця події (61 %); 4) одночасний допит раніше допитаних осіб (43 %);– допит свідка (34 %); слідчий експеримент (5 %); пред'явлення особи для впізнання (4 %); освідування (2 %)» [121, с. 120].

Аналіз наведених наукових джерел засвідчує, що загалом перелік слідчих (розшукових), які можуть проведені при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі зумовлений конкретною слідчою ситуацію, яка виникла у тому чи іншому провадженні.

Саме тому, у межах нашої роботи ми вважаємо за доцільне звернутись до деяких проблемних питань регламентації проведення окремих слідчих (розшукових) дій, які проводяться під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. І найперше, у цьому контексті слід розглянути деякі теоретико-прикладні проблеми проведення огляду.

У ч.1 ст. 237 КПК України передбачено, що огляд проводиться «з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та комп'ютерних даних».

Одним із найбільш дискусійних аспектів правозастосовної практики є питання здійснення огляду веб-сторінок та відомостей із відкритих джерел у межах кримінального провадження. Під час досудового розслідування кримінальних правопорушень, учинених у кіберпросторі, проведення цієї слідчої (розшукової) дії набуває особливої актуальності.

Разом із тим КПК України лише опосередковано врегульовує використання інформації, отриманої з відкритих джерел, зокрема з веб-сайтів,

у доказуванні. Так, у ст. 99 КПК України закріплено загальні вимоги до допустимості електронних документів, тоді як чіткого процесуального порядку збирання та фіксації відомостей, розміщених у мережі Інтернет закон не містить. Зазначена прогалина особливо загострюється в умовах здійснення кримінального провадження in absentia відносно осіб, підозрюваних або обвинувачених у вчиненні кримінальних правопорушень, передбачених ст.ст. 111[1] та 436[2] КК України, які перебувають на тимчасово непідконтрольних територіях. У таких провадженнях інформація, оприлюднена на веб-сторінках, часто виступає чи не єдиним доказом, оскільки можливості отримання доказів іншими процесуальними способами є істотно обмеженими. Водночас огляд інтернет-ресурсів зберігає значення і при розслідуванні інших категорій кримінальних правопорушень, зокрема шахрайств, учинених із використанням мережі Інтернет.

Слід зауважити, що ця проблематика вже тривалий час перебуває у фокусі наукових досліджень. Так, О.В. Малахова обґрунтовує необхідність фіксації огляду веб-сторінки шляхом складення відповідного протоколу та визначає перелік відомостей, які мають бути в ньому відображені [64, с. 68]. Більш розгорнуту структуру такого процесуального документа запропонувала А.В. Ратнова [103, с. 99-100].

У свою чергу А.В. Коваленко, звертаючись до питання щодо розслідування колабораційної діяльності, зазначає, що типовими об’єктами огляду у справах за ст. 111[1] КК України є веб-сторінки, облікові записи в соціальних мережах, публічні канали у месенджерах тощо [39, с. 416].

Водночас у науковій літературі висловлюється й протилежна позиція. Зокрема, В.І. Школьніков вважає огляд веб-сторінок у кримінальному провадженні неправомірним, вказуючи на порушення засад кримінального процесу, та наполягає на необхідності збирання такої інформації виключно шляхом зняття інформації з електронних інформаційних систем відповідно до ч. 2 ст. 264 КПК України [161, с. 174].

Ми погоджуємось із тими дослідниками, які вважають, що належним способом збирання відомостей, що розміщені у мережі Інтернет є саме складення протоколу огляду веб-сторінки, а не проведення негласних слідчих (розшукових) дій, оскільки в даній ситуації відсутня ключова ознака таких заходів – нерозголошення відомостей про факт та методи її проведення.

У правозастосовній практиці протоколи огляду веб-сторінок та інших інтернет-ресурсів загалом визнаються судами допустимими джерелами доказів. Разом із тим, визначальною проблемою при їх оцінці залишається встановлення достовірності зафіксованих відомостей, оскільки у більшості випадків відсутня можливість ідентифікувати осіб, які безпосередньо розмістили відповідну інформацію в мережі Інтернет. Така неможливість перевірки джерела походження відомостей об'єктивно породжує сумніви щодо їх достовірності, які відповідно до вимог ч. 4 ст. 17 КПК України підлягають тлумаченню на користь обвинуваченого.

Показовою у цьому аспекті є постанова Третьої судової палати ККС ВС, у якій протокол огляду інтернет-сторінки було визнано належним і допустимим доказом з огляду на те, що об'єктом огляду виступали офіційні веб-сайти державних органів держави-агресора, що істотно підвищувало рівень довіри до розміщеної на них інформації [92].

Водночас у постанові Третьої судової палати ККС ВС від 25 жовтня 2023 року, ухваленій за результатами перегляду судових рішень у кримінальному провадженні щодо обвинувачення особи у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 111 КК України, пов'язаного з незаконним зайняттям посади в окупаційному органі влади, суд звернув увагу на іншу обставину. Зокрема, було наголошено, що протокол огляду веб-сторінок не виступав єдиним доказом у справі, а оцінювався у сукупності з іншими доказами, що в цілому дозволило дійти висновку про доведеність обвинувачення. Факт зайняття посади підтверджувався, зокрема, й «іншими наявними у справі відомостями, зокрема з копіями судових рішень судді Арбітражного суду Республіки Крим «ОСОБА_8», що були отримані

ПАТ «Державний експортно-імпортний банк України» і надалі надіслані до Генеральної прокуратури України, походження та зміст яких у захисту заперечень і сумніву в ході судового розгляду не викликав» [91].

Подібний підхід було реалізовано й у Постанові Другої судової палати ККС ВС від 04 листопада 2021 року [83]. Окрім того, у Постанові Першої судової палати Касаційного кримінального суду від 22 листопада 2018 року суд врахував обставину, що обвинувачений не заперечував відомостей, зафіксованих у протоколі огляду змісту відповідної веб-сторінки [89].

Узагальнення судової практики свідчить про те, що відомості, відображені у протоколах огляду змісту веб-сторінок, дедалі частіше визнаються судами допустимими доказами у кримінальному провадженні. Водночас надання їм такої оцінки не є автоматичним і залежить від сукупності інших обставин, насамперед від можливості перевірки достовірності отриманої інформації, а також від її узгодженості та взаємозв'язку з іншими доказами, зібраними у конкретному кримінальному провадженні.

Підняте питання є складовим більш широкої проблематики збирання доказів із відкритих джерел.

Збройна агресія рф проти України ведеться на різних напрямах, одним із яких є кіберпростір. У зв'язку з цим, у вітчизняній правовій науці та практиці дедалі більшого значення набувають питання, пов'язані зі збиранням і використанням у кримінальному провадженні цифрової інформації, отриманої з відкритих джерел.

Від початку повномасштабного вторгнення у соціальних мережах та месенджерах було оприлюднено значну кількість фотографій, відеозаписів та інших цифрових матеріалів, які фактично містили зафіксовані відомості про вчинення воєнних злочинів. Як зазначає О. Дуфенюк, «наявність у широкого кола користувачів смартфонів, планшетів та інших засобів, розвиток цифрових засобів масової інформації, соціальних мереж як каналу передачі інформації дозволяють транслювати події в онлайн режимі, підтверджувати факти мультимедійними доказами, здійснювати відео та фотографічну фіксацію

перебігу та наслідків події (обстріли, вибухи, пожежі, обвали будівель та споруд, травмування, руйнування, сліди, об’єкти в повітряному просторі тощо), швидко поширювати інформацію серед багатомільйонної аудиторії» [32, с. 52].

У сучасних умовах розвідка з відкритих джерел інформації, зокрема з метою розслідування кримінальних правопорушень та формування криміналістичних версій, уже тривалий час сформувалася як самостійний напрям діяльності, відомий під назвою OSINT (Open Source Intelligence). Джерельну базу OSINT, як правило, становить будь-яка загальнодоступна інформація, доступ до якої не потребує спеціальних дозволів, зокрема дані з веб-сайтів, облікових записів у соціальних мережах, картографічних сервісів, документів, відкритих державних реєстрів тощо. Водночас збирання інформації з відкритих джерел не є випадковим процесом, а являє собою цілеспрямовану діяльність, що потребує дотримання визначених методологічних та етичних правил [146, с. 378].

У 2020 році школою права Університету Каліфорнії в Берклі у співпраці з представниками Організації Об’єднаних Націй було розроблено практичний посібник щодо належного використання цифрової інформації з відкритих джерел під час розслідування порушень міжнародного кримінального права, прав людини та міжнародного гуманітарного права, відомий як Протокол Берклі (Berkeley Protocol).

Варто зазначити, що ще до початку повномасштабної збройної агресії питання застосування OSINT-технологій знаходили відображення у вітчизняній судовій практиці, зокрема у контексті встановлення відомостей про особу [144] або виявлення її активності у соціальних мережах [132]. Нині ж, в умовах гострої потреби української системи кримінальної юстиції у масштабному розслідуванні воєнних злочинів, значення використання таких технологій істотно зросло. У зв’язку з цим актуалізується питання належного нормативного врегулювання відповідного аспекту.

Деякі кроки у цьому напрямку законодавець здійснив. Зокрема, п. 1 ч. 1 ст. 99 КПК України в редакції Закону України № 2137-IX від 15.03.2022 р. передбачає, що документами у кримінальному провадженні можуть виступати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані).

Серед різноманітних аспектів розвідки з відкритих джерел у Протоколі Берклі окрему увагу приділено питанням доказування, підходи до яких можуть істотно відрізнятися залежно від конкретної юрисдикції. У цьому документі підкреслюється, що інформація, розміщена у відкритому доступі, нерідко має змішаний характер і може поєднувати в собі ознаки як документальних доказів, так і свідчень. Зокрема, відеозапис із зафіксованою заявою певної особи потребує належної автентифікації, тоді як зміст висловлювань, що містяться у такому відео, має бути перевірений самостійно та незалежно від самого носія інформації [101]. Варто зауважити, що проблеми, пов'язані з автентифікацією відеоматеріалів, уже набувають практичного значення у вітчизняній правозастосовній діяльності. Суддя Верховного Суду Н. Антонюк вказує, що «традиційно експерти в кримінальних провадженнях звертають увагу на те, що вони можуть робити висновок лише щодо оригіналу відеозапису. Проте в європейських державах існує можливість експертного аналізу достовірності відеозаписів, що не є оригіналами. Тому виникає питання щодо можливості ширшого використання цифрових доказів, отриманих у форматі відео в національному кримінальному процесі» [80]. Як бачимо, вітчизняне законодавство у цьому аспекті дещо не відповідає сучасним потребам правозастосування.

Зазначимо, що ці дані із відкритих джерел доволі активно використовувалися під час здійснення кримінальних проваджень за ст. 438 КПК України. Аналіз постановлених у 2022-2023 р. вироків за ст. 438 КК України «Порушення законів та звичаїв війни» демонструє, що суди подекуди посилалися на відомості, які були отримані із відкритих джерел. Наприклад, у вироку Чернігівського районного суду Чернігівської області вказується

наступне: «У ході пошуку за доступними ресурсами Telegram-бот отримано відомості про належність вказаного номера особі з іменем «ОСОБА_11», ІНФОРМАЦІЯ_1, користувача сторінки «ВКонтакте» ІНФОРМАЦІЯ_4 (алгоритм пошуку оснований по прив'язці номера телефону до акаунта вказаної російської соціальної мережі). Зазначена сторінка створена у 2022 році і є активно використовуваною (останнє відвідування 29 квітня 2022 року)» [16]. Про огляд сторінок у соціальних мережах зазначається також і в інших рішеннях [14]. У вироку Макарівського районного суду Київської області указується, що в судовому засіданні були оглянуті відеозаписи з камер спостереження, наданими потерпілим [15].

Цифрова інформація, отримана з відкритих джерел, нині відіграє суттєву роль у розслідуванні кримінальних правопорушень, що підтверджується сформованою правозастосовною практикою. Водночас відповідний аспект досі залишається недостатньо врегульованим на законодавчому рівні. У зв'язку з цим, дослідження проблем, пов'язаних з отриманням таких даних, їх перевіркою, а також оцінкою допустимості як доказів у найближчій перспективі має стати одним із пріоритетних напрямів розвитку кримінальної процесуальної науки.

Утім, у доктрині вже існують різні позиції з приводу того, якими є правові можливості доказування за допомогою доказів, отриманих із відкритих джерел. Наприклад, І.В. Басиста, Л.В. Гаврилюк, А.В. Гутник та А.В. Хитра зазначають, що «розвідка за відкритими джерелами (OSINT) може бути застосовною для вирішення питання про вжиття заходів забезпечення безпеки (захисту свідків), як довідкова інформація для прийняття рішень, відшукання прихованих активів, які мали б бути обкладені санкціями тощо, але мета доказування нею переслідуватися не може, про що також зазначено у Протоколі Берклі» [6, с. 238].

На доцільність регламентації питання збирання та належного збереження доказів із відкритих джерел вказують також О.В. Бабаєва та Д.В. Авербах [4, с. 174].

О.В. Салманов та А.О. Топчій вважають за необхідне внести зміни до КПК України та дозволити проводити фіксацію таких доказів вчинення воєнних злочинів за допомогою протоколу Берклі громадянам на добровільних засадах, а надалі перевірку та долучення таких матеріалів до кримінального провадження здійснювати слідчими, щоб дані докази були допустимими та належними не лише у міжнародних судових установах, але і у національному судочинстві [109, с. 198].

Питання оцінки доказів, отриманих із відкритих джерел у літературі детально було висвітлено І.В. Гловюк. У контексті перевірки достовірності відповідних доказів, дослідниця зазначила, що: «Якщо ж є сумніви стосовно змісту первинних зафіксованих даних, їх походження у відкритих джерелах (автора контенту, особи, яка його розмістила і мету такого розміщення), створення їх ШІ, створення та поширення їх з метою дезінформації, правильності їх технічного збирання, незмінності онлайн-контенту будь-якого виду, метаданих, хеш-значеннях – мова може йти про недостовірність доказів. У цій ситуації ініціація визнання таких фактичних даних недопустимими доказами позбавлена сенсу. Результати OSINT можуть містити фактичні дані, що не мають властивість належності, але це ніяк не пов’язано з аналізом джерела походження – відкритих даних, адже встановлюється зв’язок (чи його відсутність) з усіма обставинами предмета доказування» [19, с. 258].

Аналіз доктринальних положень і правозастосовної практики дозволяє дійти висновку про те, що використання у кримінальному процесуальному доказуванні доказів із відкритих джерел потребує чіткої регламентації та закріплення оптимальної нормативної моделі. Ми вважаємо, що за допомогою доказів із відкритих джерел можуть бути доведені усі фактичні обставини, які підлягають доказуванню у кримінальному провадженні і визначені у ст. 91 КПК України, і будь-які обмеження у цьому контексті є недоцільними. Але водночас, ми дотримуємось позиції, що обвинувачення не може ґрунтуватися виключно на таких доказах. Тому при визначенні їх допустимості ми вважаємо цілком прийнятною аналогію із показаннями з чужих слів, які відповідно до

ч.6 ст. 97 КПК України не можуть бути допустимим доказом факту чи обставин, на доведення яких вони надані, якщо показання не підтверджується іншими доказами, визнаними допустимими згідно з правилами, відмінними від положень частини другої цієї статті.

Задля цього ми пропонуємо доповнити КПК України ст. 88^2 із назвою «Допустимість доказів, отриманих із відкритих джерел» та викласти її у такій редакції: «Докази, отримані із відкритих джерел можуть бути визнані допустимими виключно за умови підтвердження джерела їх походження та якщо відповідні відомості підтверджуються іншими доказами, які визнані допустимими за правилами цього Кодексу».

Ще одним складним питанням для доктрини та практики є визначення належного процесуального порядку ознайомлення з інформацією, що зберігається на цифрових пристроях, під час розслідування кримінальних правопорушень, учинених у кіберпросторі. Мобільні телефони, комп'ютери, планшети та інші електронні пристрої концентрують значні масиви персональних даних, які відображають приватне життя особи, її комунікації, пересування, професійну та сімейну сферу. Відтак доступ органів досудового розслідування до такої інформації об'єктивно пов'язаний із суттєвим втручанням у право на повагу до приватного і сімейного життя, гарантоване ст. 8 Конвенції про захист прав людини і основоположних свобод.

Дотримання належної правової процедури під час ознайомлення з даними, що містяться на цифрових пристроях, безпосередньо впливає на допустимість отриманих доказів. Нечіткість і суперечливість процесуального порядку доступу до цифрової інформації створює ризики свавільного втручання у приватне життя та подальшого використання таких відомостей у кримінальному провадженні.

Слід звернути увагу на те, що доступ до інформації, яка зберігається на цифрових пристроях, може здійснюватися у межах різних процесуальних дій, зокрема, під час огляду, обшуку, тимчасового доступу до речей і документів, а також у ході проведення негласних слідчих (розшукових) дій. Кожна з

названих процесуальних дій має самостійну правову природу та спеціально визначений порядок проведення, що по-різному впливає на рівень процесуальних гарантій прав і свобод особи. Унаслідок цього в практиці застосування кримінального процесуального законодавства формується складна правова проблема.

Особливо гостро вона проявляється при розмежуванні огляду та окремих негласних слідчих (розшукових) дій, зокрема, зняття інформації з електронних інформаційних систем. Так, відповідно до ч. 2 ст. 264 КПК України, отримання відомостей з електронних інформаційних систем або їх частин не потребує дозволу слідчого судді у випадках, коли доступ до таких систем не обмежується їх власником, володільцем чи утримувачем або не пов’язаний із подоланням засобів логічного захисту. Водночас ч. 1 ст. 237 КПК України у редакції Закону України № 2137-IX від 15 березня 2022 року встановлює, що з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення слідчий або прокурор здійснює огляд місцевості, приміщень, речей, документів, а також комп’ютерних даних.

Фактично внесені зміни до ч. 1 ст. 237 КПК України не усунули, а навпаки загострили наявні суперечності щодо визначення належного процесуального порядку ознайомлення з відомостями, що містяться на цифрових пристроях, що створює додаткові труднощі для правозастосовної практики. Хоча, відповідні питання виникали у правозастосовній практиці й раніше. Зокрема, ще у Постанові ККС ВС від 09 квітня 2020 року було зазначено: «Що ж стосується інформації, яка була наявна в мобільному телефоні ОСОБА_8, то вона була досліджена шляхом включення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем. В даному випадку орган досудового розслідування провів огляд предмета телефона та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону.

