ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

РАТНОВА АЛІНА ВОЛОДИМИРІВНА

УДК 343.140.01

ДИСЕРТАЦІЯ

КРИМІНАЛЬНІ ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ ОСНОВИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У ДОКАЗУВАННІ

081 – Право

Подається на здобуття ступеня доктора філософії

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

Науковий керівник – **Хитра Андрій Ярославович**, кандидат юридичних наук, доцент

Львів – 2021

АНОТАЦІЯ

Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. – Львівський державний університет внутрішніх справ, Львів, 2021.

Дисертацію присвячено дослідженню кримінального процесуального та криміналістичного порядку використання електронних документів під час доказування у кримінальному провадженні. З урахуванням загальної теорії доказування, міжнародного досвіду, узагальнення та аналізу судової практики розроблено основи використання електронних документів у доказуванні.

Висвітлення обраної тематики дослідження передбачає аналіз стану наукового розроблення, визначення поняття та місця електронного документа у системі джерел доказів, проведення класифікації електронних документів, розгляд критеріїв оцінки електронних документів, окреслення способів отримання та дослідження електронних документів, а також аналіз досвіду використання електронних документів у доказуванні.

У роботі сформульовано низку положень, висновків і рекомендацій, що характеризуються науковою новизною. Проведено аналіз нормативно-правових актів, які регулюють використання електронних доказів у інших галузях права, досліджено літературні джерела у галузі кримінального процесу, криміналістики з питань використання та дослідження електронних документів. Наукову розвідку здійснено на підставі загальнонаукових та спеціально-наукових методів.

Зроблено висновок про те, що не існує єдиного визначення поняття «електронного документа» у кримінальній процесуальній науці, яке станом на сьогодні також і відсутнє у Кримінальному процесуальному кодексі України. Однак, більшою проблемою є відсутність єдиного підходу до сутності та місця електронних документів у системі доказів під час здійснення слідчої та судової практики. Встановлено, що основними особливостями електронних документів є

наявність метаданих, електронна форма та необхідність візуалізації електронних документів за допомогою спеціального обладнання та програм. Запропоновано авторське визначення «електронного документа» та «метаданих». Обґрунтовано віднесення електронних документів до самостійного джерела доказів у Кримінальному процесуальному кодексі.

Проведено поділ електронних документів з точки зору використання як доказу, на дві групи юридичні та технічні. Класифіковано електронні документи за стадіями виготовлення, за комбінацією метаданих, в залежності від доступу до метаданих, за ступенем захисту, за джерелом походження, за їх місцем розташування, за формою.

Встановлено, що зміст електронних документів може підтверджувати чи спростовувати загальний предмет доказування, доказовий чи допоміжний факт. Проаналізовано судові рішення та зроблено висновок про те, що електронні документи можуть доводити подію кримінального правопорушення, мотив, мету, роль учасників кримінального правопорушення, встановлювати вид і розмір завданої шкоди, тощо. За допомогою електронних документів можуть бути висунені та перевірені різні слідчі версії. З'ясовано, що визнання судом електронних документів неналежними доказами може бути пов'язане з неможливістю встановлення взаємозв'язку даних документів з предметом доказування та порушенням вимог допустимості доказів.

Звернено увагу на необхідність дослідження електронних документів з точки зору їх допустимості за чотирма основними елементами: належний суб'єкт збирання доказу; належний спосіб збирання доказу; належне джерело отримання доказу; належна форма закріплення відомостей про факти. Наголошено на необхідності правильного розмежування слідчих (розшукових) дій та заходів забезпечення кримінального провадження залежно від ступеня втручання у права та свободи громадян та можливостей отримання електронних документів як доказів.

Оцінка електронних документів на достовірність здійснюється суб'єктами доказування шляхом його зіставлення з іншими доказами у кримінальному

провадженні. Встановлення достовірності електронних документів як джерел доказів може полягати у з'ясуванні технічної справності носія технічної інформації, встановленні інформації про власника вебсайту, облікового запису у соціальній мережі, установлення місцезнаходження технічного пристрою у період, який становить інтерес, тощо.

Встановлення достатності доказів стосується усієї зібраної сукупності доказів та залежить від наявності обов'язкових джерел доказів та доказів під час розслідування тих чи інших кримінальних правопорушень. Оцінка сукупності доказів з точки зору достатності здійснюється усіма суб'єктами доказування на підставі внутрішнього переконання.

Аргументовано, що збирання доказів, джерелом яких є електронні документи, за своїм змістом полягає у виявленні і закріпленні (фіксації) його матеріально-технічного носія. Враховуючи двоєдину форму електронних документів, в першу чергу слід отримати його фізичну (матеріальну) частину, або доступ до хмарного сховища, серверу, Інтернету, що і є збиранням доказів у такому випадку. До основних способів збирання електронних документів стороною обвинувачення відносимо надання добровільно учасником кримінального провадження (отримання); витребування доказів; тимчасовий доступ до речей та документів (як захід забезпечення), проведення слідчих (розшукових) дій (огляд; обшук) та негласних слідчих (розшукових) дій. Сторона захисту збирає електронні документи шляхом витребування та отримання доказів, ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів. Вважаємо, що сторона обвинувачення має суттєві переваги щодо сторони захисту у збиранні доказів, у тому числі електронних документів.

Аргументовано, що дослідження електронних документів може здійснюватися під час проведення наступних експертиз: семантико-текстуальна, лінгвістична, фототехнічна, портретна, комп'ютерно-технічна, апаратно-

комп'ютерна, комп'ютерно-мережева. Встановлено, що слід запровадити такий вид експертного дослідження, як експертиза електронних документів.

Проведено аналіз міжнародного досвіду використання електронних документів у процесі доказування. Констатовано, що незважаючи на відсутність визначення електронних документів у законодавстві багатьох країн Європи, міжнародні організації працюють над введенням та запровадженням єдиних правил для збору, збереження та використання електронних документів, розроблення методик та поширення кращих практик під час роботи з електронними документами. Такі рекомендації використовуються не тільки в межах транскордонного співробітництва, але і для всіх інших видів правопорушень, у яких електронні документи виступають доказами. Поступово здійснюється гармонізація законодавства держав Європи відповідно до міжнародних вимог щодо електронних документів.

Одержані в дисертації наукові результати дають підстави для формулювання висновків і рекомендацій, що мають теоретичне і практичне значення.

Ключові слова: доказ, доказування, електронний документ, електронний доказ, цифровий доказ, джерела доказів, досудове розслідування, слідча (розшукова) дія.

SUMMARY

Ratnova A.V. Criminal procedural and criminalistics fundamentals of the use of electronic documents exchange in proof of evidence. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 081 Law. – Lviv State University of Internal Affairs, Lviv, 2021.

The dissertation is dedicated to the study of criminal procedural and criminalistics procedures of the use of electronic documents exchange in proof of evidence. Considering the general theory of proof, international experience,

generalization, and analysis of judicial practice, the fundamentals of the use of electronic documents exchange in proof of evidence have been developed.

Coverage of the topic under study involves analysis of the state of scientific development, defining the concept and place of an electronic document in the system of sources of evidence, classification of electronic documents, consideration of criteria for evaluation of electronic documents, outlining ways to obtain and research electronic documents, as well as analysis of experience in the use of electronic documents in evidence.

The paper formulates a number of provisions, conclusions and recommendations that are characterized by scientific novelty. Normative legal acts regulating the use of electronic evidence in other branches of law were analysed, the literary sources in the field of criminal procedure and criminology on the use and research of electronic documents were studied. Scientific research was based on both general and special scientific methods.

It was concluded that there is a problem of the lack of a unified definition of the concept of «electronic document», which is currently absent in the Code of Criminal Procedure. However, a bigger problem is the lack of a unified approach to the nature and place of electronic documents in the evidence system during investigative and judicial practice. It was established that the main features of electronic documents included the presence of metadata, electronic form of the document, and the need to use special equipment and programs in order to visualize electronic documents. The author's definition of «electronic document» and «metadata» was offered. Consideration of electronic documents as an independent source of evidence in the Code of Criminal Procedure was justified.

The electronic documents in terms of their use as evidence were divided into two groups: legal and technical. Electronic documents were classified by stages of production, by combination of metadata, depending on access to metadata, by degree of protection, by source of origin, by their location, and by form.

It was established that the content of electronic documents can confirm or refute the general subject of proof, evidentiary or auxiliary fact. On the basis of court decisions

analysis, it was concluded that electronic documents can prove the event of a criminal offense, motive, purpose, role of participants in a criminal offense, establish the type and amount of damage, etc. Various investigative versions can be put forward and verified with the help of electronic documents. It was found that the recognition of electronic documents as inadequate evidence by court may be caused by the impossibility of establishing the relation of these documents to the subject of evidence and violation of the requirements for the admissibility of evidence.

Attention was paid to the need to study electronic documents in terms of their admissibility according to four main elements: the proper subject of evidence collection; proper method of gathering evidence; appropriate source of evidence; proper form of consolidation of information about the facts. Emphasis was placed on the need to properly distinguish between investigative actions and measures to ensure criminal proceedings depending on the degree of their interference with the rights and freedoms of citizens and the possibility of obtaining electronic documents as evidence.

Checking of electronic documents for authenticity is carried out by the subjects of evidence by comparing it with other evidence in criminal proceedings. Establishing the authenticity of electronic documents as sources of evidence may include ascertaining the technical serviceability of the technical information carrier, establishing information about the website or social network account owner, locating the technical device during the period of interest, etc.

Establishing the sufficiency of evidence applies to the entire body of evidence collected and depends on the availability of mandatory sources of evidence as well as evidence in the investigation of certain criminal offenses. The assessment of the totality of evidence from the point of view of their sufficiency is carried out by all subjects of evidence on the basis of internal conviction.

It is argued that the collection of evidence, the source of which is electronic documents, involves identifying and securing its material and technical carrier. Given the dual form of electronic documents, you should first get its physical (material) part, or access to cloud storage, server, Internet, which is the collection of evidence in this case. The main methods of collecting electronic documents by the prosecution include

voluntarily provision of the documents by a participant in criminal proceedings (receiving); request for evidence; temporary access to things and documents (as a security measure), conduction of investigative actions (inspection; search) and covert investigative actions. The defense collects electronic documents by means of requesting and obtaining evidence, initiating investigative actions, covert investigative actions and other procedural actions, performing other actions that can ensure the submission of appropriate and admissible evidence to the court. We believe that the prosecution has significant advantages over the defense in collecting evidence, including electronic documents.

The study of electronic documents can be carried out during the following examinations: semantic-textual, linguistic, photo technical, portrait, computer-technical, and computer-network examination. It was established that such type of expert research as the examination of electronic documents should be introduced.

The analysis of the international experience of using electronic documents in proof of evidence was carried out. It was stated that despite the lack of definition of electronic documents in the legislation of many European countries, international organizations are working to introduce and implement unified rules for the collection, storage and use of electronic documents, development of methods and dissemination of best practices when working with electronic documents. Such recommendations are used not only in the framework of cross-border cooperation, but also for all other types of offenses in which electronic documents can serve as evidence. Gradually, the legislation of European countries is being aligned in accordance with international requirements for electronic documents.

The scientific results obtained in the dissertation provide grounds for formulating conclusions and recommendations that have theoretical and practical significance.