За таких обставин Суд не вбачає жодних порушень вимог кримінального процесуального закону при розгляді даного кримінального провадження» [85].

В інших правових позиціях ККС ВС, оцінюючи допустимість відповідних доказів, акцентував увагу, зокрема, на добровільному характері надання цифрових пристроїв. Так, у Постанові ККС ВС від 22 лютого 2024 року Суд дійшов відповідного висновку, визнавши цю обставину істотною для оцінки законності отримання та використання цифрової інформації як доказу у кримінальному провадженні: «Що ж стосується інформації, яка була наявна в мобільному телефоні ОСОБА_7, то вона була досліджена шляхом включення телефону та огляду фотографій і текстових повідомлень, які в ньому знаходились та доступ до яких був наданий власником добровільно. При цьому ОСОБА_7 добровільно коментував наявну інформацію. В даному випадку орган досудового розслідування провів огляд предмета - телефона та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону» [90].

Фактично з наведеної правової позиції суду касаційної інстанції випливає, що добровільна передача мобільного телефону виключає наявність підстав вважати такі дії проведенням негласної слідчої (розшукової) дії. За таких обставин, релевантною процесуальною дією, спрямованою на виявлення та фіксацію відомостей, що містяться у телефоні, визнається саме проведення огляду.

Ця позиція знаходить відображення і у інших рішеннях ККС ВС. Зокрема, у Постанові ККС ВС від 13 березня 2024 року в контексті оцінки допустимості як доказів аудіофайлів, вилучених з мобільного телефону, суд вказав, що «таємниця виключається, якщо абонент (учасник) спілкування не бажає її зберігати і добровільно розкриває, зокрема, перед державними органами. За таких обставин не відбувається втручання у спілкування, а відбувається фіксація добровільно розкритої інформації, яка втрачає статус таємниці й набуває статусу відкритості. Доказом у цьому кримінальному провадженні є аудіофайли, вилучені з телефону самого засудженого, який він

безпосередньо надав органу досудового розслідування та які надалі були предметом дослідження експертом та безпосередньо судом» [88].

Зазначений підхід загалом видається виваженим і таким, що узгоджується із сучасним розумінням меж права на приватність, а також із процесуальними стандартами допустимості доказів у кримінальному провадженні. Вирішальне значення у правовій позиції ККС ВС надається саме добровільному характеру розкриття інформації особою, яка є безпосереднім учасником відповідної комунікації та власником цифрового пристрою. За таких умов, відсутні ознаки прихованого чи примусового втручання з боку представників державної влади у сферу приватного життя, що відповідно до статті 8 Конвенції про захист прав людини і основоположних свобод є ключовим критерієм оцінки правомірності обмеження цього права.

У цьому зв’язку не постає і питання щодо обсягу наданої інформації. Очевидно, що особа, надаючи згоду на ознайомлення зі змістом даних, які зберігаються на цифровому пристрої, повинна усвідомлювати неможливість подальшого контролю за тим, які саме відомості та в якому обсязі стануть доступними у ході відповідної процесуальної дії.

Водночас проблематика належної правової процедури ознайомлення з інформацією, що зберігається на цифрових пристроях, поставала і в ситуаціях, коли вилучення такого пристрою здійснювалося не добровільно, а мало примусовий характер. До прикладу, у Постанові ККС ВС від 09 квітня 2024 року Суд виснував, що «огляд інформації, що міститься в телефоні, не становить собою негласне втручання у приватне спілкування, передбачене § 2 Глави 21 КПК, і доступ до інформації, що містилася в ньому не вимагає отримання окремого дозволу у порядку, визначеному тимчасовим доступом до речей і документів, що регулюється Главою 15 КПК, якщо сторона обвинувачення отримала телефон підозрюваного в своє володіння на підставі законно проведеного обшуку, обставини якого не дають підстав для визнання цього телефону недопустимим доказом» [85].

Зазначимо, що ч.6 ст. 236 КПК України в редакції Закону України № 2137-IX від 15.03.2022 передбачає, що «якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку».

Погодитися з такою регламентацією складно, оскільки фактично йдеться про створення потенційних передумов для втручання у сферу приватного спілкування. Окрім того, сумніви викликає і якість законодавчого формулювання відповідних положень. Зокрема, не достатньо зрозумілим з цієї точки зору є зміст конструкції «виявив доступ чи можливість доступу». Очевидно, що мається на увазі ситуація, коли інформація не захищена паролем або іншими засобами логічного захисту, однак такий нормативний підхід у перспективі може створювати умови для непропорційного втручання та зловживань з боку органів досудового розслідування.

Однак в цьому контексті теж виникає низка питань. По-перше, відповідна норма не є застосовною в контексті особистого обшуку особи в ході затримання. Нормативна модель цієї процесуальної дії лишається вкрай лаконічною та недеталізованою.

Що стосується огляду житла чи іншого володіння особи, то правове регулювання цієї слідчої (розшукової) дії має певні особливості. На її проведення поширюється процесуальний порядок, встановлений для обшуку житла або іншого володіння особи. Крім того, ч. 2 ст. 237 КПК України передбачає, що огляд комп'ютерних даних здійснюється слідчим або прокурором шляхом фіксації у протоколі огляду відомостей, які вони містять, у формі, придатній для сприйняття їх змісту, зокрема із використанням

електронних засобів, фотозйомки, відеозапису, зйомки та/або відеофіксації екрана, а також шляхом відтворення інформації у паперовому вигляді.

Водночас, на відміну від обшуку, огляд житла чи іншого володіння особи, відповідно до усталеної практики ККС ВС, може бути проведений на підставі добровільної згоди особи. У зв'язку з цим, у разі вилучення мобільного телефону або іншого цифрового пристрою під час огляду таке втручання у сферу приватного спілкування фактично здійснюється без попереднього судового дозволу. За таких умов можливим є лише подальший судовий контроль, що у цьому контексті не повною мірою відповідає загальним засадам втручання у приватне спілкування, закріпленим у КПК України [149, с. 640; 151, с. 459].

Виходячи із цього, ми вважаємо, що регламентація огляду цифрових пристроїв під час проведення огляду повинна мати диференційований порядок, що відображав би правові основи проведення цієї слідчої (розшукової) дії. У зв'язку із цим, пропонуємо ч.2 ст. 237 КПК України доповнити абз. третім такого змісту: «Під час огляду житла чи іншого володіння особи виявлення та фіксація комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення огляду можлива лише за добровільною згодою володільця цього майна або якщо дозвіл на такий огляд був наданий в ухвалі слідчого судді».

Слід відзначити, що проблема допустимості огляду мобільного телефону, вилученого під час проведення обшуку, неодноразово ставала предметом наукових дискусій. Так, О.О. Торбас обґрунтовує позицію, відповідно до якої після вилучення мобільного телефону слідчий або прокурор зобов'язані звернутися до слідчого судді з клопотанням про надання тимчасового доступу до речей і документів, а саме — до мобільного телефону, що містить охоронювану законом таємницю. На думку автора, будь-які інші способи доступу до мобільного телефону з метою ознайомлення зі змістом повідомлень слід розцінювати як незаконні [124, с. 309].

Аналогічну позицію щодо правомірності ознайомлення з цифровою інформацією, що міститься у пристроях, вилучених у затриманої особи під час обшуку, висловлює і А.В. Скрипник. Науковець наголошує, що доступ до такої інформації можливий виключно на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів. Водночас без відповідного судового рішення, на його переконання, допускається здійснення лише тих дій, які спрямовані на: а) огляд зовнішнього стану пристрою; б) забезпечення його працездатності (зокрема підключення зарядного пристрою); в) запобігання знищенню або зміні інформації до моменту отримання дозволу на ознайомлення з нею (наприклад, шляхом використання екрана, клітки або щита Фарадея) [115].

Інший підхід до визначення належної процесуальної форми ознайомлення зі змістом інформації, що міститься у мобільному телефоні, обґрунтовує М.І. Пашковський. Учений зазначає, що пошук, виявлення та фіксація відомостей, які зберігаються у смартфоні, а також отримання таких даних у випадках, коли доступ до них обмежується власником, володільцем чи утримувачем або пов’язаний із подоланням засобів логічного захисту, можливі виключно на підставі відповідної ухвали слідчого судді шляхом проведення зняття інформації з електронних інформаційних систем або їх частин [76, с. 111].

Обґрунтовуючи таку позицію, дослідник виходить із того, що в межах процедури тимчасового доступу до речей і документів фактично здійснюється доступ до мобільного терміналу систем зв’язку, який сам по собі не володіє ознаками електронної інформаційної системи. Саме в цій обставині він убачає підставу для чіткого розмежування процесуальних інститутів зняття інформації з електронних інформаційних систем та тимчасового доступу до речей і документів.

Ми також поділяємо позицію, відповідно до якої будь-яке ознайомлення з інформацією, що зберігається на цифрових пристроях, повинно підлягати обов’язковій перевірці слідчим суддею, що узгоджується з конвенційними

стандартами захисту права на приватність, закріпленими у ст. 8 Конвенції про захист прав людини і основоположних свобод. У зв'язку з цим, у випадках, коли особа не надає добровільної згоди на розкриття інформації, а доступ до неї передбачає подолання засобів логічного захисту, належною процесуальною підставою має бути застосування положень ч. 1 ст. 264 КПК України.

Аналіз норм чинного кримінального процесуального законодавства України та практики ККС ВС свідчить про існування неоднозначних і суперечливих підходів до визначення належної процесуальної форми доступу до цифрових даних, зокрема у площині розмежування огляду, тимчасового доступу до речей і документів та окремих негласних слідчих (розшукових) дій [152, с. 640].

У ситуаціях, коли особа добровільно надає мобільний телефон або інший цифровий пристрій для ознайомлення, саме огляд слід розглядати як релевантну слідчу (розшукову) дію, спрямовану на фіксацію відомостей, що в ньому містяться. Такий підхід відповідає стандартам забезпечення права на приватність, оскільки особа усвідомлює, що, надаючи згоду на доступ, вона не може повністю контролювати обсяг розкритої інформації.

Водночас положення ч. 6 ст. 236 КПК України в частині використання формулювання «виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку» потребує коригування, оскільки не відповідає вимозі передбачуваності закону та створює передумови для зловживань з боку сторони обвинувачення.

У зв'язку із цим, пропонуємо викласти абзац другий ч.6 ст. 236 КПК України у такій редакції: «Прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення обшуку виключно якщо дозвіл на такий пошук наданий в ухвалі слідчого судді». Така регламентація відповідатиме міжнародним стандартам та стандартам, виокремленим ЄСПЛ у частині захисту права на повагу до

приватного життя. Чинна редакція абз. 2 ч.6 статті 236 КПК України може бути актуальною лише в умовах воєнного стану, коли публічний інтерес розслідування злочинів проти основ національної безпеки превалює над приватним, але передбачений нею порядок не може виступати ординарною правовою процедурою.

Отже, будь-який доступ до інформації, що зберігається на цифрових пристроях, має здійснюватися за умови судової перевірки правомірності такого втручання слідчим суддею, що відповідає конвенційним стандартам захисту права на приватність, передбаченим ст. 8 Конвенції. Таким чином, у випадках відсутності добровільної згоди власника цифрового пристрою на розкриття інформації та за необхідності подолання логічних засобів захисту, застосуванню підлягає процедура, визначена ч. 1 ст. 264 КПК України.

3.2. Негласні слідчі (розшукові) дії та інші процесуальні дії при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі

Особливість кримінальних правопорушень, вчинених у кіберпросторі полягає в тому, що більшість належних і допустимих доказів мають електронну форму та знаходяться в електронних комунікаційних мережах, зберігаються у провайдерів телекомунікацій або передаються в режимі реального часу. За таких умов, такі негласні слідчі (розшукові) дії, зокрема зняття інформації з електронних комунікаційних мереж, зняття інформації з електронних інформаційних систем чи встановлення місцезнаходження радіообладнання (радіоелектронного засобу), часто є чи не єдиними ефективними процесуальними діями, проведення яких дає змогу зібрати відповідні докази та встановити фактичні обставини кримінального провадження, зокрема, у контексті встановлення маршрутів передавання

даних, ролі конкретних технічних засобів та взаємозв'язків між учасниками злочинної діяльності.

Водночас, важливе значення для повного та всебічного встановлення фактичних обставин при здійсненні досудового розслідування мають й інші процесуальні дії, що не є слідчими (розшуковими) діями за своєю правовою природою, але спрямовані на забезпечення отримання засобів доказування. Зокрема, до них слід віднести тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо, арешт комп'ютерних систем чи їх частин, а також окремі процесуальні дії у межах міжнародного співробітництва. Деякі із них слід розглянути детальніше.

Передусім, у контексті нашого дослідження необхідно визначитися із колом НС(Р)Д, які можуть бути проведені у кримінальних провадженнях щодо кримінальних правопорушень, які вчиняються у кіберпросторі.

О.Ю. Довженко з цього приводу зазначає, що при під час розслідування кіберзлочинів можливим є застосування таких негласних слідчих (розшукових) дій, як аудіо- чи відеоконтроль особи (ст. 260 КПК України), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України), а також зняття інформації з електронних інформаційних систем (ст. 264 КПК України). Водночас, проведення арешту кореспонденції (ст. 261 КПК України), а також огляду і виїмки кореспонденції (ст. 262 КПК України) на практиці є фактично неможливим, оскільки для цілей цих норм кореспонденцією визнаються виключно листи, бандеролі, посилки, поштові контейнери, грошові перекази, телеграми та інші матеріальні носії передавання інформації між особами. Таким чином, зазначені положення прямо виключають можливість віднесення електронного листування до поняття кореспонденції. Крім того, автор звертає увагу на суперечливість правової регламентації та, як наслідок, обмеженість застосування такого заходу, як моніторинг банківських рахунків (ст. 269 КПК України), який може

здійснюватися лише у кримінальних провадженнях щодо тяжких або особливо тяжких злочинів, до категорії яких більшість кіберзлочинів не належать [29, с. 108].

Ю. О. Виходець, В. Г. Дрозд, М. М. Єфімов, В. Б. Коба, І. О. Луговий, Н. В. Павлова, К. О. Чаплинський на підставі узагальнення слідчої практики зазначають, що специфічною ознакою кримінальних правопорушень у кіберпросторі є необхідність проведення цілого ряду НСРД та ОТЗ, пов'язаних із встановленням кіберзлочинця та його зв'язків, серед яких 1) аудіо-, відеоконтроль особи; 2) зняття інформації з електронних комунікаційних мереж; 3) зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача; 4) спостереження за особою в публічно доступних місцях; аудіо-, відеоконтроль місця [121, с. 154].

О.Р. Пелещак, досліджуючи питання щодо початкового етапу розслідування кібердиверсій указує, що аби «зробити висновки, висунути версії щодо причетності особи або групи осіб до вчиненого кримінального правопорушення повинні бути проведені відповідні негласні слідчі (розшукові) дії, зокрема аудіо-, відеоконтроль особи (ст. 260 КПК України), накладення арешту на кореспонденцію (ст. 261 КПК України), огляд і виїмка кореспонденції (ст. 262 КПК України), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України) та електронних інформаційних систем (ст. 264 КПК України), фіксація та збереження інформації, отриманої з телекомунікаційних мереж за допомогою технічних засобів та в результаті зняття відомостей з електронних інформаційних систем (ст. 265 КПК України), спостереження за особою, річчю або місцем (ст. 269 КПК України), аудіо-, відеоконтроль місця (ст. 270 КПК України)» [78, с. 98].

Аналіз наведених доктринальних позицій дозволяє дійти висновку про доволі типовий перелік НСРД, який проводиться у кримінальному провадженні щодо кримінальних правопорушень, вчинених у кіберпросторі.

Характер нашого дослідження вимагає більш детального аналізу нормативної регламентації та практики реалізації окремих НСРД, зокрема, зняття інформації з електронних комунікаційних мереж

У ч.1 ст. 263 КПК України зазначається, що «зняття інформації з електронних комунікаційних мереж (комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг) є різновидом втручання у приватне спілкування, що проводиться без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можливо встановити обставини, які мають значення для кримінального провадження».

Відзначимо, що назва відповідної НСРД у первісній редакції кодексу була іншою – зняття інформації з транспортних телекомунікаційних мереж. Утім, Законом України № 2137-IX від 15.03.2022 була змінена на чинну. До речі, у доктрині деякі автори наголошують на некоректності такої новелізації. Наприклад, В.В. Луцик зазначає, що «таке визначення не повністю узгоджується із європейськими стандартами у сфері електронних комунікацій. Зокрема, згідно п. 1. ч. 1 ст. 2 Директиви «Про запровадження Європейського кодексу електронних комунікацій» «електронна комунікаційна мережа» означає системи передачі, незалежно від того, чи вони базуються на постійній інфраструктурі або централізованому адмініструванні потужностей, і, якщо застосовно, обладнання для комутації або маршрутизації та інші ресурси, включаючи неактивні елементи мережі, які дозволяють передавати сигнали через дротові, радіо-, оптичні або інші електромагнітні засоби, включаючи супутникові мережі, мережі фіксованого (з комутацією каналів та з комутацією пакетів, включаючи Інтернет) та мобільного зв’язку, електросилові кабельні системи, в тій мірі, в якій вони використовуються для передачі сигналів, мережі радіо- та телевізійного мовлення та мережі кабельного телебачення, незалежно від типу переданої інформації» [64, с. 501].

Відповідно до Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні зняття інформації з транспортних телекомунікаційних мереж поділяється на два види: «1) контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється; 2) зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються» [33].

У літературі неодноразово указувалось на завдання, які переслідуються проведенням саме цієї НС(Р)Д. Зокрема Ж.В. Удовенко у межах свого дослідження зазначає, що найчастіше зняття інформації з електронних комунікаційних мереж спрямоване на: «1) встановлення обставин, що мають значення для кримінального провадження – в 39 % випадків; 2) встановлення злочинних зв’язків, виявлення можливих співучасників злочину – 34,5 %; 3) виявлення фактів протидії розслідуванню – 9,6 %; 4) встановлення місцезнаходження розшукуваних осіб – 4,2 %; 5) встановлення місцезнаходження викраденого майна – 4,2 %; 6) завдання, пов’язані з оперативно-розшуковою діяльністю – 2,1 %; 7) завдання не були конкретизовані – 6,4 %» [127, с. 123].