Keywords: proof, evidence, electronic document, electronic evidence, digital evidence, sources of evidence, pre-trial investigation, investigative action.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Ратнова А.В. Проведення огляду облікового запису користувача в соціальній мережі під час досудового розслідування кримінального провадження. *Науково-практичний журнал «Прикарпатський юридичний вісник»*. 2020. Випуск №3 (32). С. 97-102 *(стаття в науковому виданні, включеному до переліку наукових фахових видань України з присвоєнням категорії «Б»)*.

2. Ratnova A. The state of scientific development of an electronic document as evidence in criminal proceedings. *Visegrad Journal on Human Rights*. 2020. № 5. P. 210-214 *(стаття в періодичному науковому виданні іншої держави, яка входить до Організації економічного співробітництва та розвитку і Європейського Союзу)*.

3. Ратнова А.В. Класифікація електронних документів, як джерел доказів, у кримінальному провадженні. *Журнал східноєвропейського права.* 2021. №84. С. 42-47 *(стаття в науковому виданні, включеному до переліку наукових фахових видань України з присвоєнням категорії «Б»)*.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4. Ратнова А.В. Електронний документ як джерело доказу у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування:* збірник тез науково-практичного семінару (01 груд. 2017 р.) / упор. А.Я. Хитра, Р.М. Шехавцов, Є.В. Пряхін, С.І. Марко. Львів: ЛьвДУВС. 2017. С. 90-94.

5. Ратнова А.В. Використання даних геолокації під час доказування у кримінальному провадженні. *Механізм правового регулювання правоохоронної та правозахисної діяльності в умовах формування громадянського суспільства (осінні читання)*: збірник тез Всеукраїнської наукової конференції здобувачів вищої освіти (23 лист. 2018 р.) / упор. Л.В. Павлик. Львів: ЛьвДУВС, 2018. С. 351-354.

6. Ратнова А.В. Використання метаданих під час проведення експертизи електронного документа у кримінальному провадженні. *Процесуальне та*

криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 лист. 2018 р.) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2018. С. 81-83.

7. Ratnova A. Legal admissibility of electronic documents as evidence in Ukraine. *Право. Комунікація. Суспільство. Law. Communication. Society. Das recht. Die kommunikation. Das geselschaft. Le droit. La communication. La société*: матеріали науково-практичної конференції здобувачів вищої освіти (українською та іноземними мовами) (12 квіт. 2019 р.) / за заг. ред. канд. філол. наук, доц. І.Ю. Сковронської. Львів: ЛьвДУВС. 2019. С. 117-119.

8. Ратнова А.В. Використання роздруківки та скріншоту інтернет-сторінки під час доказування у кримінальному провадженні. *Кримінальне процесуальне та криміналістичне забезпечення досудового розслідування*: матеріали науково-практичного семінару (25 жовт. 2019 р.) / упор. Р. М. Шехавцов. Львів: ЛьвДУВС. 2019. С. 92-95.

9. Ратнова А.В. Електронні документи як докази під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків. *Процесуальне та криміналістичне забезпечення досудового розслідування:* тези доповідей учасників науково-практичного семінару (30 жовт. 2020 р.) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2020. С. 81-83.

Наукові праці, які додатково відображають наукові результати дисертації:

10. Ратнова А.В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2018. Вип. 3. С. 231-241.

11. Ратнова А.В. Допустимість електронних документів у кримінальному провадженні на етапі збирання доказів. *Sciences of Europe.* 2019. VOL 4. № 44. С. 37-42.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ГПК	–	Господарський процесуальний кодекс України
ГУНП	–	Головне управління Національної поліції
ДНДЕКЦ	–	Державний науково-дослідний експертно-криміналістичний центр
ДНР	–	Донецька народна республіка
ДСТУ	–	Державний стандарт України
ЕОМ	–	Електронно-обчислювальна машина
Європол	–	Європейське поліцейське управління
ЄРДР	–	Єдиний реєстр досудових розслідувань
ЄС	–	Європейський союз
ЄСПЛ	–	Європейський суд з прав людини
ІТ	–	Інформаційні технології
КАС	–	Кодекс адміністративного судочинства України
КК	–	Кримінальний кодекс України
КМУ	–	Кабінет Міністрів України
КПК	–	Кримінальний процесуальний кодекс України
КпАП	–	Кодекс України про адміністративні правопорушення
МВС	–	Міністерство внутрішніх справ
млн	–	мільйон
млрд	–	мільярд
НДЕКЦ	–	Науково-дослідний експертно-криміналістичний центр
ООН	–	Організація Об’єднаних Націй
СУ	–	Слідче управління
ЦПК	–	Цивільний процесуальний кодекс України

ВСТУП

Обґрунтування вибору теми дослідження. Дії практично кожної особи повсякденно фіксуються в електронному вигляді. Використання мобільних телефонів, комп'ютерів та Інтернету дають можливість спілкуватись та передавати інформацію між фізичними та юридичними особами незважаючи на часові пояси та державні кордони. Легкість користування електронними пристроями сприяє також вчиненню кримінальних правопорушень з їх використанням.

Згідно з даними звіту «DIGITAL 2021: Global Digital Overview» (в перекладі з англ. «Цифровий 2021: Глобальний цифровий огляд»), який проведений за участі «DataReportal» спільно з компаніями «We Are Social» і «Hootsuite» кількість осіб, які користуються Інтернетом, соціальними мережами невпинно зростає. Зокрема, станом на січень 2021 року 4,66 млрд людей у всьому світі користуються Інтернетом, що на 316 млн (+7,3%) більше, ніж у січні минулого року (4,54 млрд осіб), а активних користувачів соціальних мереж стало 4,20 млрд осіб, тобто їх кількість зросла на 13%, або на 490 млн у порівнянні з січнем 2020 року (+3,8 млрд осіб). Загалом кількість користувачів соціальних мереж зросла більше ніж удвічі у порівнянні з січнем 2016 року (+2,31 млрд осіб) [6].

Зростаюча глобалізація та розвиток сучасних технологій призводить до того, що електронні документи можуть бути розміщені або збережені в будь-якій точці світу. Особливо, це стосується випадків кіберзлочинності, оскільки кіберзлочинність є проблемою транскордонного співробітництва. Однак, все частіше електронні документи стосуються усіх видів кримінальних правопорушень. Отже, недостатньо сказати, що електронні документи мають значення лише у провадженнях про кіберзлочини.

Згідно зі звітом Департаменту кіберполіції Національної поліції України, протягом 2020 року кримінальні правопорушення були виявлені у таких сферах: обігу протиправного контенту і телекомунікацій (ст. ст. 176, 229, ч. 3, 4, 5 ст. 301 КК) – 235, що на 72 кримінальні правопорушення більше ніж у 2019 році

(163); у банківській (ст. ст. 185, 200, 231, 362 КК) – 1079, що на 378 кримінальних правопорушень більше ніж у 2019 році (701); онлайн шахрайств (ч. 3, 4 ст. 190 КК) – 822, що у два рази більше ніж за попередній рік (354); комп'ютерних систем (ст.ст. 361, 361-1, 361-2, 363, 363-1 КК) – 737, що на 116 кримінальних правопорушень більше ніж у 2019 році (621) (додаток Б).

У 2017 році до ЦПК, ГПК та КАС внесено зміни, серед яких «електронні докази» віднесено до засобів доказування. Аналогічних змін до КПК здійснено не було, що спричиняє неоднакове розуміння електронних документів як на досудовому, так і на судовому етапі кримінального провадження.

У зв'язку з необхідністю роботи з електронними документами практично у більшості кримінальних проваджень нагальними стають розроблення єдиних правил роботи з таким видом доказів, підготовка криміналістичних рекомендацій для практичних працівників. Під час роботи з електронними документами суб'єкти доказування повинні знати особливості електронних документів, вміти вилучати електронні документи без пошкодження та зміни інформації, володіти ґрунтовними знаннями щодо тактики проведення окремих слідчих (розшукових) та інших процесуальних дій, спрямованих на збирання та дослідження електронних документів.

Актуальність даного дослідження також пов'язане з тим, що відсутнє законодавче та наукове визначення електронних документів у кримінальному провадженні, його обов'язкові реквізити та місце у системі доказів.

Питання використання електронних документів у доказуванні в адміністративному, господарському та цивільному процесі досліджували О.І. Антонюк, А.Т. Боннер, І.В. Булгакова, Н.Ю. Голубєва, І.І. Демчишин, К.Б. Дрогозюк, О.П. Євсеєв, І.В. Казачук, А.Ю. Каламайко, О.М. Лазько, Е.М. Мурадьян, Ю.С. Павлова, О.О. Присяжнюк, І.В. Решетнікова, М.С. Строгович, Н.О. Чечина, О.С. Чорний, К.С. Юдельсон та інші науковці.

Під час дослідження особливостей розслідування комп'ютерних злочинів, злочинів вчинених у кіберпросторі частково розглянуто питання електронного документа у роботах Г.С. Бідняка, В.А. Динту, О.О. Загуменного,

С.П. Кушніренко, Д.О. Максимуса, В.А. Мещерякова, О.І. Мотляха, О.А. Самойленко, С.С. Чернявського, Є.С. Шевченка, О.О. Юхна.

До теми електронних документів у кримінальному процесі та криміналістиці звертались Н.М. Ахтирська, Є.П. Бєгалов, С.Й. Гонгало, М.І. Демура, І.В. Єна, Д.І. Клепка, А.В. Коваленко, С.О. Ковальчук, І.О. Крицька, Т.Е. Кукарникова, Д.О. Літкевич, О.П. Метелев, В.В. Мурадов, Ю.Ю. Орлов, А.О. Просняк, М.В. Салтевський, А.В. Скрипник, С.М. Стахівський, А.В. Столітній, Є.С. Хижняк, Д.М. Цехан, Г.Л. Чигрина, О.В. Шведова, А.В. Шило.

Зростання потреби здійснення комплексного монографічного дослідження електронних документів у кримінальному провадженні обумовило вибір теми дисертації.

Зв'язок роботи з науковими програмами, планами, темами.

Дослідження проведено згідно з Тематикою наукових досліджень і науково-технічних розробок на 2020-2024 роки, затвердженого наказом Міністерства внутрішніх справ України №454 від 11.06.2020 р. та відповідно до Плану науково-дослідної роботи Львівського державного університету внутрішніх справ (у межах теми «Протидія злочинам, підслідним Національній поліції: правові, кримінологічні та криміналістичні аспекти», номер державної реєстрації 0118U005374). Тема дисертаційного дослідження відповідає науковому напрямку кафедри кримінального процесу та кафедри криміналістики факультету №1 Львівського державного університету внутрішніх справ. Тему дисертації затверджено Вченою радою Львівського державного університету внутрішніх справ 31.10.2017 року (протокол №3).

Мета і завдання дослідження. Основною метою дослідження є визначення основних засад використання електронних документів під час доказування у кримінальному провадженні.

Для досягнення цієї мети було поставлено такі основні завдання:

- визначити стан наукової розробленості використання електронних документів у кримінальному провадженні та напрями подальших досліджень в Україні;

- з’ясувати поняття «електронного документа» як джерела доказів у кримінальному провадженні та його місце в системі джерел доказів;

- здійснити класифікацію електронних документів, з урахуванням їх значення для доказування у кримінальному провадженні ;

- визначити особливості оцінки електронних документів у кримінальному провадженні на предмет їх належності, допустимості, достатності та достовірності;

- сформулювати особливості тактики отримання електронних документів у кримінальному провадженні;

- розглянути види досліджень електронних документів та охарактеризувати особливості їх проведення;

- з’ясувати міжнародний досвід використання електронних документів під час доказування та перспективи його застосування в Україні;

- сформулювати пропозиції щодо внесення відповідних змін до нормативно-правових актів та створення єдиної практики її застосування.