В доктрині існує дискусія щодо можливості проведення зняття інформації з електронних комунікаційних мереж до постановлення відповідної ухвали слідчим суддею у невідкладних випадках. У ст. 250 КПК України зазначається про те, що «у виняткових невідкладних випадках, пов’язаних із врятуванням життя людей та запобіганням вчиненню тяжкого

або особливо тяжкого злочину, передбаченого розділами I, II, VI, VII (статті 201 та 209), IX, XIII, XIV, XV, XVII Особливої частини Кримінального кодексу України, негласна слідча (розшукова) дія може бути розпочата до постановлення ухвали слідчого судді *у випадках, передбачених цим Кодексом*, за рішенням слідчого, узгодженого з прокурором, або прокурора». Системний аналіз Глави 21 КПК України дозволяє виділити тільки дві НСРД, які можуть бути розпочаті до постановлення ухвали слідчим суддею – це установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ч.4 ст. 268 КПК України) та спостереження за особою (ч.3 ст. 269 КПК України). Відповідно, зняття інформації з електронних комунікаційних мереж до цього переліку не належить.

В.Г. Уваров, посилаючись на законодавчий досвід ФРН у цьому контексті зазначає, що у вказаному правопорядку розпорядження про контроль і фіксацію інформації, що передається засобами телекомунікації, може дати тільки суддя. У разі небезпеки зволікання розпорядження може бути віддано й прокуратурою. При цьому розпорядження прокуратури втрачає чинність, якщо воно не буде підтверджено суддею протягом трьох днів» [126, с. 123]. Автор відстоює позицію, що таке правове регулювання відповідає практичним потребам. Нерідко зняття інформації з технічних каналів зв’язку потребує невідкладного реагування, тоді як проходження процедури отримання судового дозволу, зокрема в апеляційному суді, може зумовити втрату істотних доказів, важливих для кримінального провадження.

Безумовно, основна ідея невідкладного проведення НСРД полягає у необхідності запобіганню вчиненню кримінального правопорушенню, недопустимості запобігання втраті доказів та їх оперативної фіксації. Враховуючи, що зняття інформації з електронних комунікаційних мереж є тим різновидом НСРД, що спрямований на фіксацію динамічної інформації, яка циркулює у мережах, звісно, що незважаючи навіть на стислі строки розгляду клопотання слідчим суддею суду апеляційної інстанції, існує істотний ризик

втрати відомостей, які мають важливе значення для встановлення фактичних обставин кримінального провадження.

Враховуючи наведене, пропонуємо доповнити статтю 263 КПК України ч.5 такого змісту: «Зняття інформації з електронних комунікаційних мереж до постановлення ухвали слідчого судді може бути розпочато на підставі постанови слідчого, прокурора лише у випадку, передбаченому частиною першою статті 250 цього Кодексу».

Окремі питання виникають і у контексті належного процесуального порядку складання протоколу зняття інформації з електронних інформаційних мереж. У ч.1 ст. 252 КПК України встановлено, що фіксація ходу і результатів негласних слідчих (розшукових) дій повинна відповідати загальним правилам фіксації кримінального провадження, передбаченим КПК України. За результатами проведення негласної слідчої (розшукової) дії складається протокол, до якого в разі необхідності долучаються додатки.

Цей порядок деталізується у положеннях 4.2. Інструкції, які передбачають, що «періодичність складання протоколів залежить від виду негласної слідчої (розшукової) дії, терміну її проведення (одномоментно чи упродовж часу), від доручення слідчого, прокурора, але в будь-якому випадку безпосередньо після отримання фактичних даних, які можуть використовуватись як докази для встановлення місця перебування особи, що розшукується, про кожний випадок огляду, виїмки, дослідження матеріалів про результати негласної слідчої дії тощо» [33].

І хоча така регламентація видається, на перший погляд, чіткою й несуперечливою, у контексті зняття інформації з електронних комунікаційних мереж вона породжує певні труднощі у правильному тлумаченні, адже цей вид НСРД характеризується довготривалістю та динамічністю. Ця проблема піднімалася і у доктрині, і у правозастосовній практиці.

М.Г. Щербаковський та В.А. Коршенко зазначають, що практика виробила таку процедуру, яка не суперечить закону, але певною мірою оптимізує проведення даної НСРД. Вона полягає в тому, що в дорученні

передбачається можливість періодичного ознайомлення слідчого або іншої уповноваженої особи з інформацією, яка надходить упродовж строку дії дозволу на проведення негласної слідчої (розшукової) дії. За переконанням авторів, застосування такого підходу має позитивний ефект, оскільки дозволяє слідчому своєчасно розуміти реальний зміст розмов чи інших повідомлень між кореспондентами, а регулярний перегляд отриманих матеріалів дає змогу виокремлювати з усього масиву лише ті відомості, що мають значення для розслідування. Накопичена впродовж проведення негласної слідчої (розшукової) дії релевантна інформація надалі узагальнюється та викладається у протоколі в стислому й систематизованому вигляді. У результаті до протоколу вносяться лише ті фрагменти спілкування, які містять дані, важливі для кримінального провадження. Крім того, завчасне отримання такої інформації ще до остаточного оформлення протоколу надає слідчому можливість оперативно вжити заходів для припинення злочину, що готується або вчиняється, а також своєчасно ініціювати проведення інших гласних чи негласних слідчих (розшукових) дій [163, с. 157].

Питання щодо належного порядку складання протоколу зняття інформації з електронних комунікаційних мереж виникало і у практиці ККС ВС. У Постанові ККС ВС від 09 травня 2024 року було «висновки суду про необхідність щоденного складання протоколів за результатами триваючої НСРД - зняття інформації з транспортних текомунікаційних мереж, що здійснювалося впродовж кількох днів, не відповідають вимогам кримінального процесуального закону. Адже пунктом 1 статті 106 КПК передбачено документування процесуальної дії незалежно від її тривалості протоколом як єдиним цілісним документом. Направлення таких протоколів прокурору за межами встановленого частиною 3 статті 252 КПК 24-годинного строку суттєво не вплинуло на процесуальні права ОСОБА_8 і не є істотним порушенням кримінального процесуального закону, яке б тягнуло недопустимість доказів, одержаних в результаті НСРД» [87].

Ми підтримуємо позицію щодо правомірності варіативного порядку складання протоколу зняття інформації з електронних інформаційних мереж – як протоколу за результатами всієї НСРД, так і окремих її етапів, що відповідає як вимогам законодавства, так і потребам правозастосовної практики.

Як зазначалось вище, доволі поширеною процесуальною дією під час здійснення досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі є тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв’язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

У зв’язку із цим, необхідно більш детально розкрити деякі особливості та окремі проблеми нормативної регламентації цієї процесуальної дії.

Одразу слід зазначити, що тимчасовий доступ до речей і документів є заходом забезпечення кримінального провадження та спрямований на досягнення дієвості кримінального провадження, що прямо випливає із положень ч.1 ст. 131 КПК України. Однак, незважаючи на це, значення цього заходу для отримання доказів при розслідуванні розглядуваної нами категорії кримінальних правопорушень є визначальною.

Передусім, у контексті нашого дослідження слід звернути увагу на обсяг інформації, доступ до якої може бути затребуваний шляхом тимчасового доступу до речей і документів у порядку п.7 ч.1 ст. 162 КПК України.

Цей аспект у доктрині досліджувався С.Р. Тагієвим. Автор зазначає, що слідчі судді місцевих судів уповноважені розглядати клопотання про тимчасовий доступ саме статичної інформації, яка знаходиться у операторів та провайдерів та телекомунікацій (зв'язок абонента, надання телекомунікаційних послуг, їх тривалість, зміну, маршрути передавання) [119, с. 19].

Одразу слід зазначити, що буквальне тлумачення норми п.7 ч.1 ст. 162 КПК України дозволяє дійти висновку, що перелік інформації, яка може бути витребувана у оператора телекомунікацій не є вичерпною, про що свідчить

використання частки «тощо». І як демонструє судова практика, слідчі судді постановляють ухвали, якими надають доступ до доволі широкого кола даних у аналізованому процесуальному порядку. Так, наприклад, ухвалою слідчого судді Кам'янець-Подільського міськрайонного суду Хмельницької області було надано тимчасовий доступ до інформації про «фінансові операції з зарахування, поповнення, переведення та виведення грошових коштів з використанням абонентським номером НОМЕР_5 та НОМЕР_6 , з зазначенням отримувача грошових коштів, суми транзакцій, дати та часу виконання з можливістю отримання копії (в тому числі електронних документів)» [136].

Ухвалою слідчого судді Личаківського районного суду Львівської області натомість було надано тимчасовий доступ до «даних про використання Wi-Fi дзвінків (VoWiFi) - інформацію про з'єднання, включаючи ідентифікацію Wi-Fi мереж, до яких підключався абонент; інформації про всі заміни SIM-картки, які були здійснені абонентом за певний період, включаючи дати активації нових SIM-карток; інформації про всі налаштування переадресації дзвінків та повідомлень (на які номери здійснювалась переадресація, коли були активовані/деактивовані ці налаштування); інформації про активацію та використання додаткових послуг або додатків, наданих оператором (мобільний банкінг, електронний гаманець, тощо); деталей про випадки блокування або тимчасового відключення номеру, включаючи причини (несплата рахунку, втрата SIM-карти, розслідування шахрайських дій тощо)» [139].

Питання також виникають і у контексті визначення періоду, за який надається інформація, передбачена п.7 ч.1 ст. 162 КПК України. Норми ст. 162 КПК України не містять спеціальних положень, які регламентують цей аспект. Аналіз судової практики демонструє, що слідчі судді задовольняють клопотання, у який запитується інформація про надані оператором телекомунікацій послуги за доволі значні періоди часу. До прикладу, ухвалою слідчого судді Ніжинського міськрайонного суду Чернігівської області

тимчасовий доступ було надано до «інформації, яка знаходиться у володінні оператора мобільного зв`язку - ПрАТ « ІНФОРМАЦІЯ_5 », яке розташоване за адресою: АДРЕСА_1 , про зв`язок кінцевих обладнань споживачів телекомунікаційних послуг здійснених за абонентським номером НОМЕР_4 - у період з моменту активації сім-картки абонентом, що використовував номер 25.02.2023, до моменту витребування документів» [140].

Загалом, такий підхід не викликає заперечень з точки зору дотримання принципу законності, але породжує питання щодо дотримання загального правила застосування заходів забезпечення кримінального провадження, передбаченого п.2 ч.3 ст. 132 КПК України, відповідно до якого застосування заходів забезпечення кримінального провадження не допускається, якщо слідчий, дізнавач, прокурор не доведе, що потреби досудового розслідування виправдовують такий ступінь втручання у права і свободи особи, про який ідеться в клопотанні слідчого, дізнавача, прокурора. Саме тому, відповідне втручання у права та свободи буде правомірним лише за умови, що слідчий, прокурор доведуть, що за результатами виконання ухвали мають намір встановити фактичні обставини, які вимагають витребування інформації саме за такий тривалий період і обґрунтують це у поданому клопотанні.

У фаховій літературі вказувалося також і на проблему несвоєчасного виконання операторами телекомунікацій ухвали слідчого судді про тимчасовий доступ до речей і документів. Так, наприклад, В.М. Данатарова зазначає, що «деякі компанії мобільного зв’язку, мотивують затягування тим, що термін виконання ухвали строком 30 днів, ще не сплив, та просять зачекати ще, чи встановлюють певні правила, щодо отримання запитуваної інформації на підставі ухвали, встановлюючи термін виконання строком 30 днів. Однак зазначене унеможливлює розкриття правопорушення не тільки по «гарячим» слідам, а й взагалі, оскільки за цей час телефон може неодноразово змінити власника, сім карту» [25, с. 217].

На сторінках нашої праці ми неодноразово наголошували на тому, що однією із іманентних ознак цифрової інформації є її здатність бути

спотвореною або знищеною у короткий проміжок часу. У цьому контексті безумовно, слід цілком погодитись, що чинна регламентація виконання ухвали про тимчасовий доступ до речей і документів є неадаптованою до процедур, пов'язаних із вилученням цифрової інформації, оскільки не враховує вимоги оперативності як розгляду відповідних клопотань, так і виконання ухвал за результатами їх розгляду.

У зв'язку із цим ми пропонуємо, ч.4 ст. 163 КПК України доповнити абзацом другим і викласти його у такій редакції: «Клопотання слідчого, прокурора про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо розглядається слідчим суддею у день його надходження». Водночас, ст. 165 КПК України доповнити ч. 5 та викласти її у такій редакції: «Ухвала слідчого судді про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо підлягає негайному виконанню».

У доктрині неодноразово лунали пропозиції на користь спрощення процесуального порядку тимчасового доступу до речей і документів, передбачених п.7 ч.1 ст. 162 КПК України, зокрема, у контексті обмеження судового контролю.

Наприклад, І.І. Татарин та І.М. Євхутич пропонують надати прокурору та слідчому (за погодженням з прокурором) повноваження «у виняткових невідкладних випадках, пов'язаних із запобіганням знищення речей і документів, втрати інформації, яка в них міститься, у разі наявності обґрунтованої загрози щодо цього або ж для запобігання вчинення тяжкого або особливо тяжкого злочину, здійснювати тимчасовий доступ до визначеної в п. 7, 8 ч. 1 ст. 162 КПК України інформації, через уповноважені оперативні

підрозділи, які мають автоматизований доступ до інформації, що знаходиться в операторів та провайдерів телекомунікацій, шляхом винесення відповідної постанови» [120, с. 34].

Більш деталізовану модель обмеження судового контролю у розглядуваному аспекті пропонують С.С. Чернявський та В.О. Фінагєєв. Науковці пропонують надати слідчому та прокурору можливості тимчасового доступу до речей і документів та їх подальшого (в разі потреби) вилучення без ухвали слідчого судді, якщо ці речі або документи не містять охоронюваної законом таємниці (ст. 162 КПК України), а також, «надати можливість тимчасового доступу до речей і документів без відповідної ухвали, навіть якщо ці предмети містять охоронювану законом таємницю, але особа, у володінні якої знаходяться речі і документи, дає письмову згоду (сповіщає про готовність) забезпечити доступ до них уповноважених органів (звертатися з клопотанням до слідчого судді лише в разі необхідності вилучення оригіналів)» [158, с. 184].

Обидві пропоновані моделі обмеження судового контролю видаються дискусійними та такими, що містять істотні ризики для дотримання гарантій прав людини. Надання слідчому й прокурору повноважень здійснювати тимчасовий доступ і вилучення без ухвали слідчого судді, навіть за умови відсутності охоронюваної законом таємниці, створює передумови для зловживань та нівелювання судового контролю як ключової процесуальної гарантії на стадії досудового розслідування.

Існували й законопроектні пропозиції у даному контексті. Зокрема, Проектом Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо спрощення та удосконалення діючих норм Закону з метою уникнення покарання винними особами та розвантаження судових органів» від 03.04.2020 р. № 3303 пропонувалося доповнити ст. 159 КПК України положенням, відповідно до якого «тимчасовий доступ до інформації операторів мобільного зв'язку здійснюється на підставі постанови слідчого або прокурора» [100].

Більшість пропозицій, які передбачають обмеження судового контролю у контексті тимчасового доступу до речей і документів ґрунтуються на ідеї, яка полягає в тому, що у випадку тимчасового доступу до інформації, передбаченої п.7 ч.1 ст. 162 КПК України втручання у приватне спілкування не відбувається, оскільки зміст спілкування не розкривається, а отже і потреба у судовому контролі не є нагальною.

Позицію щодо неприпустимості обмеження судового контролю у контексті тимчасового доступу до речей і документів, передбачених п.7 ч.1 ст. 162 КПК України у доктрині послідовно відстоює С.Л. Шаренко. Авторка зазначає, що «відсутність доступу до змісту інформації, яка передається засобами зв'язку, ще не свідчить, що обмеження конституційних прав виключається. Аналіз матеріалів судової практики демонструє, що у межах тимчасового доступу до інформації операторів мобільного зв'язку може бути встановлено: 1) адреси розташування та номери базових станцій, які забезпечували зв'язок; 2) маршрути передавання інформації з прив'язкою до місцевості як місцезнаходження запитуваного абонента, так і його співрозмовників; 3) типи з'єднань (вхідні, вихідні дзвінки, SMS, MMS, GPRS, переадресація); 4) дата, час та тривалість з'єднання; 5) ідентифікаційні ознаки кінцевого обладнання (абонентський, серійний, IMSI номери сім-картки, IMEI); 6) ідентифікаційні ознаки терміналу, з яким відбувався сеанс зв'язку; 7) з'єднання нульової тривалості; 8) за наявності контрактної угоди або відповідної реєстрації – відомості про абонентів; 9) номера скретч-карток, якими поповнювався номер мобільного телефону (дата, час, сума поповнення та інша інформація щодо руху коштів за певний період часу) тощо» [160, с. 104-105]. На переконання дослідниці усе це свідчить про те, що його застосування обмежує передбачене ст. 32 Конституції право особи на особисте життя.

З цією позицією однозначно можна погодитись, однак із певними уточненнями. Мова йде про випадок, коли за допомогою інформації про зв'язки особи, передавання інформації, переміщення особи можна легко

реконструювати події, пов’язані із її приватним життям, що безумовно є втручанням з боку держави, яке потребує судового дозволу, у тому числі з точки зору міжнародним стандартів захисту прав людини, проаналізованих у роботі.

Беззаперечною актуальністю сьогодні відзначається питання, пов’язане із здійсненням тимчасового доступу до речей і документів в умовах воєнного стану. Як випливає із норми п.2 ч.1 ст. 615 КПК України, в умовах воєнного стану у разі відсутності об’єктивної можливості виконання слідчим суддею повноважень щодо надання дозволу на тимчасовий доступ до речей і документів, такі повноваження виконує керівник відповідного органу прокуратури за клопотанням прокурора або за клопотанням слідчого, погодженим з прокурором. У літературі певні аспекти цього питання були досліджені О.О. Кравчуком. Автор зазначає, що при реалізації прокурором відповідних повноважень, виникає питання щодо дотримання згаданого нами вище правила, встановленого у ч.3 ст. 132 КПК України щодо необхідності обставин, які вказують що потреби досудового розслідування виправдовують такий ступінь втручання у права і свободи особи, про який ставиться питання в клопотанні. Як приклад, автор наводить якраз таки тимчасовий доступ до інформації, передбаченої п.7 ч.1 ст. 162 КПК України, зазначаючи, що «далеко не завжди при розслідуванні одноепізодного злочину потреби досудового розслідування виправдовують доступ до інформації про дзвінки та Інтернет-з’єднання з мобільних телефонів особи за трирічний період або з мобільних телефонів членів сім’ї потенційного підозрюваного або свідка. Так само, далеко не завжди є необхідність вилучення оригіналів документів – у багатьох випадках, достатньо обмежитися копіями» [55, с. 112].