Об’єктом дослідження є кримінальні процесуальні суспільні відносини між учасниками кримінального провадження, котрі виникають під час використання електронних документів у доказуванні.

Предметом дослідження є кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні.

Методологічна основа проведення дослідження. Методологічною основою дослідження є система загальнонаукових та спеціальних наукових методів і підходів, що забезпечить об’єктивний аналіз досліджуваного предмета. З урахуванням специфіки теми, мети та завдань дослідження використовувалася низка методів: *історично-правовий метод* застосовано під час дослідження стану наукової розробленості електронних документів в Україні та закордоном (підрозділи 1.1, 3.3); *діалектичний метод* дозволив розглянути всі питання в

динаміці, виявити їх взаємозв'язок і взаємозумовленість, сприяв розумінню об'єкта дослідження щодо поєднання потреб наукової та практичної діяльності органів досудового розслідування та суду (підрозділи 2.1, 2.2, 2.3, 3.2); *системно-структурний метод* застосовувався при визначенні основних реквізитів електронних документів, проведенні класифікації електронних документів, для дослідження проблем, пов'язаних із процесуальним порядком доказування; при розробці тактики проведення окремих слідчих (розшукових) дій та інших процесуальних дій під час роботи з електронними документами (підрозділи 1.2, 1.3, 3.1); *порівняльно-правовий метод* сприяв зіставленню норм нормативно-підзаконних актів, що дало можливість сформулювати конкретні пропозиції для вдосконалення КПК (підрозділи 1.1, 1.2, 1.3., 2.2., 3.1); *формально-логічні методи* застосовувалися для обґрунтування висновків і пропозицій щодо доповнення чи уточнення норм КПК (підрозділи 1.2., 1.3, 2.2, 3.1); *статистичні методи* використовувалися у процесі вивчення й узагальнення слідчої та судової практики, формування і обґрунтування висновків за їх результатами (підрозділи 1.1, 1.3, 2.1). *Соціологічний метод* анкетування застосовано для складення питань та одержання відповідей на них від респондентів, а статистичне зведення – для узагальнення результатів опитування (підрозділи 1.1, 1.3, 3.1).

Емпіричну базу дослідження становлять дані офіційної статистики Офісу Генерального прокурора; статистичні дані роботи Департаменту боротьби з наркозлочинністю та Департаменту кіберполіції Національної поліції України за 2017-2020 рр.; судові рішення, внесені до Єдиного реєстру судових рішень України (опрацьовано 248 рішень, ухвал та вироків); рішення Європейського суду з прав людини; національне законодавство України та окремих закордонних держав; зведені дані анкетування 207 слідчих та оперативних працівників підрозділів Національної поліції України.

Під час підготовки дисертації використано досвід роботи дисертанта в органах досудового розслідування, зокрема на посаді слідчого Калуського ВП ГУНП України в Івано-Франківській області.

Наукова новизна отриманих результатів полягає в тому, що здійснене дослідження електронних документів у кримінальному провадженні є одним із перших в Україні, у якому на монографічному рівні сформульовано низку наукових положень, висновків і рекомендацій щодо основ кримінального процесуального та криміналістичного використання електронних документів. До найвагоміших результатів, які відображають концептуально нові наукові положення та висновки й мають важливе теоретичне і практичне значення, належать такі:

вперше:

- запропоновано критерії допустимості, належності та достовірності електронних документів з урахуванням їх особливостей;
- розглянуто особливості збирання електронних документів суб'єктами доказування;

удосконалено:

- наукове визначення поняття електронних документів;
- обґрунтування необхідності віднесення електронних документів до окремого джерела доказів;
- класифікацію електронних документів за основними критеріями;
- тактику проведення окремих слідчих (розшукових) дій з метою збирання електронних документів суб'єктами доказування;

дістало подальший розвиток:

- визначення стану наукової розробленості електронних документів у кримінальному провадженні на підставі здійсненого аналізу монографічних досліджень, навчальної та наукової літератури з кримінального процесуального права та криміналістики;
- розмежування електронних документів за джерелами доказів – документом чи речовим доказом;
- дослідження електронних документів під час проведення експертизи.

Практичне значення очікуваних результатів. Отримані наукові результати наукового дослідження можуть бути використані у: *науково-дослідній*

діяльності – для подальшої розробки та розв'язання питань з використання електронних документів як доказів у кримінальному провадженні; *законодавчій діяльності* – при внесенні змін до КПК та деяких інших підзаконних нормативно-правових актів; *освітньому процесі* – при розробці курсів лекцій, навчально-методичних матеріалів і проведенні занять за відповідними темами з навчальних дисциплін «Кримінальний процес», «Криміналістика», «Теоретичні проблеми кримінального судочинства», «Досудове розслідування», «Дізнання» (акт впровадження Львівського державного університету внутрішніх справ від 25.01.2021 № 10); *практичній діяльності* – під час проведення досудового розслідування слідчими, прокурорами, оперативними працівниками та судами під час судового розгляду (акт впровадження в діяльність СУ ГУНП України у Львівській області від 25.01.2021 №1133).

Особистий внесок здобувача. Теоретичні висновки та результати дисертації отримано на підставі особистих досліджень автора. Дисертацію виконано автором самостійно.