Ми теж підтримуємо позицію про те, що чинна регламентація п.2 ч.1 ст. 615 КПК України не є пропорційною у частині делегування повноважень слідчого судді керівнику органу прокуратури, у тому числі у контексті тимчасового доступу до речей і документів. Саме тому, пропонуємо дещо змінити чинний перелік повноважень слідчого судді, які можуть бути виконані

керівником органу прокуратури в умовах воєнного стану в частині тимчасового доступу до речей і документів і норму п.2 ч.1 ст. 164 КПК України уточнити наступним чином «відсутня об'єктивна можливість виконання слідчим суддею повноважень, передбачених статтями 140, 163, 164 (крім тимчасового доступу до речей і документів, що містять охоронювану законом таємницю)…(далі у чинній редакції)».

Враховуючи транскордонний характер кримінальних правопорушень, вчинених у кіберпросторі, важливе значення у кримінальному процесуальному доказуванню відіграють процесуальні дії, що вчиняються у межах міжнародного співробітництва. У випадках співробітництва з країнами-членами Ради Європи, безумовно, його правовою основою є Будапештська конвенція. Компетентні органи України направляють та виконують запити про співробітництво при здійсненні розслідування цієї категорії кримінальних правопорушень. Про це свідчить й судова практика. Наприклад, в ухвалі слідчого судді Голосіївського районного суду м. Києва зазначалось наступне: «Посилаючись на ст. ст. 16, 17 Конвенції про кіберзлочинність (Будапешт) ІНФОРМАЦІЯ_8 , орган поліції за згоди прокурора звернувся ще перед допитом ОСОБА_5 до відповідних українських органів з проханням про негайне збереження даних, збережених у комп`ютерній системі, а саме: збереження даних з електронної адреси ІНФОРМАЦІЯ_5 . У результаті цього запиту 15.06.2021 було повідомлено відповідними українськими органами, що вказану інтернетову адресу адмініструє ТОВ « ІНФОРМАЦІЯ_7 ». Згодом, 27.07.2021, українськими органами повідомлено, що дані було з боку ТОВ « ІНФОРМАЦІЯ_7 » збережено.

З урахуванням вищевикладеного є очевидним, що розкриття злочинів, які перевіряються, залежить від придбання доказів в Україні. Ці докази не можна придбати в Чеській Республіці. Щоб можна було продовжити кримінальне провадження й належним чином розкрити справу, необхідно отримати зміст електронного листування, здійсненого ІНФОРМАЦІЯ_9 стосовно закупівлі антигенних тестів від китайського виробника компанії

ІНФОРМАЦІЯ_10 і далі стосовно продажу й поставки цих антигенних тестів Міністерству внутрішніх справ Чеської Республіки, а також стосовно фінансування цієї угоди й подальшого розподілу коштів, придбаних в результаті зазначеної угоди» [130].

Відповідно, на виконання запиту компетентного органу іноземної держави, в Україні здійснюється тимчасовий доступ до речей і документів, спрямований на збереження цифрових доказів. Останнє є найпоширенішою формою співробітництва між державами при розслідуванні кіберзлочинів.

Однак правові рамки співробітництва у цьому контексті не обмежуються лише Будапештською Конвенцією. Наприклад, в ухвалі про арешт майна слідчого судді Голосіївського районного суду м. Києва указується: «досудовим розслідуванням встановлено, що в ході досудового розслідування від National center for missing and exploited children (Національного центру пошуку зниклих та експлуатованих дітей США) надійшла інформація щодо можливої протиправної діяльності групи осіб, які можуть бути причетними до виготовлення та розповсюдження дитячої порнографії з використанням мережі інтернет. Зазначена організація взаємодіє з більшістю правоохоронних органів світу з метою попередження сексуальної експлуатації дітей в мережі Інтернет, в тому числі й з Національною поліцією України шляхом надання працівникам Департаменту кіберполіції доступу до веб-порталу для обміну такою інформацією http://lesp.ncmec.org/CybertiplineCaseManagement/.

Вищезазначена організація надсилає на відомчу електрону пошту Департаменту кіберполіції звіти щодо можливих випадків сексуальної експлуатації дітей в мережі Інтернет, в тому числі й розповсюдження порнографічних матеріалів особами, які для з`єднання з мережею Інтернет використовують IP-адреси українських Інтернет-провайдерів. Звіт на електронну пошту включає наступні реквізити: номер звіту, пріоритетність, інформатор, електронна пошта, дані особи, яка вчиняє протиправні дії, нікнейм користувача, який вчиняє протиправні дії, дата надання доступу до інформації, кількість файлів, країна, якої стосується» [131].

Як убачається зі змісту судового рішення, на підставі наведеної інформації слідчими було проведено огляди цифрових платформ, за результатами яких виявлено відомості у електронній формі.

Із цього випливає висновок, що міжнародне співробітництво у розглядуваному контексті здійснюється як шляхом виконання запитів у порядку, передбаченому КПК України, так і шляхом постійного обміну інформацією задля забезпечення оперативності досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

3.3. Використання спеціальних знань при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі

Кримінальні правопорушення, вчинені у кіберпросторі традиційно пов’язані із втручанням у функціонування комп’ютерних систем, мереж, програмного забезпечення, хмарних сервісів, криптографічних механізмів і цифрових слідів, правильне виявлення та фіксація яких потребують глибоких спеціальних знань у сфері інформаційних технологій і цифрової криміналістики. Саме ці обставини обумовлюють нагальну необхідність використання спеціальних знань при розслідування цієї категорії кримінальних правопорушень.

Використання спеціальних знань дає змогу встановити механізм вчинення кіберзлочину, ідентифікувати способи несанкціонованого доступу, визначити роль конкретних осіб та причинно-наслідковий зв’язок між діями певних осіб і завданою шкодою. Відповідно, залучення спеціалістів та експертів дає змогу забезпечити належне збирання, фіксацію, збереження та дослідження електронних доказів аби запобігти їх втраті чи спотворенню.

Але передусім, контекст нашого дослідження передбачає звернення до змісту та сутності поняття «спеціальні знання».

Так, наприклад, на думку А.М. Тимчишина під спеціальними знаннями у кримінальному процесі слід розуміти «апробовані наукові знання, практичні вміння та навички, які сформувалися в особи під час здобуття професійної освіти, проходження спеціальної підготовки, курсів підвищення кваліфікації, досвіду роботи тощо і які можна використати відповідно до процедурних правил кримінально-процесуального закону для вирішення завдань кримінального провадження» [123, с. 96].

Ю.М. Комар вважає, що спеціальні знання у кримінально-процесуальному аспекті – «це наукові, технічні або інші знання, які потрібні для дачі відповіді суб'єкта – носія цих знань на поставлені йому під час розслідування злочинів питання. Спеціальними вважаються знання, що не є загальнопоширеними, загальновідомими, а лише ті, яких набули спеціалісти, експерти, слідчі в тій чи іншій галузі науки, техніки, мистецтва, ремесла, тощо» [49, с. 115].

На думку Б.В. Романюка під спеціальними знаннями слід розуміти сукупність науково обґрунтованих відомостей окремого (спеціального) виду, якими володіють особи (спеціалісти) у межах будь-якої професії в різних галузях науки, техніки, мистецтва та ремесла, і які відповідно до норм кримінально-процесуального законодавства використовуються для успішного вирішення завдань кримінального судочинства [106, с. 7-8].

Поняття спеціальних знань у кримінальному провадженні нерозривно пов'язане із поняттям обізнаної особи, що є абсолютно логічним, адже саме останні є носіями таких знань. У цьому контексті Д.В. Куриленко визначає спеціальні знання як «знання з будь-якої галузі людської діяльності за виключенням права, що застосовуються обізнаними особами, залученими у кримінальне провадження в межах своєї компетенції». Натомість під обізнаною особою автор розуміє «людину, яка в результаті професійного освітянського або самостійного навчання та досвіду оволоділа спеціальними знаннями у певній галузі людської діяльності та навичками щодо їх застосування, безпосередньо або опосередковано, у процесуальній або

непроцесуальній формах, обов'язково або на розсуд уповноваженої особи (органу) залучається під час досудового розслідування або судового розгляду з метою сприяння щодо рішення завдань кримінального провадження, а надані нею відомості, висновки та документи використовуються як джерела доказів або орієнтуюча інформація» [59, с. 12].

Дещо схожої думки з цього приводу дотримується й М.Л. Грібов, зазначаючи, що «спеціальними знаннями, уміннями та навичками, що використовують у кримінальному провадженні, є професійні компетентності осіб, залучених до виконання його завдань слідчим, прокурором, захисником, слідчим суддею, судом на підставах і в порядку, передбачених кримінальним процесуальним законодавством» [23, с. 18].

Отже, незважаючи на доволі різні підходи до визначення поняття спеціальних знань у кримінальній процесуальній та криміналістичній доктрині, аналіз наведених дефініцій дає змогу виокремити деякі спільні ознаки, які є об'єднуючими: 1) спеціальні знання являють собою наукові знання, а також практичні навички, здобуті в межах академічної кваліфікації та професійного досвіду; 2) носіями таких знань є особи, залучені до кримінального провадження слідчим, прокурором, слідчим суддею, судом; 3) метою залучення цих осіб є вирішення питань, що мають значення для повного та всебічного встановлення фактичних обставин у кримінальному провадженні.

На підставі виокремлених ознак можна визначити ***спеціальні знання при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі*** *як сукупність наукових знань і практичних навичок у сфері інформаційних технологій, комп'ютерних систем і мереж, цифрової та комп'ютерно-технічної криміналістики, телекомунікацій, інформаційної безпеки, програмування, аналізу шкідливого програмного забезпечення та електронних фінансових технологій, здобутих у межах академічної підготовки й професійного досвіду, носіями яких є залучені до кримінального провадження за рішенням слідчого, прокурора, слідчого судді чи суду особи, що*

використовуються з метою вирішення питань, необхідних для повного, всебічного й об'єктивного встановлення фактичних обставин кримінального провадження.

Не менш важливим питанням доктринального характеру є питання щодо форм використання спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі.

Зокрема, Є. Д. Лук'янчиков, Б. Є. Лук'янчиков і С. Ю. Петряєв розмежовують дві форми використання спеціальних знань залежно від суб'єкта слідчого пізнання: безпосередню та опосередковану. Безпосередня форма полягає у застосуванні спеціальних знань самим слідчим або судом. У межах цієї форми не формується самостійне джерело доказів, однак вона істотно підвищує ефективність проведення слідчих (розшукових) дій, зокрема огляду місця події (ч. 2 ст. 238 КПК), місцевості, приміщень, речей і документів (ч. 1 ст. 237 КПК) тощо. Завдяки безпосередньому використанню спеціальних знань без призначення експертизи можливо оперативно встановити обставини, що мають значення для кримінального провадження, наприклад, прочитати залитий текст, виявити підчистки чи інші зміни, а також належним чином зафіксувати нововиявлені відомості у протоколі огляду речових доказів.

Опосередковане використання спеціальних знань, своєю чергою, здійснюється через залучення інших осіб, які володіють такими знаннями, і реалізується у декількох формах: по-перше, участі спеціаліста у проведенні слідчих дій; по-друге, наданні спеціалістом усних консультацій або письмових роз'яснень у суді; по-третє, шляхом призначення та проведення судової експертизи [63, с. 129].

Дещо схожої думки щодо критеріїв класифікації спеціальних знань дотримується Р.Л. Степанюк. Він пропонує за суб'єктом застосування виокремлювати такі різновиди спеціальних знань у кримінальному провадженні: «1) «професійні знання осіб, котрі здійснюють кримінальне провадження»; 2) «фахові знання підозрюваних, обвинувачених, професійних

захисників»; 3) «професійні знання осіб, яких залучають сторони процесу й суд для розв'язання завдань кримінального провадження» [117, с. 42].

Безумовно, сторона обвинувачення та всі учасники кримінального провадження, які здійснюють його від імені держави можуть мати певні базові знання у галузі інформаційних технологій, комп'ютерних систем і мереж та використовувати їх при здійсненні певних процесуальних дій. Однак не можна сказати, що залучені спеціалісти виконують у цьому контексті лише компенсаторну роль. При здійсненні досудового розслідування кримінальних правопорушень у кіберпросторі їх консультації та роз'яснення, безумовно, відіграватимуть провідну роль враховуючи надзвичайно складний (у переважній більшості випадків) механізм вчинення таких правопорушень.

І.В. Гора дотримується думки, що в «основі поділу форм використання спеціальних знань в кримінальному судочинстві має бути такий критерій, як доказове значення результату використання спеціальних знань у досудовому розслідуванні та судовому розгляді матеріалів кримінальних проваджень» [20, с. 211].

Доволі поширеним у кримінальній процесуальній та криміналістичній доктрині підходом є виокремлення таких форм використання спеціальних знань як процесуальна та непроцесуальна. Зокрема, О. В. Бишевець звертає увагу на те, що до процесуальних форм використання спеціальних знань у кримінальному провадженні слід відносити проведення судових експертиз відповідно до ст. ст. 242–245 КПК України, а також залучення спеціалістів до участі в окремих слідчих (розшукових) діях на підставі ст. ст. 71, 226, 227, 491 КПК України. Таке залучення здійснюється з метою надання допомоги слідчому у виявленні, фіксації та вилученні слідів кримінального правопорушення й речових доказів, наданні консультацій із питань, що потребують спеціальних знань, а також застосуванні технічних засобів у кримінальному провадженні як одного зі способів виявлення та закріплення доказової інформації (п. 2 ч. 1 ст. 103, ч. 2 ст. 104, п. п. 1, 3, 4 ч. 2 ст. 105, ч. ч. 1–4 ст. 107 КПК України). До процесуальних форм також відносяться

письмові пояснення спеціалістів, які брали участь у слідчих (розшукових) діях, щодо специфіки виявлення та фіксації слідів і інших об'єктів (п. 2 ч. 2 ст. 105 КПК України).

Водночас до непроцесуальних форм використання спеціальних знань дослідниця зараховує проведення ревізій та аудиторських перевірок, здійснення попередніх досліджень об'єктів, а також надання спеціалістами консультацій [8, с. 191].

Аналогічні форми у доктрині виокремлює й І.І. Когутич. Серед основних процесуальних форм використання спеціальних знань автор називає наступні: «1) безпосереднє використання їх слідчим, прокурором, складом суду під час виконання своїх процесуальних функцій збирання, дослідження та оцінки доказів; 2) участь спеціаліста у провадженні слідчих (розшукових) дій; 3) призначення і провадження судових експертиз. Серед непроцесуальних форм доцільно розглядати: 1) консультативну та довідкову діяльність суб'єктів спеціальних знань; 2) проведення ревізій чи аудиторських дій; 3) участь суб'єктів спеціальних знань в оперативно-розшукових заходах; 4) попередні дослідження матеріальних об'єктів спеціалістами та експертами; 5) результати перевірок за криміналістичними обліками» [44, с. 114].

При розслідуванні кримінальних правопорушень, вчинених у кіберпросторі актуальними є як процесуальні, так і непроцесуальні форми використання спеціальних знань. Процесуальні форми здебільшого проявляються у залучення відповідних спеціалістів при проведенні слідчих (розшукових) дій. Для цього існують й належні правові підстави. Наприклад, у абз. 3 ч.6 ст. 236 КПК України зазначено, що «особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку». Непроцесуальна форма використання спеціальних знань проявлятиметься здебільшого у консультативній та довідковій діяльності суб'єктів спеціальних знань.

У доктрині також наявні підходи до визначення спеціальних форм використання спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі.

Л. Будник, О. Карапетян та І. Метельський зазначають, що при розслідуванні кіберзлочинів найчастіше застосовуються три форми використання спеціальних знань: «1) залучення спеціаліста для надання письмової консультації; 2) залучення спеціаліста для надання безпосередньої технічної допомоги під час здійснення процесуальних дій; 3) залучення експерта для проведення судової експертизи» [9,с. 160].

Аналіз наукових джерел засвідчує, що саме перші дві форми використання спеціальних знань є найбільш поширеними у правозастосовній діяльності.

О.А. Самойленко вказує, що при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі можуть використовуватися безліч форм спеціальних знань. Зокрема, авторка зазначає, що «у справах щодо кіберзлочинів письмові пояснення спеціаліста є додатковим способом підтвердження джерела формування такого доказу, як документ – електронний носій інформації. В абсолютній більшості проваджень пояснення надають штатні працівники кіберполіції, які є фахівцями з інформаційних технологій або електроніки й телекомунікацій, і в процесуальному статусі спеціаліста були залучені під час проведення огляду місця події. У письмовому поясненні такий спеціаліст описує методи так званого експрес-аналізу (процес встановлення фактичних даних, що мають значення для конкретного факту правопорушення); методи вилучення (копіювання) та збереження нетрадиційних (цифрових) слідів злочину» [110, с. 27].

Про залучення спеціаліста як пріоритетну форму використання спеціальних знань веде мову й С.М. Розумний. Як підкреслює дослідник, «під час проведення огляду місця події до участі як спеціаліста зазвичай залучається фахівець у сфері комп’ютерної техніки. Уже на підготовчому етапі такий спеціаліст надає слідчому допомогу у забезпеченні належної

технічної готовності слідчої дії, зокрема у доборі та підготовці комп'ютерної техніки, яка використовуватиметься для зчитування, копіювання та збереження вилученої інформації. Крім того, він забезпечує наявність необхідних з'єднувальних кабелів, адаптерів та інших допоміжних пристроїв, а також спеціалізованого програмного забезпечення, що дозволяє здійснювати оперативний аналіз цифрових даних і створення їх копій безпосередньо на місці події. Така участь спеціаліста сприяє підвищенню ефективності огляду та мінімізації ризиків втрати або спотворення електронної інформації» [105, с. 246].

Досить ґрунтовно сферу використання консультацій спеціаліста під час розслідування кримінальних правопорушень, учинених у кіберпросторі, окреслив Я. В. Неділько, який виокремив основні напрями такої консультативної діяльності, а саме: «надання рекомендацій під час формування слідчих версій і розроблення плану розслідування; роз'яснення щодо цільового призначення та методики застосування технічних засобів у процесі фіксації електронних слідів; надання порад стосовно послідовності виявлення, фіксації та дослідження засобів інформаційно-комп'ютерних технологій; рекомендації щодо доцільності залучення спеціаліста іншої спеціалізації; термінологічна допомога під час оформлення протоколів відповідних процесуальних дій; пояснення принципів функціонування апаратних (технічних) і програмних засобів; визначення, який саме засіб інформаційно-комп'ютерних технологій необхідно дослідити в першу чергу; поради щодо направлення вилучених засобів інформаційно-комп'ютерних технологій на відповідну експертизу та формулювання питань, які доцільно поставити перед експертом; а також роз'яснення щодо необхідності проведення додаткових процесуальних дій» [73, с. 77].

Окрему увагу у межах нашого дослідження слід приділити питанням призначення та проведення експертиз при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Проведенню експертиз у кримінальному провадженні щодо кримінальних правопорушень, вчинених у кіберпросторі завжди передують слідчі (розшукові) дії, в межах яких вилучаються відповідні об’єкти для експертного дослідження. Зокрема, Ю.Ю. Нізовцев та О.С. Омельян зазначають, що під час огляду атакованої системи як об’єкти дослідження можуть бути вилучені: носії інформації або їх клони чи бітові образи; дампи оперативної пам’яті; лог-файли служб і додатків; налаштування логіювання; файли-звіти діагностичних утиліт; налаштування роботи діагностичних утиліт; схеми будови автоматизованих систем, їх об’єднання у кластери, мережі; схеми внутрішніх мереж (LAN, Local Area Network) і під’єднання до глобальної мережі (WAN, Wide Area Network); налаштування мережевого обладнання; налаштування програмного забезпечення (системного, серверного, користувацького) автоматизованої системи, зокрема налаштування віддаленого доступу; листування електронною поштою – насамперед листи з вкладеними файлами (потенційно шкідливими програмними засобами) або зовнішні посилання (потенційні джерела завантаження шкідливих програмних засобів) [74, с. 62].

Найбільш поширеними видами експертиз під час розслідування кримінальних правопорушень, вчинених у кіберпросторі, як показує досвід правозастосовної діяльності, є комп’ютерно-технічна експертиза та експертиза електронних комунікацій.

Відповідно до п.13.1 Інструкції «до основних завдань експертизи комп'ютерної техніки і програмних продуктів належать: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку» [96].

Нормативно визначена сфера застосування даного виду експертного дослідження, дає змогу дійти висновку, що комп'ютерно-технічна експертиза є одним із ключових засобів доказування у кримінальних провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі. Її основні можливості полягають у дослідженні комп'ютерної техніки, цифрових носіїв інформації, програмного забезпечення та електронних даних з метою встановлення обставин вчинення кримінального правопорушення. За допомогою комп'ютерно-технічної експертизи можна відновити видалені або приховані дані, встановити факт і спосіб несанкціонованого доступу до комп'ютерних систем, визначити характер і послідовність дій користувача, а також з'ясувати час створення, зміни чи знищення файлів.

Експертиза дозволяє ідентифікувати програмні засоби, що використовувалися для вчинення кіберзлочину, у тому числі шкідливе програмне забезпечення, засоби маскування або віддаленого керування. Крім того, вона дає змогу встановити зв'язок між конкретним пристроєм, обліковим записом і подією, що розслідується, а також забезпечує належну фіксацію та інтерпретацію електронних доказів для їх подальшої оцінки судом.

О.Ю. Довженко зазначає, що судова комп'ютерно-технічна експертиза у кримінальних провадженнях щодо кіберзлочинів, як правило, призначається на початковому етапі досудового розслідування, після проведення огляду місця події та обшуку, коли наявних відомостей виявляється недостатньо для подальшого розвитку розслідування. У такій ситуації слідчий приймає рішення про доцільність призначення судової комп'ютерно-технічної експертизи стосовно об'єктів, які були виявлені та (або) вилучені під час проведення зазначених слідчих (розшукових) дій [28, с. 125].

У кримінальній процесуальній та криміналістичній доктрині часто наголошується на тому, що комп'ютерно-технічна експертиза не повинна включати в себе правові питання. Зокрема, О.В. Курман зазначає, що «у контексті комп'ютерно-технічної експертизи (телекомунікаційних систем та засобів) таким правовим питанням визначається, наприклад, наступне – «чи

використовується на комп'ютері контрафактне (неліцензоване) програмне забезпечення?» Експерт може лише визначити характеристики програмних, апаратних та інформаційних продуктів, представлених на експертизу в якості об'єкта дослідження, і вказати на ознаки, які вказують на контрафактність. Сам же факт контрафактності програмного забезпечення встановлюється під час досудового розслідування слідчим та остаточно визначається судом. Також некоректним буде питання «який розмір завданої матеріальної шкоди від використання конкретного програмного забезпечення» або «яка загальна вартість програмного забезпечення, встановленого на комп'ютері», адже визначення розміру шкоди чи вартості чогось – це прерогативний предмет дослідження інших видів судових експертиз» [60, с. 480].

Ще одним поширеним видом експертиз при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі є експертиза електронних комунікацій.

Нормативні основи експертизи електронних комунікацій, як і всіх судових експертиз, закладені в Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої Наказом Міністерства юстиції України від 08.10.1998 № 53/5. У п. 14.2 Наказу основними завданнями відповідного роду експертних досліджень визначені: «1) визначення характеристик та параметрів мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів та випромінювальних пристроїв; 2) встановлення фактів та способів передачі (отримання) інформації з використанням мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв; 3) встановлення фактів та способів доступу до мереж, ресурсів та інформації у сфері електронних комунікацій; 4) визначення технічних чинників якості надання електронних комунікаційних послуг на рівні їх споживання; 5) встановлення конфігурації та робочого стану мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв; 6) встановлення типу, марки, моделі та

інших класифікаційних категорій мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв; 7) дослідження алгоритмів обробки інформації та її захисту в мережах електронних комунікацій та їх складових, радіообладнанні, радіоелектронних засобах, випромінювальних пристроях» [96].

Розкриваючи значення цієї експертизи для кримінального провадження, В. А. Коршенко наголошує, що «воно полягає у дослідженні засобів і систем телекомунікацій, а також відповідної інформації з метою виявлення слідів кримінального правопорушення та криміналістично значущих відомостей у об'єктах, які були виявлені під час проведення слідчих (розшукових) дій. Окрім цього, така експертиза спрямована на встановлення змісту та характеристик інформації, зібраної в результаті проведення негласних слідчих (розшукових) дій, отриманої з транспортних телекомунікаційних мереж, а також здобутої під час здійснення процесуальних дій у межах дистанційного кримінального провадження з використанням телекомунікаційних технологій» [52, с. 10].

Водночас у правозастосовній практиці досить поширеними є ситуації, коли перед експертами додатково порушується питання про те, чи належать окремі пристрої до електронно-обчислювальної техніки, а також щодо визначення їх функціонального призначення та можливостей виконання відповідних операцій. Наприклад, в ухвалі слідчого судді Індустріального районного суду м. Дніпропетровська при призначенні судової телекомунікаційної експертизи перед експертом були поставлені такі питання: «1) Чи відносяться надані на дослідження пристрої до електронно-обчислювальної машини (ЕОМ, комп'ютер)? Якщо так, то за якими ознаками?; 2) Чи може надані на дослідження пристрої виконувати функції кодграббера-ретранслятора або в просторіччі «удочка», чи «довга рука»? Якщо так, чи може наданий на дослідження пристрій виконувати дії по ретрансляції сигналу автомобільної системи типу «Keyless Go» або «SmartKey» (система комфортного доступу)?; 3) Чи може надані на

дослідження пристрої виконувати функції пригнічення електронних сигналів, якщо так до якого типу відноситься?» [133].

Окрім визначення технічних характеристик відповідного засобу, у межах експертизи електронних комунікацій перед експертами досить часто ставляться також питання, пов'язані з ідентифікацією пристрою та його мережевих параметрів, зокрема щодо встановлення IMEI такого пристрою, визначення номера мобільного оператора, що використовується у наявній SIM-карті, а також з'ясування відомостей про оператора мобільного зв'язку SIM-карти, інтегрованої або встановленої в технічному пристрої [143].

Аналіз судової практики свідчить, що зазначений вид експертних досліджень досить часто застосовується у кримінальних провадженнях, розпочатих за ст. 176 Кримінального кодексу України (порушення авторського права і суміжних прав). У справах цієї категорії така експертиза, як правило, призначається з метою встановлення можливості об'єднання окремих апаратних засобів у телекомунікаційну мережу, а також з'ясування способів і шляхів маршрутизації передавання даних та інших технічних аспектів функціонування мережевої інфраструктури. Для прикладу того, які питання можуть бути поставлені при призначенні експертизи електронних комунікацій під час досудового розслідування кримінального правопорушення, передбаченого с. 176 КК України наведемо перелік питань, які були поставлені експертам в ухвалі слідчого судді Галицького районного суду м. Львова від 17 січня 2019 року: «1) Чи могли вищезазначені апаратні засоби об`єднуватись у телекомунікаційну мережу та за якими ознаками ?; 2) Які шляхи маршрутизації даних у вищевказаній телекомунікаційній системі ?; 3) Чи можливо використання вищевказаних телекомунікаційних засобів для прийому та передачі супутникових сигналів ?; 4) Чи можливо використання зазначеного телекомунікаційного обладнання для трансляції наступних телеканалів «1+1», «2+2», «ТеТ», «Плюс Плюс», «Бігуді», «Уніан», «СТБ», «ICTV», «Новий канал», «М-1», «М-2», «ОЦЕ ТБ», «ТРК Україна», «Футбол 1» та «Футбол - 2» ? [129].

Окремої уваги потребує те, що під час розслідування кримінальних правопорушень, учинених у кіберпросторі, досить часто призначаються також комплексні комп'ютерно-технічні експертизи та експертизи електронних комунікацій. Необхідність їх проведення зумовлена потребою всебічного дослідження цифрової інформації та процесів електронного обміну даними у випадках, коли встановлення обставин кримінального провадження вимагає одночасного застосування спеціальних знань у сфері інформаційних технологій і телекомунікацій. Комплексний характер такої експертизи пояснюється тим, що відомості про кіберзлочин зазвичай містяться як на матеріальних носіях інформації – комп'ютерах, мобільних пристроях, серверах, так і у нематеріальній формі, зокрема у вигляді даних про передавання інформації в мережах електронного зв'язку. Зокрема, можливості цієї експертизи передбачають паралельне дослідження програмного забезпечення, мережевих параметрів, лог-файлів, історії доступу та використання інформаційних систем, а також встановлення взаємозв'язку між конкретними технічними пристроями, абонентами, обліковими записами й подіями у цифровому середовищі. У результаті забезпечується інтеграція технічних і телекомунікаційних аспектів цифрових слідів у єдину логічно узгоджену систему доказів.

Як приклад, ухвалою слідчого судді Кіровського районного суду м. Кропивницького про призначення комплексної (комп'ютерно-технічної та у сфері телекомунікаційних систем і мереж) експертизи у кримінальному провадженні перед експертом були поставлені, зокрема, такі питання: «1) чи інсталювано на «Smart TV BOX X96 mini» (MAC:900EB30ADDF3) Android додаток «fry!TV»?; 2) який принцип дії та функціональні можливості Android додаток «fry!TV»?; 3) чи є можливість, використовуючи Android додаток «fry!TV» перегляд (ретрансляція, трансляція) телеканалів «1+1», «2+2», «ТЕТ», «Плюс Плюс», «Бігуді», «УНІАН», «Paramount Comedy» та «KVARTAL TV», якщо так, то яким саме чином?; 4) яка мережева активність даного додатку, адреса та спосіб передачі інформації?; 5) чи є на веб-ресурсі

«https://4pda.ru» Android додаток «fry!TV» та чи є він ідентичний додатку, що інстальовано на «Smart TV BOX X96 mini» (MAC:900EB30ADDF3)?» [138].

Ухвалою Новозаводського районного суду Чернігівської області від 01 травня 2025 року про призначення комплексної ком'ютерно-технічної експертизи та експертизи електронних комунікацій на вирішення експерту були поставлені наступні питання: «1) Чи створювалась інформація в додатку «Telegram» із обліковим записом зареєстрованим на номер телефону НОМЕР_1 , з абонентом під ім`ям (нік неймом) « ОСОБА_8 » на цьому телефоні «Xiaomi Redmi Note 9» моделі «M2003J6B2G» коди IMEI 1) НОМЕР_2 , 2) НОМЕР_3 , чи вона була перенесена на вказаний мобільний телефон з іншого носія (пристрою)?; 2) чи міститься на наданому на дослідження об`єкті, а саме мобільному телефоні «Xiaomi Redmi Note 9» моделі «M2003J6B2G» коди IMEI 1) НОМЕР_2 , 2) НОМЕР_3 програмне забезпечення (електронні файли), яке має ознаки шкідливого програмного забезпечення (вірусів, троянів, бекдорів тощо)?; 3) якщо так, то до якого виду шкідливого програмного забезпечення воно відноситься?; 4) чи здатне виявлене шкідливе програмне забезпечення надавати третім особам несанкціонований (віддалений) доступ до вказаного мобільного пристрою і чи можливо за допомогою такого програмного забезпечення віддалено проводити листування у мессенджері «Telegram»?; 5) чи містяться на мобільному телефоні «Xiaomi Redmi Note 9» моделі «M2003J6B2G» відомості, що свідчать про здійснення несанкціонованого (відділеного) доступу до нього третіх осіб (відповідні сесії, підключення, використання функцій з віддаленого керування, лог-файли тощо)?; 6) якщо так, то чи можливо визначити дату несанкціонованого (віддаленого) доступу до зазначеного мобільного телефону, IP-адреси пристроїв, з яких здійснено несанкціонований (відділений) доступ до нього, а також IP-адреси даного мобільного телефону у момент такого доступу?» [128].

В інших ухвалах, якими було призначено комплексну комп'ютерно-технічну та у сфері телекомунікаційних систем і мереж експертизу перед

експертами також ставилось питання про «діапазон IP-адрес, до яких входить IP-адреса, на якій розміщується веб-сайт/ресурс» [141], а також «наявність ознак несанкціонованого втручання в роботу електронно-обчислюваних машин (комп`ютерів), автоматизованих систем та комп`ютерних мереж чи мереж електрозв`язку, що призвело до витоку, втрати, підробки блокування інформації» [142].

Аналіз наведених судових рішень дозволяє дійти висновку, що призначення саме комплексної експертизи в означених ситуаціях було зумовлене складним і багатокомпонентним характером досліджуваних об'єктів та обставин кримінального правопорушення. Питання, що охоплюються комп'ютерно-технічною експертизою були включені з метою встановити технічні аспекти функціонування комп'ютерних систем і пристроїв: спосіб збереження та обробки інформації, факт втручання в роботу системи, використання спеціального програмного забезпечення, а також дії користувача на конкретному цифровому носії. Водночас, цього недостатньо для повного з'ясування механізму вчинення кримінального правопорушення, якщо він був вчинений через мережеві взаємодії.

Питання, що відповідно до законодавства про судову експертизу охоплюються експертизою електронних комунікацій, у свою чергу, були спрямовані на дослідження процесів передавання інформації: аналіз трафіку, мережевих з'єднань, обміну повідомленнями, використання каналів зв'язку, облікових записів і сервісів електронних комунікацій. Таке поєднання можливостей двох експертиз потенційно надає змогу відтворити повний ланцюг подій - від дій на конкретному пристрої до їх реалізації в мережевому середовищі, встановити роль кожного технічного елемента та забезпечити повноту й об'єктивність встановлення фактичних обставин у кримінальному провадженні.

Процесуальний порядок призначення експертизи електронних комунікацій загалом не має специфічних особливостей: сторона обвинувачення залучає експерта для проведення такої експертизи за

дорученням, а сторона захисту на договірних засадах або шляхом звернення до слідчого судді у порядку ст. 244 КПК України (ч.1 ст. 244 КПК України) [153, с. 350].

Як показує аналіз судової практики, при зверненні до слідчого судді та подальшому розгляді клопотання, сторона захисту загалом стикається із доволі традиційними для даної категорії клопотань проблемами. Це зокрема, стосується доказування неможливості самостійного залучення експерта та наявності об'єктивних сумнівів щодо правильності висновків та їх обґрунтованості [137], а також визначення об'єктів для експертного дослідження [134]. Крім того, на практиці виникають питання щодо коректного тлумачення підстав залучення експерта, передбачених ч. 1 ст. 244 КПК України, зокрема у випадках, коли об'єкт, що підлягає експертному дослідженню, не знаходиться у володінні сторони захисту. До прикладу, в одній із ухвал слідчим суддею було зазначено наступне: «Так, захисник посилається на неможливість надати експерту на дослідження телекомунікаційний засіб, оскільки він вилучений в ході проведення обшуку та перебуває у слідчого.

Однак, залучення експерта та надання йому об`єкта експертизи не є тотожними поняттями. Відмови слідчого у надані експерту для дослідження вилученого телекомунікаційного засобу матеріали клопотання не містять» [135].

У цьому зв'язку варто зазначити, що положення ст. 244 КПК України не покладають на сторону захисту обов'язку попереднього звернення до слідчого чи прокурора з клопотанням про призначення експертизи. Крім того, у ч.8 ст. 244 КПК України передбачено, що «при задоволенні клопотання про залучення експерта слідчий суддя у разі необхідності має право за клопотанням особи, яка звернулася з клопотанням про залучення експерта, вирішити питання про отримання зразків для експертизи відповідно до ст. 245 КПК України». Водночас обов'язок доведення наявності підстав, визначених ч. 1 ст. 244 КПК України, безперечно покладається на сторону захисту. При

цьому, на неї також покладається завдання належного формулювання запитань, які підлягають постановці перед експертом, а також обґрунтування доцільності проведення відповідного експертного дослідження.