Апробація результатів дисертації. Наукову роботу підготовлено на кафедрі кримінального процесу та криміналістики факультету № 1 Інституту підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ, обговорено на засіданні кафедри, схвалено і рекомендовано до захисту. Окремі положення дисертації оприлюднено на науково-практичних заходах: науково-практичному семінарі «Процесуальне та криміналістичне забезпечення досудового розслідування» (м. Львів, 01 грудня 2017 року), всеукраїнській науковій конференції здобувачів вищої освіти «Механізм правового регулювання правоохоронної та правозахисної діяльності в умовах формування громадянського суспільства (осінні читання)» (м. Львів, 23 листопада 2018 року), науково-практичному семінарі «Процесуальне та криміналістичне забезпечення досудового розслідування» (м. Львів, 30 листопада 2018 року), науково-практичній конференції здобувачів вищої освіти (українською та іноземними мовами) «Право. Комунікація. Суспільство. Law. Communication. Society. Das recht. Die

kommunikation. Das geselschaft. Le droit. La communication. La société» (м. Львів, 12 квітня 2019 року), науково-практичному семінарі «Процесуальне та криміналістичне забезпечення досудового розслідування» (м. Львів, 25 жовтня 2019 року), науково-практичному семінарі «Процесуальне та криміналістичне забезпечення досудового розслідування» (м. Львів, 30 жовтня 2020 року).

Публікації. Основні положення та висновки, наведені у дисертації, викладені й опубліковані у п’ятьох статтях. З них: дві статті опубліковано у наукових виданнях, включених до переліку наукових фахових видань України з присвоєнням категорії «Б», інша – опублікована у періодичному науковому виданні іншої держави, яка входить до Організації економічного співробітництва та розвитку та Європейського Союзу. Опубліковано шість тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з анотації, переліку умовних позначень, вступу, трьох розділів, що об’єднують дев’ять підрозділів, висновків, списку використаних джерел (274 найменування на 29 сторінках) та 5 додатків. Повний обсяг дисертації становить 248 сторінок, із них основний текст – 178 сторінок.

РОЗДІЛ 1
ПОНЯТТЯ, ОЗНАКИ ТА КЛАСИФІКАЦІЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

1.1. Стан розробки наукового дослідження та перспективи подальших досліджень

Постійне використання комп'ютерних технологій призвело до використання інформації в електронному вигляді у всіх сферах людської діяльності.

Створення і поширення електронних документів є швидким способом спілкування, збереження, обміну інформації, замовлення послуг, проведення платежів та інших повсякденних дій. Нормативно-правове забезпечення використання електронних документів впродовж тривалого часу розроблялося і вводилося в дію у різних галузях державного регулювання суспільних відносин. Зокрема, держава дає можливість звертатись до органів державної влади, місцевого самоврядування шляхом надсилання електронних звернень, електронних петицій [172], вчиняти правочини та отримувати прибуток дистанційно з використанням інформаційно-телекомунікаційних систем [170], сплачувати штрафи за допомогою онлайн-сервісу «Дія» та ряд інших послуг, які поступово збільшуються та модернізуються.

Розширення сфери використання комп'ютерних технологій дає можливість спростити та пришвидшити отримання необхідних даних, покращити якість і актуальність опрацьованих даних, доступність інформаційних ресурсів та їх систематизацію. Водночас, збільшується можливість вчинення кримінальних правопорушень з використанням сучасних ІТ. Зокрема, згідно з звітом Департаменту кіберполіції Національної поліції України, протягом 2020 року було виявлено 2873 кримінальні правопорушення у сфері використання високих ІТ, що на 56% більше ніж у 2019 році – 1839 кримінальних правопорушень (додаток Б).

Внаслідок використання комп'ютерної обробки інформації на зміну письмових паперових документів з'явились так звані «безпаперові» документи, які виготовлені комп'ютерами та зберігаються на технічних носіях інформації у пам'яті електронних пристроїв. У зв'язку з цим, документ почали ототожнювати з матеріальним носієм, так як інформація, яка міститься на ньому, піддається однаковим процесам: запис, зберігання та передача, одержання (збирання та пошук) та читання [192, с.307].

Одним з перших нормативно-правових актів в Україні, який був створений з метою встановлення основних організаційно-правових засад електронного документообігу та використання електронних документів в Україні був Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року [169].

З 01 січня 2019 року в Україні набрав чинності державний стандарт 51 ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів». Цей стандарт був прийнятий з метою гармонізації національної нормативної бази з міжнародним законодавством і розроблений методом перекладу тексту з відповідного міжнародного стандарту ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence», що був прийнятий спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) ще у 2012 році.

Рекомендації, що викладені в стандарті, стосуються специфічної діяльності з оброблення потенційних цифрових доказів, а саме процесів: ідентифікації, збирання, здобуття та збереження цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів — прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших інстанціях. Але запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Тому в стандарті зазначається,

що для підтримання цілісності цифрових доказів користувачам цього документу потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних національних законодавчих вимог [58, с.70; 104].

Одним з найважливіших кроків у інституті доказування є прийняття закону України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 03 жовтня 2017 року. Згідно з цим законом, вперше у вищевказаних кодексах визначено поняття «електронного доказу» [164].

Прийняття закону України «Про електронну комерцію», внесення змін до ЦПК, ГПК, КАС та інших нормативно-правових актів, які пов’язані з використанням електронних документів спричинило поштовх до наукових досліджень у цих галузях.

Питання використання електронних документів у ЦПК, ГПК, КАС досліджували О.І. Антонюк, А.Т. Боннер, І.В. Булгакова, Н.Ю. Голубєва, І.І. Демчишин, К.Б. Дрогозюк, О.П. Євсеєв, І.В. Казачук, А.Ю. Каламайко, О.М. Лазько, Е.М. Мурадьян, Ю.С. Павлова, О.О. Присяжнюк, І.В. Решетнікова, М.С. Строгович, Н.О. Чечина, О.С. Чорний, К.С. Юдельсон та інші науковці.