Але задля усунення усіх протиріч у коректному визначенні підстав залучення експерта за клопотання сторони захисту, вважаємо за доцільне доповнити ч.6 ст. 244 КПК України другим абзацом та викласти його у такій редакції: «Слідчий суддя не може відмовити у задоволенні клопотання про залучення експерта з тих підстав, що сторона захисту не зверталась попередньо із відповідним клопотанням до слідчого, прокурора».

Проведений аналіз правозастосовної практики дає підстави дійти висновку, що експертиза електронних комунікацій посідає одне з провідних місць серед засобів доказування у кримінальних провадженнях щодо правопорушень, учинених у кіберпросторі. Її значущість обумовлена об’єктивною складністю виявлення, ідентифікації та вилучення цифрових слідів злочинної діяльності, а також потребою застосування спеціальних знань для встановлення технічних характеристик електронних пристроїв, способів передавання даних, функціональних можливостей телекомунікаційних систем і взаємозв’язку між окремими подіями, що мали місце у цифровому середовищі.

Завдання експертизи електронних комунікацій є різноплановими та комплексними й охоплюють як визначення технічних параметрів пристроїв і мереж, так і встановлення фактів доступу до інформації, маршрутизації та передачі даних, а також з’ясування функціонального призначення телекомунікаційного обладнання. Особливо вагоме практичне значення цей вид експертизи має у кримінальних провадженнях, у межах яких об’єктами дослідження виступають складні технічні системи або програмно-апаратні комплекси, зокрема у справах про порушення авторського права і суміжних прав, несанкціонований доступ до інформаційних систем чи незаконне використання телекомунікаційних мереж.

ВИСНОВКИ

1. Основними напрямками дослідження проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі є: 1) наукові дослідження, присвячені криміналістичним проблемам розслідування кримінальних правопорушень, вчинених у кіберпросторі; 2) наукові дослідження, присвячені криміналістичним проблемам розслідування окремих категорій кримінальних правопорушень, вчинених у кіберпросторі; 3) наукові дослідження, які присвячені питанням використання електронних (цифрових) доказів у кримінальному процесуальному доказуванні; 4) наукові дослідження, які присвячені питанням використання спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі; 5) наукові дослідження, присвячені питанням кримінологічного аналізу кіберзлочинності та розробки заходів протидії цьому явищу; 6) наукові дослідження, присвячені питанням міжнародно-правового співробітництва у сфері боротьби зі злочинністю; 7) міждисциплінарні дослідження проблем протидії кіберзлочинності та дослідження протидії кіберзлочинності у межах інших галузей науки.

2. Кримінальне правопорушення, вчинене у кіберпросторі – це передбачене законом України про кримінальну відповідальність суспільно небезпечне винне діяння, що вчиняється суб’єктом кримінального правопорушення у межах або з використанням кіберпростору як особливого соціально-технічного та інформаційного середовища, шляхом застосування інформаційно-комунікаційних технологій, комп’ютерних систем, мереж чи цифрових даних, та посягає на охоронювані кримінальним законом суспільні відносини.

3. Класифікацію кримінальних правопорушень, вчинених у кіберпросторі доцільно здійснювати залежно від способу реалізації їх об’єктивної сторони.

За цим критерієм слід виокремлювати виключно кіберпросторові кримінальні правопорушення, які можуть бути вчинені виключно у кіберпросторі та варіативно-кіберпросторові кримінальні правопорушення, об'єктивна сторона яких може бути реалізована як у фізичному середовищі, так і у кіберпросторі.

До виключно кіберпросторових кримінальних правопорушень слід віднести, зокрема, такі кримінальні правопорушення як: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України); 2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК України); 3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2 КК України); 4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК); 5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України).

Варіативно-кіберпросторовими кримінальними правопорушеннями є: 1) шахрайство (ст. 190 КК України); 2) порушення недоторканності приватного життя (ст. 182 КК України); 3) погроза вбивством (ст. 129 КК України); 4) ввезення, виготовлення, збут і розповсюдження порнографічних предметів (у частині розповсюдження) (ст. 301 КК України); 5) легалізація (відмивання) доходів, одержаних злочинним шляхом (ст. 209 КК України); 6) дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або

на захоплення державної влади (ст. 109 КК України); 7) колабораційна діяльність (ст. 111^1 КК України); 8) виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436^2 КК України) тощо.

4. Мінімальними гарантіями захисту права на повагу до приватного та сімейного життя у кіберпросторі відповідно до вимог статті 8 Конвенції, які випливають із прецедентної практики ЄСПЛ є: 1) чітке законодавче визначення категорій осіб та даних, щодо яких можливе перехоплення; 2) наявність попереднього судового контролю або ефективного подальшого нагляду за спостереженням; 3) нормативне формулювання критеріїв, за якими ухвалюється рішення про ініціювання перехоплення; 4) обмеження строків зберігання даних та встановлення чіткого порядку їх знищення.

5. Основними міжнародними стандартами розслідування кіберзлочинів у процесуальному аспекті, які є спільними для усіх регіональних систем захисту прав людини є наступні: 1) обов'язок держав запровадити чітку правову основу для отримання доступу до інформації, яка зберігається в електронних системах; 2) зобов'язання держав адаптувати компетенцію національних органів і включити до неї переслідування транскордонних злочинів, а також забезпечити можливість здійснення кримінального переслідування, коли правопорушник чи наслідки злочину охоплюють кілька держав-учасниць; 3) здійснення правоохоронними органами пошуку та вилучення виключно у межах конкретного кримінального провадження із забезпеченням оригінальності вилучених даних, цілісності доказів, а також обов'язковим документуванням відповідних правових процедур; 4) забезпечення можливості екстрадиції осіб, які вчинили кіберзлочини; 5) визначення основних видів міжнародно-правової допомоги при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі, серед яких: передача запитів між центральними органами, обмін інформацією, доказами, документами, матеріальними та цифровими даними, у т.ч. без вимоги подвійної криміналізації; 6) забезпечення конфіденційності інформації,

отриманої у межах міжнародно-правової допомоги; 7) необхідність санкціонування компетентним органом процесуальних дій, які передбачають втручання у приватне життя осіб.

6. Електронні (цифрові) докази є фактичними даними в електронній формі, які отримані в передбаченому КПК України порядку, характеризуються цілісністю, автентичністю та придатністю для дослідження та мають значення для встановлення фактів та обставин кримінального провадження. З огляду на їх існування в електронній формі, електронні (цифрові) докази відображаються на відповідному електронному носії – як фізичному, так і віртуальному.

Класифікацію електронних (цифрових) доказів доцільно здійснювати за їх формою, на основі якої виокремлювати електронні документи, електронні повідомлення, віртуальні активи, технічні дані та іншу інформацію в електронній (цифровій) формі.

Задля вдосконалення механізму формування та використання електронних (цифрових) доказів у кримінальному процесуальному доказуванні КПК України необхідно доповнити статтею 99-1 у такій редакції:

«Стаття 99-1. Електронні (цифрові) докази

1. Електронними (цифровими) доказами є фактичні дані в електронній формі, які отримані в передбаченому цим Кодексом порядку, характеризуються цілісністю, автентичністю та придатністю для дослідження та мають значення для встановлення фактів та обставин кримінального провадження.

2. До електронних (цифрових) доказів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати:

1) електронні документи та інші носії інформації в електронній формі, передбачені пунктами 1, 3 частини другої статті 99 цього Кодексу;

2) електронні повідомлення;

3) віртуальні активи;

4) логи, дані клієнтського середовища, контекстні дані, метадані та інші технічні дані;

5) інша інформація в електронній (цифровій) формі».

7. Джерелами електронних (цифрових) доказів є будь-які електронні носії фактичних даних, які існують у фізичному або віртуальному виді. До джерел електронних (цифрових) доказів у ході досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, належать: 1) електронні пристрої, які містять значиму для кримінального провадження інформацію; 2) електронні комунікаційні системи, які використовувалися в ході підготовки до кримінальних правопорушень у кіберпросторі, їх вчинення та приховування наслідків цих правопорушень; 3) сервери постачальників електронних комунікаційних послуг, хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів.

8. При формуванні нормативної моделі допустимості доказів, отриманих із відкритих джерел, цілком прийнятною є аналогія із регламентацією допустимості показань з чужих слів, які відповідно до ч.6 ст. 97 КПК України не можуть бути допустимим доказом факту чи обставин, на доведення яких вони надані, якщо показання не підтверджується іншими доказами, визнаними допустимими згідно з правилами, відмінними від положень частини другої цієї статті.

Виходячи із цього, доцільно доповнити КПК України ст. 88^2 із назвою «Допустимість доказів, отриманих із відкритих джерел» та викласти її у такій редакції: «Докази, отримані із відкритих джерел можуть бути визнані допустимими виключно за умови підтвердження джерела їх походження та якщо відповідні відомості підтверджуються іншими доказами, які визнані допустимими за правилами цього Кодексу».

9. Положення абз. 2 ч. 6 ст. 236 КПК України в частині використання формулювання «виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку» потребує коригування, оскільки не відповідає вимозі передбачуваності закону та

створює передумови для зловживань з боку сторони обвинувачення під час проведення обшуку.

У зв'язку із цим, пропонуємо викласти абзац другий ч.6 ст. 236 КПК України у такій редакції: «Прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення обшуку виключно якщо дозвіл на такий пошук наданий в ухвалі слідчого судді». Така регламентація відповідатиме міжнародним стандартам та стандартам, виокремленим ЄСПЛ у частині захисту права на повагу до приватного життя. Чинна редакція абз. 2 ч.6 статті 236 КПК України може бути застосовною лише в умовах воєнного стану, коли публічний інтерес розслідування злочинів проти основ національної безпеки превалює над приватним, але передбачений нею порядок не може виступати ординарною правовою процедурою.

10. Зняття інформації з електронних комунікаційних мереж є тим різновидом НСРД, що спрямований на фіксацію динамічної інформації, яка циркулює у мережах, і незважаючи навіть на стислі строки розгляду слідчим суддею суду апеляційної інстанції відповідного клопотання, існує істотний ризик втрати відомостей, які мають важливе значення для встановлення фактичних обставин кримінального провадження.

Враховуючи наведене, пропонуємо доповнити статтю 263 КПК України ч.5 такого змісту: «Зняття інформації з електронних комунікаційних мереж до постановлення ухвали слідчого судді може бути розпочато на підставі постанови слідчого, прокурора лише у випадку, передбаченому частиною першою статті 250 цього Кодексу».

11. Спеціальні знання при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі – це сукупність наукових знань і практичних навичок у сфері інформаційних технологій, комп'ютерних систем і мереж, цифрової та комп'ютерно-технічної криміналістики, телекомунікацій, інформаційної безпеки, програмування, аналізу шкідливого програмного

забезпечення та електронних фінансових технологій, здобутих у межах академічної підготовки й професійного досвіду, носіями яких є залучені до кримінального провадження за рішенням слідчого, прокурора, слідчого судді чи суду особи, що використовуються з метою вирішення питань, необхідних для повного, всебічного й об'єктивного встановлення фактичних обставин кримінального провадження.

При розслідуванні кримінальних правопорушень, вчинених у кіберпросторі актуальними є як процесуальні, так і непроцесуальні форми використання спеціальних знань. Процесуальні форми здебільшого проявляються у залучення відповідних спеціалістів при проведенні слідчих (розшукових) дій. Непроцесуальна форма використання спеціальних знань проявлятиметься здебільшого у консультативній та довідковій діяльності суб'єктів спеціальних знань.

Найпоширенішими видами експертиз, які призначаються у кримінальних провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі є комп'ютерно-технічна експертиза та експертиза електронних комунікацій.

При зверненні до слідчого судді та подальшому розгляді клопотання про залучення експерта у порядку ст. 244 КПК України у кримінальному провадженні щодо відповідної категорії кримінальних правопорушень, сторона захисту загалом стикається із доволі традиційними для даної категорії клопотань проблемами. Це зокрема, стосується доказування неможливості самостійного залучення експерта та наявності об'єктивних сумнівів щодо правильності висновків та їх обґрунтованості , а також визначення об'єктів для експертного дослідження.

Задля усунення протиріч у коректному визначенні підстав залучення експерта за клопотанням сторони захисту, вважаємо за доцільне доповнити ч.6 ст. 244 КПК України другим абзацом та викласти його у такій редакції: «Слідчий суддя не може відмовити у задоволенні клопотання про залучення

експерта з тих підстав, що сторона захисту не зверталась попередньо із відповідним клопотанням до слідчого, прокурора».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістик*и. 2023. Вип. 1 (30). С. 126-143.

2. Алєксєєва-Процюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247-253.

3. Анапольська А.І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків: дис. … канд. юрид. наук : 12.00.09. Луганськ, 2011. 224 с.

4. Бабаєва О.В., Авербах Д.В. Щодо питання про використання доказів, отриманих з від-критих джерел, у кримінальному провадженні. *Науковий вісник Ужгородського Національного Університету: Серія «Право». Випуск 83: частина 3*. С. 169-174.

5. Басай В.Д., Томин С.В. Дослідження віртуальних слідів – перспективний напрямок криміналістичного слідознавства. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 220-223.

6. Басиста І.В., Гаврилюк Л.В., Гутник А.В., Хитра А.В. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Серія «Право».* 2024. Вип.17(29). С. 227-243.

7. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414.-418.

8. Бишевець О.В. Використання спеціальних знань у доказуванні в кримінальних провадженнях. *Вісник кримінального судочинства*. 2015. № 2. С. 187-193.

9. Будник Л., Карапетян О., Метельський І. Кіберзлочини: типології, фінансова розвідка, використання спеціальних знань. *Актуальні проблеми правознавства*. 2022. № 3. С. 158-164.

10. Вапнярчук В.В. Щодо дослідження змісту електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку під час кримінального провадження. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 967-972.

11. Васильковський І.І. Взаємодія правоохоронних органів при розслідуванні кіберзлочинів : дис. … канд. юрид. наук : спец. 12.00.09. Київ, 2019. 257 с.

12. Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін.; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Видавництво Національної академії внутрішніх справ, 2020. 104 с.

13. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації / авт. колектив: А.В. Захарко, А.Г. Гаркуша, В.В. Рогальська, І.В. Краснобрижий, О.В. Брягін Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. 73 с.

14. Вирок Ічнянського районного суду Чернігівської області від 26 квітня 2023 року, судова справа № 733/923/22. URL: https://reyestr.court.gov.ua/Review/110482776

15. Вирок Макарівського районного суду Київської області від 20 квітня 2023 року, судова справа № 370/179/23. URL: https://reyestr.court.gov.ua/Review/110354341

16. Вирок Чернігівського районного суду Чернігівської області від 17 лютого 2023 року, судова справа № 748/1824/22. URL: https://reyestr.court.gov.ua/Review/109074116

17. Галушко П.П. Кримінологічна характеристика та протидія кіберзлочинності в Україні в умовах війни : дис. … д-ра філософії. 081 «Право». Харків, 2025. 236 с.

18. Глинська Н.В., Клепка Д.І. Основні аспекти стратегії унормування інституту цифрових доказів в кримінальному процесуальному законодавстві. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 48-66.

19. Гловюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету. Серія «Право»*. 2025. Випуск 91. Частина 4. С. 251-259.

20. Гора І.В. Проблеми використання спеціальних знань у кримінальному судочинстві України. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 209-214.

21. Господарський процесуальний кодекс України від 06.11.1991 р. № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12

22. Гринько Л.П. Фішинг як спосіб вчинення шахрайства у мережі інтернет. *Полтавський правничий часопис*. 2022. № 4. С. 16-39.

23. Грібов М.Л. Поняття та правове регулювання використання спеціальних знань, умінь і навичок у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ*. 2019. № 1. С. 13-21.

24. Гутник А.В., Хитра А.Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні. Львів: Львівський державний університет внутрішніх справ, 2022. 204 с.

25. Данатарова В.М. Особливості тимчасового доступу до речей і документів операторів та провайдерів телекомунікацій при розслідуванні шахрайства, вчиненого з використанням засобів мобільного зв'язку. *Актуальні проблеми експертного забезпечення досудового розслідування* : матеріали наук.-практ. семінару (Дніпро, 29 травня 2020 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. С. 215-218.

26. Демура М.І., Клепка Д.І., Крицька І.О. Щодо обмеження прав особи під час вилучення цифрових джерел доказової інформації у кримінальному провадженні. *Форум права*. 2020. № 1 (60). С. 37-46.

27. Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 19–22.

28. Довженко О.Ю. Деякі питання призначення комп’ютерно-технічної експертизи під час розслідування кіберзлочинів. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2019. Вип. 55. Т. 2. С. 124-127.

29. Довженко О.Ю. Основи методики розслідування кіберзлочинів : дис. … канд. юрид. наук : 12.00.09. Одеса, 2020. 235 с.

30. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи 2003 року. URL: https://zakon.rada.gov.ua/laws/card/994_687

31. Докази та доказування у кримінальному провадженні: навчальний посібник / Р.І. Благута, Ю.В. Гуцуляк, О.М. Дуфенюк та ін. Львів: Львівський державний університет внутрішніх справ, 2018. 272 с.

32. Дуфенюк О. Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації. Baltic Journal of Legal and Social Sciences. 2022. №. 1. С. 46–56.

33. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: затверджено Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text

34. Каланча І.Г. Докази електронної форми у кримінальному процесі України: теорія та практика: дис. … д-ра юрид. наук. 12.00.09. Київ, 2025. 617 с.

35. Капліна О.В. Правозастосовне тлумачення норм кримінально-процесуального права: монографія. Харків: Право, 2008. 296 с.

36. Кіберзлочинність та електронні докази: навчальний посібник / Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан; за ред. О. Денькович, Г. Шмельцер. Електронне видання. Львів: Львівський національний університет імені Івана Франка, 2022. 298 с.

37. Коваленко А. Класифікація оглядів комп'ютерних даних у кримінальному провадженні. *Актуальні питання судової експертизи і криміналістики*: матеріали Міжнародної науково-практичної конференції (м. Харків, 23 травня 2025 року). Харків: ННЦ «ІСЕ ім. Засл. проф. М.С. Бокаріуса», 2025. С. 212-215.

38. Коваленко А.В. Криміналістичне вчення про збирання, дослідження та використання доказів у кримінальному провадженні: монографія. Київ: Алерта, 2024. 558 с.