Вказаними вченими обґрунтовано правову природу та особливості практичного застосування електронних документів при здійсненні судочинства. Праці цих науковців в основному стосуються порядку використання електронно-цифрового підпису, дослідженню проблем збирання, оцінки, дослідження електронного доказу, укладення договорів у мережі Інтернет та інших питань. Водночас, практичне використання електронних доказів науковцями майже не досліджувалось [183, с. 233].

Внесення змін до ГПК, ЦПК, КАС хоч і не стосується кримінального процесуального законодавства, однак є суттєвим прогресом для інституту доказування, адже ним вперше проведено поділ засобів доказування на письмові, речові та електронні, визначено що є оригіналом, а що є копією електронного

доказу, порядок зберігання та повернення оригіналів електронних доказів та основне: надано визначення електронного доказу

Проте, порядок збирання, фіксації, дослідження електронних доказів не регламентований, що спричиняє труднощі з їх використання.

Швидка еволюція ІТ спричиняє виникнення прогалин у теорії кримінального процесуального права. Незважаючи на велику кількість інформації та обговорення даної тематики серед учених, питання «електронних доказів» у кримінальному провадженні залишається невирішеним. Серед науковців немає єдиної думки щодо даного явища [159, с. 246].

Одним з перших, хто говорив про можливість використання «електронного документу» як доказу у кримінальних провадженнях, був В.К. Лисиченко. Він зазначав, що поширене використання фото-, відео-, фоно- засобів, які за своєю суттю та значенням відмінні від традиційних документів, а також можливість їх використання у доказуванні повинно позитивно впливати не тільки на практику слідчих і судових органів, але і на розвиток норм процесуального права. У зв'язку з цим, він рекомендує врегулювати питання доказового значення носіїв фактичної інформації, зафіксованої за допомогою таких засобів [138, с. 11-12].

А.Р. Бєлкін зазначив, що широке використання комп'ютерної техніки у різних сферах людської діяльності потребує першочергового вирішення питання про використання в доказуванні документів на безпаперових носіях інформації [39, с. 164-165].

У посібнику з криміналістики М.В. Салтевський писав, що оскільки зараз у сучасному документообігу, в тому числі й при розслідуванні кримінальних правопорушень, дедалі більшу вагу здобувають документи, виконані на сучасних електронно-обчислювальних і механічних друкуючих системах, що також піддаються змінам (підробкам, виправленням), документи в криміналістиці вірніше розуміти в широкому сенсі, як і в кібернетиці, а розділ, що вивчає такі документи, називати криміналістичною документалістикою [191, с.209].

У посібнику «Криміналістична тактика і методика розслідування окремих видів злочинів» звернено увагу на те, електронні докази можуть бути доказами

під час проведення досудового розслідування кримінальних правопорушень проти власності, у сфері обігу наркотичних засобів, у сфері економіки тощо. Для криміналістів також дедалі звичніше стає пошук та аналіз у комп'ютерних системах інформації, яку можна використати як доказ при розгляді кримінального провадження у суді. Науковці надали визначення електронного доказу, звернули увагу на особливість підготовки відповідних фахівців, роз'яснили методологію розслідування злочинів з використанням електронних документів та електронних речових доказів [45, с. 451-452].

Незважаючи на необхідність дослідження електронних документів у кримінальному процесі, про нього лише частково згадується у роботах, пов'язаних з розслідуванням кіберзлочинів. Дослідження кіберпростору в контексті засобів або обстановки вчинення злочинів здійснювалось такими науковцями як В.А. Динту, С.П. Кушніренко, В.А. Мещеряков, О.А. Самойленко, Є.С. Шевченко та іншими криміналістами. Використання сучасних ІТ під час досудового розслідування кіберзлочинів розглянуто у наукових працях О.В. Линника, О.О. Юхно, Д.О. Максимуса, О.О. Загуменного та ін. Вирішенню криміналістичних питань розслідування комп'ютерних злочинів займались науковці Г.С. Бідняк, О.І. Мотлях, С.С. Чернявський.

До теми електронних документів у кримінальному процесі та криміналістиці звертались Н.М. Ахтирська, Є.П. Бєгалов, С.Й. Гонгало, М.І. Демура, І.В. Єна, Д.І. Клепка, А.В. Коваленко, С.О. Ковальчук, І.О. Крицька, Т.Е. Кукарникова, Д.О. Літкевич, О.П. Метелев, В.В. Мурадов, Ю.Ю. Орлов, А.О. Просняк, М.В. Салтевський, А.В. Скрипник, С.М. Стахівський, А.В. Столітній, Є.С. Хижняк, Д.М. Цехан, Г.Л. Чигрина, О.В. Шведова, А.В. Шило.

У дисертації «Електронний документ в кримінальному процесі та криміналістиці», яка проведена за Кримінально-процесуальним кодексом Російської Федерації та опублікована у 2003 році, Т.Е. Кукарникова вперше розглянула «електронний документ» як різновид доказу у кримінальному процесі [136].

Г.Л. Чигрина у своїй роботі зазначила, що «електронний документ» доцільно використовувати як джерело доказу тоді, коли у ньому наявна інформація, яка має значення для правильного вирішення провадження. Вона також пропонує порядок залучення «електронного документа» до кримінального процесу, який, на її думку, доцільно закріпити у КПК [262, с.15].

Г.С. Бідняк у своїй дисертації «Використання спеціальних знань під час розслідування шахрайств» зазначає, що використання «електронних документів» є поширеним під час вчинення шахрайства. У дослідженні запропоновано порядок огляду, вилучення та упакування комп'ютерних пристроїв, на яких можуть міститись електронні документи. Звернено увагу на необхідність залучення спеціаліста при огляді та вилученні електронних документів [43].