39. Коваленко А.В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. *Війна в Україні: зроблені висновки та незасвоєні уроки* : збірник тез Міжнародної науково-практичної конференції (22–23 лютого 2024 року) / упор. У. О. Цмоць. Львів : Львівський державний університет внутрішніх справ, 2024. С. 413-417.

40. Коваленко А.В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка*. 2022. Вип. 4 (100). С. 226-236.

41. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів: дис. ..д-ра філос. 081 «Право». Дніпро, 2022. 229 с.

42. Ковальчук С.О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи: дис. … д-ра юрид. наук: 12.00.09. Одеса, 2018. 636 с.

43. Ковальчук С.О., Крет Г.Р. Науково-практичний коментар до Глави 21 Кримінального процесуального кодексу України «Негласні слідчі (розшукові) дії». Київ: Прецедент, 2024. 244 с.

44. Когутич І. І. Окремі питання сутності та форм використання спеціальних знань у кримінальному провадженні. *Вісник Академії адвокатури України*. 2015. Т. 12. Ч. 2 (33). С. 112–123.

45. Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15

46. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418-421.

47. Колеснікова І. Значення цифрових слідів під час розслідування кримінальних правопорушень. *Актуальні питання судової експертизи і криміналістики*: збірник матеріалів Міжнародної науково-практичної конференції з нагоди 100-річчя Національного наукового центру «Інститут судових експертиз ім. засл. проф. М. С. Бокаріуса» (м. Харків, 10 листопада 2023 року). Харків: ННЦ «ІСЕ ім. Засл. проф. М.С. Бокаріуса», 2023. С. 194-196.

48. Коломійцев С.О. Поняття та види комп'ютерних даних, їх носіїв у кримінальному провадженні. *Права людини в Україні: минуле, сьогодення, майбутнє*: тези доповідей учасників ІІІ Всеукраїнської науково-практичної конференції (м. Харків, 9 грудня 2022 року). Харків: НДІ ППСН, 2022. С. 127.

49. Комар Ю.М. Визначення поняття спеціальні знання та їх використання у кримінальному процесі. *Актуальні питання криміналістики*: матеріали Всеукр. наук.-практ. конф. (Київ, 20 груд. 2019 р.). Київ : Нац. акад. внутр. справ, 2019. С. 113-116.

50. Конвенція про кіберзлочинність від 23.11.2001 р., ратифікована із застереженнями і заявами Законом України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575

51. Концептуальні основи цифровізації кримінального провадження України: монографія / за заг. ред. Н.В. Глинської. Харків: Право, 2024. 452 с.

52. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис….канд. юрид. наук. 12.00.09. Харків, 2017. 22 с.

53. Коршикова Т.В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки: дис. … канд. юрид. наук : 12.00.09. Київ, 2021. 255 с.

54. Косович В. Правові дефініції як засіб забезпечення створення досконалих нормативно-правових актів України. *Вісник Львівського університету. Серія: Юридична*. 2013. Вип. 57. С. 43-52.

55. Кравчук О.О. Тимчасовий доступ до речей і документів в умовах воєнного часу. *Проблеми кваліфікації та розслідування кримінальних правопорушень в умовах воєнного стану*: матеріали наук.-теор. конф. (м. Київ, 26 травня 2022 р.). Київ: Нац. акад. внутр. Справ, 2022. С. 108-112.

56. Крижановський А.С. Критерії віднесення електронної інформації до видів доказів. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 1027-1032.

57. Крицька І.О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301-305.

58. Кульбашна О.А. До питання правової природи електронних документів. *Юридичний науковий електронний журнал*. 2024. № 4. С. 379-382.

59. Куриленко Д.В. Інститут обізнаних осіб у змагальному кримінальному провадженні: автореф. …дис. канд. юрид. наук. 12.00.09. Харків, 2017. 16 с.

60. Курман О.В. Судові експертизи у сфері інформаційних технологій: деякі проблеми підготовки та проведення. *Аналітично-порівняльне правознавство*. 2023. № 9. С. 477-481.

61. Липкан І.І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій: дис. … канд. юрид. наук. Київ, 2025. 259 с.

62. Логіка: підручник / О.М. Юркевич, С.В. Качурова, О.П. Невельська-Гордєєва та ін.; за заг. ред. О.Г. Данильяна. Харків: Право, 2022. 220 с.

63. Лук’янчиков Є.Д., Лук’янчиков Б.Є., Петряєв С.Ю. Використання спеціальних знань у кримінальному провадженні. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2019. Випуск 4 (44). С. 125-130.

64. Луцик В.В. Зняття інформації з електронних комунікаційних мереж: фокус новел. *Юридичний науковий електронний журнал*. 2022. № 8. С 500-504.

65. Любченко М.І. Юридична термінологія: поняття, особливості, види: монографія. Харків: ТОВ «Видавництво «Права людини»», 2015. 280 с.

66. Малахова О.В. До питання огляду сторонами кримінального провадження змісту Інтернет-сторінок. *Вісник кримінального судочинства*. 2017. № 1. С. 64-69.

67. Маркіна А.В. Сутність електронних доказів у кримінальному провадженні. *Право і суспільство*. 2025. № 2. С. 387-393.

68. Методика розслідування шахрайства в інтернет-комерції: теорія та практика : монографія / К. О. Чаплинський, А. В. Рейнгольд, Н. В. Павлова. Одеса : Видавництво «Юридика», 2024. 242 с.

69. Михайленко І.В. Право людини на недоторканність приватного життя: поняття, аспекти, механізм реалізації: автореф. дис. …канд. юрид. наук. 12.00.01. Харків, 2014. 21 с.

70. Мілімко Л.В., Жидовцев Я.В. Електронні докази в кримінальному судочинстві України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. Вип. 88. Ч. 3. С. 302-308.

71. Московчук Д.О. Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження: дис. … д-ра філософії: 081 «Право». Одеса, 2023. 198 с.

72. Настільна книга судді: матеріали для розгляду справ про міжнародні злочини. Київ: Національна школа суддів України, 2024. 823 с.

73. Неділько Я.В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп’ютерних технологій : дис. … д-ра філософії. 081 «Право». Київ, 2023. 257 с.

74. Нізовцев Ю.Ю., Омельян О.С. Щодо підготовки та призначення судових експертиз у кримінальних провадженнях, пов’язаних із кібератаками. *Криміналістичний вісник (Forensic Herald)*. 2021. № 2(36). С. 59-68.

75. Орлов Ю.Ю., Чернявський С.С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 12-24.

76. Пашковський М.І. Про колізійність приписів щодо процесуальної форми доступу до змісту відомостей, що містяться в мобільних терміналах систем зв’язку. *Процесуальне та криміналістичне забезпечення досудового розслідування*: тези доповідей учасників науково-практичного семінару (26 листопада 2021 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2021.С. 108-111.

77. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : спец. 12.00.09. Харків, 2007. 228 с.

78. Пелещак О.Р. Типові слідчі ситуації початкового етапу розслідування кібердиверсій. *Соціально-правові студії*. 2021. № 2. С. 94-100.

79. Петрик В.В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90. Ч.4 С. 324-328.

80. Підхід до оцінки допустимості доказів, у тому числі цифрових, має бути універсальним у всіх провадженнях, незалежно від того, стосуються вони воєнних чи інших категорій кримінальних правопорушень: суддя ВС Антонюк. URL: https://advokatpost.com/pidkhid-do-otsinky-dopustymosti- dokaziv-u-tomu-chysli-tsyfrovykh-maie-buty-universalnym-u-vsikh- provadzhenniakh-nezalezhno-vid-toho-stosuiutsia-vony-voiennykh-chy- inshykh-katehorij-kryminalnykh-pravop/

81. Погорецький М.А. Документування і доказування міжнародних злочинів в Україні: процесуально-криміналістичні та цифрові стандарти прийнятності доказів для Міжнародного кримінального суду та спеціального військового трибуналу. *Аналітично-порівняльне правознавство*. 2025. № 6. Ч. 3. С. 599-615.

82. Постанова Верховного Суду від 12 червня 2024 р., судова справа № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340

83. Постанова Верховного Суду від 04 листопада 2021 року, судова справа № 326/1385/18. URL: https://reyestr.court.gov.ua/Review/101100299

84. Постанова Верховного Суду від 06 лютого 2024 р., судова справа № 645/6247/16-к . URL: https://reyestr.court.gov.ua/Review/116862907

85. Постанова Верховного Суду від 09 квітня 2020 року, судова справа № 727/6578/17. URL: https://reyestr.court.gov.ua/Review/88749345

86. Постанова Верховного Суду від 09 квітня 2024 року, судова справа № 369/4929/19. URL: https://reyestr.court.gov.ua/Review/118465118

87. Постанова Верховного Суду від 09 травня 2024 року, судова справа № 496/5125/15-к. URL: https://lpd.court.gov.ua/legal-position/12401/document/43699

88. Постанова Верховного Суду від 13 березня 2024 року, судова справа № 953/3558/22. URL: https://reyestr.court.gov.ua/Review/117757857

89. Постанова Верховного Суду від 22 листопада 2018 року, судова справа № 477/233/16-к. URL: https://reyestr.court.gov.ua/Review/78160586

90. Постанова Верховного Суду від 22 лютого 2024 року, судова справа № 208/3704/22. URL: https://reyestr.court.gov.ua/Review/117277325

91. Постанова Верховного суду від 25 жовтня 2023 року, судова справа № 755/3105/17. URL: https://reyestr.court.gov.ua/Review/114581899

92. Постанова Верховного Суду від 27 жовтня 2021 року, судова справа № 759/7443/17. URL: https://reyestr.court.gov.ua/Review/100734866

93. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 25 вересня 2023 р., судова справа № 208/2160/18. URL: https://reyestr.court.gov.ua/Review/113817314

94. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів: проєкту Закону України» від 01.09.2020 р. (реєстраційний № 4004), внесений народними депутатами України Д.А. Монастирським та ін. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771.

95. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20

96. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: Наказ Міністерства юстиції від 08.10.98 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/en/z0705-98#Text

97. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

98. Про порядок денний чотирнадцятої сесії Верховної Ради України дев'ятого скликання: Постанова Верховної Ради України від 03.09.2025 р. № 4586-IX. URL: https://zakon.rada.gov.ua/laws/show/4586-IX

99. Про хмарні послуги: Закон України № 2075-IX від 17.02.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2075-20

100. Проект Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо спрощення та удосконалення діючих норм Закону з метою уникнення покарання винними особами та розвантаження судових органів» від 03.04.2020 р. № 3303. URL: https://ips.ligazakon.net/document/ji01796i

101. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

102. Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філософії. 081 «Право». Львів, 2021. 248 с.

103. Ратнова А.В. Проведення огляду облікового запису користувача в соціальній мережі під час досудового розслідування кримінального провадження. *Прикарпатський юридичний вісник*. 2020. Вип. 3 (32). С. 97-102.

104. Рейнгольд А.В. Основи методики розслідування шахрайства в інтернет-комерції : дис. … д-ра філософії. 081 «Право». Дніпро, 2023. 250 с.

105. Розумний С.М. Залучення спеціаліста для проведення слідчих (розшукових) дій при розслідуванні кіберзлочинів. *Актуальні проблеми кримінально-правового, кримінального процесуального та криміналістичного забезпечення протидії злочинності* : матер. Міжнар. наук.-практ. конф. (08 груд. 2023 р., м. Дніпро). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2024. С. 244-247.

106. Романюк Б.В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві: автореф дис. ... канд. юрид. наук. 12.00.09. Київ, 2002. 20 с.

107. Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140-150.

108. Романюк В.В., Фоміна Т.Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. *Вісник Кримінологічної асоціації України*. 2024. № 2 (32). С. 344-353.

109. Салманов О. В., Топчій А.О. Особливості фіксації доказів учинення воєнних злочинів із відкритих джерел Інтернету. *Злочинність і протидія їй в умовах війни: глобальний, регіональний та національний виміри*: зб. доп. наук.-практ. конф. (м. Вінниця, 12 квіт. 2023 р.) Харків: ХНУВС, 2023. С. 195-198.

110. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник / О. А. Самойленко. Одеса, 2020. 112 с.

111. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

112. Серьогін В.О. Зміст і обсяг права на недоторканність приватного життя (прайвесі). *Вісник Академії правових наук України*. 2010. № 4. С. 88–97.

113. Сисолятін В.В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … д-ра філософії. 081 «Право». Київ, 2024. 230 с.

114. Скрипник А.В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні: дис. … д-ра філософії. 081 «Право». Харків, 2021. 379 с.

115. Скрипник А.В. Окремі цифрові аспекти обшуку затриманої особи. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/10/149.pdf

116. Смаль І.А. Теоретичні засади формування і практика застосування електронних доказів у кримінальному процесі: дис. … д-ра філософії: 081 «Право». Чернігів, 2025. 329 с.

117. Степанюк Р.Л. Поняття спеціальних знань у кримінальному провадженні. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2014. Спецвип. С. 38–42.

118. Сусукайло В.А. Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем : дис. … д-ра філософії: 125 «Кібербезпека». Львів, 2024. 196 с.

119. Тагієв С.Р. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 13-24.

120. Татарин І.І., Євхутич І.М. Тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, як захід забезпечення кримінального провадження. *Polish Journal of Science*. 2021. № 36. С. 32-35.

121. Теоретичні та праксеологічні засади розслідування кримінальних правопорушень у кіберпросторі: монографія / Ю.О. Виходець, В.Г. Дрозд, М.М. Єфімов, В.Б. Коба, І.О. Луговий, Н.В. Павлова, К.О. Чаплинський. Дніпро: Дніпровський державний університет внутрішніх справ, 2025. 212 с.

122. 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 : спец. 12.00.09. Київ, 2021. 268 с.

123. Тимчишин А.М. Спеціальні знання у кримінальному процесі України: теорія та практика: дис. …д-ра юрид. наук. 12.00.09. Кропивницький, 2023. 438 с.

124. Торбас О. Оцінка законності огляду телефону, який було вилучено під час обшуку. *Теоретико-прикладні проблеми правового регулювання в Україні* : матеріали V Всеукраїнської науково-практичної конференції (м. Львів, 10 грудня 2021 р.) / за заг. ред. І. В. Красницького. Львів : Львівський державний університет внутрішніх справ, 2021. С. 306-310.

125. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса: Видавництво «Юридика», 2024. 180 с.

126. Уваров В.Г. Зняття інформації з телекомунікаційних мереж. *Актуальні проблеми вітчизняної юриспруденції*. 2017. № 2. Том 1. С. 121-124.

127. Удовенко Ж.В. Проблеми забезпечення охорони таємниці приватного життя під час зняття інформації з транспортних телекомунікаційних мереж. *Наукові записки НаУКМА. Юридичні науки*. 2019. Том 3. С. 120-126.

128. Ухвала Новозаводського районного суду Чернігівської області від 01 травня 2025 року, судова справа № 751/6543/23. URL: https://reyestr.court.gov.ua/Review/127102410

129. Ухвала слідчого судді Галицького районного суду м. Львова від 17 січня 2019 року, судова справа № 461/4904/18. URL: https://reyestr.court.gov.ua/Review/79240375

130. Ухвала слідчого судді Голосіївського районного суду м. Києва від 11 квітня 2022 року, судова справа № 752/2703/22. URL: https://reyestr.court.gov.ua/Review/104096012

131. Ухвала слідчого судді Голосіївського районного суду м. Києва від 27 вересня 2021 року, судова справа № 752/24690/20. URL: https://reyestr.court.gov.ua/Review/10065388

132. Ухвала слідчого судді Жовтневого районного суду м. Полтави від 15 лютого 2019 р., судова справа № 554/10454/18. URL: https://reyestr.court.gov.ua/Review/79874609

133. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 05 березня 2019 року, судова справа № 202/403/19. URL: https://reyestr.court.gov.ua/Review/80249913

134. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 02 листопада 2023 року, судова справа № 202/13474/23. URL: https://reyestr.court.gov.ua/Review/115016510

135. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 15 листопада 2023 року, судова справа № 202/13474/23. URL: https://reyestr.court.gov.ua/Review/115050551

136. Ухвала слідчого судді Кам'янець-Подільського міськрайонного суду Хмельницької області від 05 жовтня 2023 року, судова справа № 676/6868/23. URL: https://reyestr.court.gov.ua/Review/114017509

137. Ухвала слідчого судді Ківерцівського районного суду Волинської області від 29 червня 2022 року, судова справа № 158/806/22. URL: https://reyestr.court.gov.ua/Review/105036977

138. Ухвала слідчого судді Кіровського районного суду м. Кіровограда від 08 жовтня 2019 року, судова справа № 404/7345/19. URL: https://reyestr.court.gov.ua/Review/84872136

139. Ухвала слідчого судді Личаківського районного суду Львівської області від 04 грудня 2025 року, судова справа № 463/11174/25. URL: https://reyestr.court.gov.ua/Review/132320289

140. Ухвала слідчого судді Ніжинського міськрайонного суду Чернігівської області від 26 червня 2023 року, судова справа № 740/3959/23. URL: https://reyestr.court.gov.ua/Review/111772056

141. Ухвала слідчого судді Печерського районного суду м. Києва від 30 травня 2019 року, судова справа № 757/27912/19-к. URL: https://reyestr.court.gov.ua/Review/82217099

142. Ухвала слідчого судді Печерського районного суду м. Києва від 30 травня 2019 року, судова справа № 757/27940/19-к. URL: https://reyestr.court.gov.ua/Review/82217090

143. Ухвала слідчого судді Рівненського міського суду Рівненської області від 02 жовтня 2019 року, судова справа № 569/18629/19. URL: https://reyestr.court.gov.ua/Review/84709802

144. Ухвала слідчого судді Святошинського районного суду м. Києва від 31 липня 2019 року, судова справа № 759/13808/19. URL: https://reyestr.court.gov.ua/Review/83480188

145. Фігурський В. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: юридичні науки*. 2023. № 4. С. 97-105.

146. Філімонов М.В. Використання цифрової інформації з відкритих джерел у кримінальному процесуальному доказуванні: постановка проблеми. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень* : у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 трав. 2023 р.) / за загальною редакцією С.В. Ківалова. Одеса: Видавництво «Юридика». 2023. Т. 2. С. 377-380.

147. Філімонов М.В. Втручання в електронне приватне спілкування у практиці європейського суду з прав людини: окремі питання. *Актуальні питання розвитку юридичної науки в період воєнного стану* : Міжнародна науково-практична конференція. Науково-дослідний інститут публічного права, 17 травня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 358-360.

148. Філімонов М.В. До питання щодо стану наукової розробленості проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі у юридичній доктрині. *Право і суспільство*. 2024. №6. С. 340-345. URL: http://pravoisuspilstvo.org.ua/archive/2024/6_2024/51.pdf

149. Філімонов М.В. Допустимість доказів, отриманих із веб-сайтів та інтернет-ресурсів: проблеми, доктрини та тенденції судової практики. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів*: матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 463-465.

150. Філімонов М.В. Міжнародні стандарти та зарубіжний досвід нормативної регламентації розслідування кримінальних правопорушень, вчинених у кіберпросторі. *Право і суспільство*. 2025. №3. Т. 2. С. 657-662. URL: http://pravoisuspilstvo.org.ua/archive/2025/3_2025/part_2/91.pdf

151. Філімонов М.В. Належний процесуальний порядок ознайомлення із інформацією, що міститься на цифрових пристроях: окремі питання у контексті практики ККС ВС. *Правові новели*. 2025. № 25. С.456-461. URL: http://legalnovels.in.ua/journal/25_2025/60.pdf ;

152. Філімонов М.В. Окремі питання допустимості доказів, отриманих у результаті зняття інформації з електронних інформаційних систем. *Європейські*

орієнтири України: нові виміри у воєнний час: матеріали міжнар.наук.- практ. конф. (Одеса, 16 травня 2025 р.). Одеса, 2025. С. 639-641.

153. Філімонов М.В. Окремі питання призначення експертизи електронних комунікацій під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. *Правові новели*. 2024. № 24. С. 347-355. URL: http://legalnovels.in.ua/journal/24_2024/48.pdf

154. Філімонов М.В. Питання забезпечення права особи на повагу до приватного життя у кіберпросторі в практиці Європейського суду з прав людини. *Юридичний науковий електронний журнал*. 2025. № 4. С. 632-634. URL: http://lsej.org.ua/4_2025/155.pdf

155. Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник Харківського національного університету внутрішніх справ*. 2023. № 3 (102). С. 207-220.

156. Фурашев В.А. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162-169.

157. Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15

158. Чернявський С.С., Фінагеєв В.О. Проблеми тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 179-185.

159. Чучко С.В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філософії. 081 «Право». Дніпро, 2021. 203 с.

160. Шаренко С.Л. Окремі питання здійснення судового контролю при застосуванні тимчасового доступу до речей і документів. *Вісник кримінального судочинства*. 2020. № 1-2. С. 102-111. С. 104-105.

161. Школьніков В.І. Правова основа отримання інформації з мережі інтернет у кримінальному провадженні. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2018. Вип. 4 (40). 172-174.

162. Щербаковський М., Сезонов В. Збирання та дослідження електронних документів із застосуванням спеціальних знань. *Теорія та практика судової експертизи і криміналістики*. 2024. Вип. 3 (36). С. 10-23.

163. Щербаковський М.Г., Коршенко В.А. Тактичні та організаційні особливості зняття інформації з транспортних телекомунікаційних мереж. *Криміналістика і судова експертиза*. Вип. 63. С. 154-162.

164. Яцишин М.Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю: дис. … канд. юрид. наук : 12.00.11. Київ, 2019. 230 с.

165. African Union Convention on Cyber Security and Personal Data Protection. URL:https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

166. Arab Convention on Combating Information Technology Offences 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

167. Case of Antović and Mirković v. Montenegro: Judgement of European Court of Human Rights (Application № 70838/13), 28 November 2017. URL: https://hudoc.echr.coe.int/fre?i=001-178904

168. Case of Azer Ahmadov v. Azerbaijan: Judgement of European Court Human Rights (Application № 3409/10), 22 July 2021. URL: https://hudoc.echr.coe.int/eng?i=001-211101

169. Case of Barbulescu v. Romania: Judgement of European Court Human Rights (Application № 61496/08), 28 November 2017. URL: https://hudoc.echr.coe.int/eng?i=001-17708

170. Case of Benedik v. Slovenia: Judgement of European Court of Human Rights (Application № 62357/14), 24 April 2018. URL: https://hudoc.echr.coe.int/fre?i=001-182455

171. Case of Big Brother Watch and others v. The United Kingdom: Judgement of European Court Human Rights (Application № 58170/13, 62322/14, 24960/15), 25 May 2021. URL: https://hudoc.echr.coe.int/fre?i=001-210077

172. Case of Breyer v. Germany: Judgement of European Court of Human Rights (Application № 50001/12), 30 January 2020. URL: https://hudoc.echr.coe.int/ukr?i=001-200442

173. Case of Centrum för Rättvisa v. Sweden: Judgement of European Court Human Rights (Application № 35252/08), 25 May 2021. URL: https://hudoc.echr.coe.int/fre?i=001-210278

174. Case of Denisov v. Ukraine: Judgement of European Court of Human Rights (Application № 76639/11), 25 September 2018. URL: https://hudoc.echr.coe.int/eng?i=001-186216

175. Case of Ekimdzhiev and Others v. Bulgaria: Judgement of European Court Human Rights (Application № 70078/12), 11 January 2022. URL: https://hudoc.echr.coe.int/eng? i=001-214673

176. Case of Gillberg v. Sweden: Judgement of European Court of Human Rights (Application № 41723/06), 3 April 2012. URL: https://hudoc.echr.coe.int/eng?i=001-110144

177. Case of Podchasov v. Russia: Judgement of European Court of Human Rights (Application № 33696/19), 13 February 2024. URL: https://hudoc.echr.coe.int/fre?i=001-230854

178. Case of Roman Zakharov v. russia: Judgement of European Court Human Rights (Application № 47143/06), 04 December 2015. URL: https://hudoc.echr.coe.int/fre?i=001-159324

179. Case of S. and Marper v. United Kingdom: Judgement of European Court of Human Rights (Applications № 30562/04 and 30566/04), 4 December 2008. URL: https://hudoc.echr.coe.int/fre?i=001-117816

180. Case of Sidabras and Džiautas v. Lithuania: Judgement of European Court of Human Rights (Applications № 55480/00 and 59330/00), 27 July 2004. URL: https://hudoc.echr.coe.int/eng?i=001-61942

181. Case of Szabó and Vissy v. Hungary: Judgement of European Court Human Rights (Application № 37138/14), 12 January 2016. URL: https://hudoc.echr.coe.int/eng?i=001-160020

182. Computer Fraud and Abuse Act (CFAA). URL: https://www.justice.gov/jm/jm-9-48000-computer-fraud

183. Computer Misuse Act 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents

184. Data Protection Act 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents

185. David G. Post. Governing Cyberspace. *Wayne Law Review*, 1996. Vol. 43. p. 155-171.

186. David R. Johnson & David G. Post. Law and Borders - The Rise of Law in Cyberspace. *Stanford Law Review*, 1996. Vol. 48. p. 1367-1402.

187. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

188. Electronic Communications Privacy Act of 1986. URL: https://www.congress.gov/bill/99th-congress/house-bill/4952

189. European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2018_346_R_0005&utm_

190. Henry H. Perritt, Jr. Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism? *Berkeley Technology Law Journal*, 1997. Vol. 12, pp. 413–482.

191. Trotter Hardy. The Proper Legal Regime for «Cyberspace». *University of Pittsburgh Law Review*, 1994. Vol. 55. p. 993-1055.

192. Investigatory Powers Act 2016. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents

193. Joel R. Reidenberg. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*, 1996. Vol. 45. p. 911-930.

194. Joel R. Reidenberg. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, Vol. 76. p. 553-559.

195. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: https:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001

196. Josh Goldfoot & Aditya Bamzai. A Trespass Framework for the Crime of Hacking. *The George Washington Law Review*. 2016.Vol. 84. p. 1477-1499.

197. Julie E. Cohen. Cyberspace As/And Space. *Columbia Law Review*. 2007. Vol. 107. № 1. pp. 210–256.

198. Kesari A. Deterring Cybercrime: Focus on Intermediaries. *Berkeley Technology Law Journal*. 2017. Vol. 32. pp. 1093-1133.

199. Laurent Sacharoff. Criminal Trespass and Computer Crime. *William & Mary Law Review*. 2020. Vol. 62, pp. 571–647.

200. Lawrence Lessig. The Zones of Cyberspace. *Stanford Law Review*. 1996. Vol. 48, pp. 1403–1411.

201. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

202. Neal K. Katyal. Criminal Law in Cyberspace. *University of Pennsylvania Law Review*. 2001.Vol. 149. pp. 1003-1114.

203. Orin S. Kerr. Cybercrime's Scope: Interpreting «Access» and «Authorization» in Computer Misuse Statutes. *New York University Law Review*. 2003. Vol. 78. Number 5. pp.1596 -1668.

204. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng

205. Susan W. Brenner & Joseph J. Schwerha IV. Transnational Evidence Gathering and Local Prosecution of International Cybercrime. *The John Marshall Journal of Computer & Information Law*. 2002.Vol. 20. Issue 3. pp. 347-396.

ДОДАТКИ

Додаток 1

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Філімонов М.В. Окремі питання призначення експертизи електронних комунікацій під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. *Правові новели*. 2024. № 24. С. 347-355. URL: http://legalnovels.in.ua/journal/24_2024/48.pdf

2. Філімонов М.В. До питання щодо стану наукової розробленості проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі у юридичній доктрині. *Право і суспільство*. 2024. №6. С. 340-345. URL: http://pravoisuspilstvo.org.ua/archive/2024/6_2024/51.pdf

3. Філімонов М.В. Міжнародні стандарти та зарубіжний досвід нормативної регламентації розслідування кримінальних правопорушень, вчинених у кіберпросторі. *Право і суспільство*. 2025. №3. Т. 2. С. 657-662. URL: http://pravoisuspilstvo.org.ua/archive/2025/3_2025/part_2/91.pdf

4. Філімонов М.В. Питання забезпечення права особи на повагу до приватного життя у кіберпросторі в практиці Європейського суду з прав людини. *Юридичний науковий електронний журнал*. 2025. № 4. С. 632-634. URL: http://lsej.org.ua/4_2025/155.pdf

5. Філімонов М.В. Належний процесуальний порядок ознайомлення із інформацією, що міститься на цифрових пристроях: окремі питання у контексті практики ККС ВС. *Правові новели*. 2025. № 25. С.456-461. URL: http://legalnovels.in.ua/journal/25_2025/60.pdf

наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Філімонов М.В. Використання цифрової інформації з відкритих джерел у кримінальному процесуальному доказуванні: постановка проблеми. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень* : у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 трав. 2023 р.) / за загальною редакцією С.В. Ківалова. Одеса: Видавництво «Юридика». 2023. Т. 2. С. 377-380.

2. Філімонов М.В. Втручання в електронне приватне спілкування у практиці європейського суду з прав людини: окремі питання. *Актуальні питання розвитку юридичної науки в період воєнного стану* : Міжнародна науково-практична конференція. Науково-дослідний інститут публічного права, 17 травня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 358-360. DOI https://doi.org/10.36059/978-966-397-395-1-105.

3. Філімонов М.В. Допустимість доказів, отриманих із веб-сайтів та інтернет-ресурсів: проблеми, доктрини та тенденції судової практики. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів*: матеріали Міжнар.наук.-практ. конф. (м. Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 463-465.

4. Філімонов М.В. Окремі питання допустимості доказів, отриманих у результаті зняття інформації з електронних інформаційних систем. *Європейські орієнтири України: нові виміри у воєнний час* : матеріали міжнар.наук.- практ. конф. (м. Одеса, 16 травня 2025 р.). Одеса, 2025. С. 639-641.

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

Положення та висновки дисертаційного дослідження обговорювались під час засідання кафедри кримінального процесу Національного університету «Одеська юридична академія». Основні результати наукового дослідження були висвітлені у доповідях на наукових, науково-практичних конференціях, зокрема на: Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень» (м. Одеса, 19 травня 2023 р.) – форма участі заочна; Міжнародній науково-практичній конференції «Актуальні питання розвитку юридичної науки в період воєнного стану» (м. Львів, 17 травня 2024 р.) – форма участі заочна; Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.) – форма участі заочна; Міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: нові виміри у воєнний час» (м. Одеса, 16 травня 2025 р.) – форма участі заочна.

Додаток 2

Пропозиції щодо внесення змін і доповнень до Кримінального процесуального кодексу України

1. Доповнити КПК України ст. 88^2 під назвою «Допустимість доказів, отриманих із відкритих джерел» та викласти її у такій редакції:

«Докази, отримані із відкритих джерел можуть бути визнані допустимими виключно за умови підтвердження джерела їх походження та якщо відповідні відомості підтверджуються іншими доказами, які визнані допустимими за правилами цього Кодексу».

2. Частину 4 ст. 163 КПК України доповнити абзацом другим і викласти його у такій редакції:

«Клопотання слідчого, прокурора про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо розглядається слідчим суддею у день його надходження».

3. Статтю 165 КПК України доповнити ч. 5 та викласти її у такій редакції:

«Ухвала слідчого судді про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо підлягає негайному виконанню».

4. Доповнити ч.2 ст. 237 КПК України абз. третім такого змісту:

«Під час огляду житла чи іншого володіння особи виявлення та фіксація комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення огляду можлива лише за добровільною згодою володільця цього майна або якщо дозвіл на такий огляд був наданий в ухвалі слідчого судді».

5. Абзац другий ч.6 ст. 236 КПК України у такій редакції:

«Прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення обшуку виключно якщо дозвіл на такий пошук наданий в ухвалі слідчого судді».

6. Частину 6 ст. 244 КПК України другим абзацом та викласти його у такій редакції:

«Слідчий суддя не може відмовити у задоволенні клопотання про залучення експерта з тих підстав, що сторона захисту не зверталась попередньо із відповідним клопотанням до слідчого, прокурора».

Додаток 3

Акт впровадження

ЗАТВЕРДЖУЮ
Ректор
Національного університету
«Одеська юридична академія»
професор

Олег ТОДОЩАК

«19» січня 2026 р.

АКТ
впровадження в освітній процес
Національного університету «Одеська юридична академія»
результатів дисертаційного дослідження

«19» січня 2026 року м. Одеса

Філімонова Микити Володимировича
«Особливості доказування при здійсненні
досудового розслідування кримінальних правопорушень,
вчинених у кіберпросторі»
на здобуття ступеня доктора філософії
за спеціальністю 081 «Право»

Комісія у складі:

1) начальника навчально-методичного відділу Національного університету «Одеська юридична академія» Кузнецової Л.В.

2) завідувача кафедри кримінального процесу Національного університету «Одеська юридична академія», доктора юридичних наук, професора Торбаса О.О.

3) завідувача кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія», доктора юридичних наук, професора Аркуші Л.І.

4) доцента кафедри кримінального процесу Національного університету «Одеська юридична академія», кандидата юридичних наук, доцента Завтура В.А.,

склала цей акт з приводу того, що комісією розглянуто матеріали дисертаційного дослідження здобувача ступеня доктора філософії за спеціальністю 081 «Право» НУ «ОЮА» Філімонова Микити Володимировича на тему: «Особливості доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі», які, зокрема, відображені у наукових публікаціях:

1. Філімонов М.В. Окремі питання призначення експертизи електронних комунікацій під час досудового розслідування кримінальних правопорушень,

вчинених у кіберпросторі. Правові новели. 2024. № 24. С. 347-355. URL: http://legalnovels.in.ua/journal/24_2024/48.pdf

2. Філімонов М.В. До питання щодо стану наукової розробленості проблем розслідування кримінальних правопорушень, вчинених у кіберпросторі у юридичній доктрині. Право і суспільство. 2024. №6. С. 340-345. URL: http://pravoisuspilstvo.org.ua/archive/2024/6_2024/51.pdf

3. Філімонов М.В. Міжнародні стандарти та зарубіжний досвід нормативної регламентації розслідування кримінальних правопорушень, вчинених у кіберпросторі. Право і суспільство. 2025. №3. Т. 2. С. 657-662. URL: http://pravoisuspilstvo.org.ua/archive/2025/3_2025/part_2/91.pdf

4. Філімонов М.В. Питання забезпечення права особи на повагу до приватного життя у кіберпросторі в практиці Європейського суду з прав людини. Юридичний науковий електронний журнал. 2025. № 4. С. 632-634. URL: http://lsej.org.ua/4_2025/155.pdf

5. Філімонов М.В. Належний процесуальний порядок ознайомлення із інформацією, що міститься на цифрових пристроях: окремі питання у контексті практики ККС ВС. Правові новели. 2025. № 25. С.456-461. URL: http://legalnovels.in.ua/journal/25_2025/60.pdf

6. Філімонов М.В. Використання цифрової інформації з відкритих джерел у кримінальному процесуальному доказуванні: постановка проблеми. Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 трав. 2023 р.) / за загальною редакцією С.В. Ківалова. Одеса: Видавництво «Юридика». 2023. Т. 2. С. 377-380.

7. Філімонов М.В. Втручання в електронне приватне спілкування у практиці європейського суду з прав людини: окремі питання. Актуальні питання розвитку юридичної науки в період воєнного стану : Міжнародна науково-практична конференція. Науково-дослідний інститут публічного права, 17 травня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 358-360. DOI https://doi.org/10.36059/978-966-397-395-1-105.

8. Філімонов М.В. Допустимість доказів, отриманих із веб-сайтів та інтернет-ресурсів: проблеми, доктрини та тенденції судової практики. Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів: матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2024. С. 463-465.

9. Філімонов М.В. Окремі питання допустимості доказів, отриманих у результаті зняття інформації з електронних інформаційних систем. Європейські орієнтири України: нові виміри у воєнний час: матеріали міжнар.наук.- практ. конф. (Одеса, 16 травня 2025 р.). Одеса, 2025. С. 639-641.

Комісія вважає, що представлені матеріали, отримані на основі проведеного самостійного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, можуть бути використані в освітньому процесі Національного університету «Одеська юридична академія», зокрема, під час викладання навчальних дисциплін

«Кримінальний процес», «Сучасні проблеми кримінально-процесуального права», «Проведення слідчих (розшукових) дій», «Оперативно-розшукові заходи та негласні слідчі (розшукові) дії», «Забезпечення законності проведення оперативно-розшукових заходів та слідчих (розшукових) дій».

Члени комісії: **Людмила КУЗНЕЦОВА**

Олександр ТОРБАС

Лариса АРКУША

Віктор ЗАВТУР