Ю.Ю. Орлов та С.С. Чернявський зазначили, що між «класичними» документами й так званими «електронними документами» є багато відмінностей, які стосуються не лише форми подання інформації, а також її змісту і, крім того, – походження доказу, його природи, можливостей експертного дослідження. Ці відмінності «класичних» документів від так званих «електронних документів» у своїй сукупності дозволяють говорити про два різних джерела доказів. «Електронні документи» як джерела доказів у кримінальному провадженні, на їх думку, неможливо віднести до традиційних документів. Через цю обставину, а також з метою уникнення термінологічних непорозумінь, вони пропонують використовувати термін «електронне відображення» та виокремити їх у самостійне джерело доказів та вид доказів у кримінальному провадженні [154].

Є.С. Хижняк досліджував сутність терміну «електронний документ» та його властивості, вивчав особливості процесуального закріплення електронних доказів, а також тактичні особливості оформлення результатів слідчого огляду [255].

На думку О.В. Сіренко, слід надалі продовжувати дослідження категорій «електронні докази» та «електронні документи». Першочерговим питанням є встановлення порядку збору та фіксації електронних доказів, формування методики їх дослідження [201, с. 211].

С.М. Стахівський виділяє електронні речові докази та електронні документи. Науковець пропонує визначення електронних речових доказів, а саме, що це будь-які носії комп'ютерної інформації чи програмні об'єкти, які містять специфічні сліди злочину чи інформацію, що буде сприяти встановленню злочину. Вчений зазначає, що електронний документ це комп'ютерна інформація в цілому, яка має доказове значення у кримінальному провадженні та пропонує використання комп'ютерної мережі в процесі доказування [211, с. 21].

Д.М. Цехан досліджує «цифрові докази», зазначає про необхідність залучення спеціаліста, використання сертифікованого програмного забезпечення для фіксації таких доказів та пропонує способи забезпечення допустимості [257, с. 257].

О.А. Самойленко у посібнику «Виявлення та розслідування кіберзлочинів» ототожнює поняття «інформація в електронній формі», «електронні дані», «електронний документ». Вона вважає, що такий доказ не може існувати без носія інформації – джерела електронних даних як доказів, якими є різноманітні носії інформації (моноблоки, мобільні телефони, планшетні комп'ютери, цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, що містить звуко- та відеозаписи тощо;) невидимі «неозброєним оком» і для їх сприймання та дослідження використовують спеціальні програми та технічні засоби; також вони можуть пошкодитись, знищитись чи змінитись під час користування пристроєм, або під впливом різних чинників. У посібнику розглянуто типові слідчі ситуації та тактичні операції під час розслідування кіберзлочинів, запропоновано тактичні правила проведення слідчих (розшукових) дій спрямованих на збирання, вилучення доказів в електронній формі, досліджено загальні тактичні особливості проведення негласних слідчих (розшукових) дій [193].

М.М. Федотов пропонує використовувати поняття «форензика» для найменування відносно нового розділу криміналістики, який вивчає комп'ютерні докази. Науковець відмічає про існування електронних документів, електронних слідів, необхідність використання і дослідження електронної пошти, наявні

особливості проведення комп'ютерно-технічної експертизи електронного документа. Він пояснює, що електронні документи є дешевші в зберіганні та обробці у порівнянні з паперовими [252, с. 11, 47].

О.В. Шведова у своїй науковій розробці провела дослідження теоретичних, методологічних і практичних засад комплексного криміналістичного дослідження документів, виконаних за допомогою комп'ютерних технологій. Вона приділила увагу поняттю та класифікації предмета, завдань, об'єктів, методів і методик комплексного криміналістичного дослідження документів, виконаних за допомогою комп'ютерних технологій. Крім того, науковець дає наукове визначення «електронного документа», розглядає основні характеристики та ознаки електронного документа та пропонує класифікацію електронних документів [266].

Окрім О.В. Шведової, дослідженням електронного документа займався С.Й. Гонгало у дисертації «Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку», яка захищена у 2013 році ним класифіковано і охарактеризовано електронні документи за видами, запропоновано методику дослідження електронних документів, розглянуто особливості експертного дослідження електронних документів у середовищі їх існування, особливості отримання криміналістично значущої інформації, зокрема комп'ютерної, яка міститься у документах. С.Й. Гонгало визначає «електронний документ» різновидом традиційного документа, що відрізняється від нього лише електронно-цифровою формою та потребує розкодування – візуалізації. Електронний документ, на його думку, є стадією розвитку документа після рукописного, друкованого та комбінованого документа з елементами захисту від підроблення [91].

Дослідження О.В. Шведової та С.Й. Гонгало присвячені більшою мірою криміналістичним основам дослідження електронного документа та проведенню його експертизи. В основному дослідженням електронних доказів під час досудового розслідування займались вчені-криміналісти, натомість у галузі кримінального процесу таких досліджень практично не проводилось. Однак, для

належного впровадження електронних доказів у кримінальне провадження необхідна обопільна підтримка науковців з обох названих сфер знань [121, с. 242].

Колективи авторів закладів вищої освіти із специфічними умовами навчання, які здійснюють підготовку здобувачів за спеціальністю «Право» теж досліджували поняття електронного документа. Зокрема, у Дніпропетровському державному університеті внутрішніх справ видано методичні рекомендації «Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів», у якому автори дослідили поняття та види електронних носіїв інформації, тактичні особливості отримання доступу до електронних носіїв інформації, порядок пошуку власника Інтернет-сторінки, особливості призначення експертиз носіїв інформації та інші питання [59].

На базі Національної академії внутрішніх справ у 2020 році опубліковано друге, доповнене видання методичних рекомендацій «Використання електронних (цифрових) доказів у кримінальних провадженнях». У даних рекомендаціях розглянуто поняття та особливості електронних доказів, порядок їх виявлення, збирання та фіксації, особливості вилучення різних технічних пристроїв, запропоновано перелік питань для проведення експертиз електронних доказів [58].

А.В. Столітній, І.Г. Каланча висловили думку, що формування інституту «електронного доказу» в науці кримінального процесу є штучним. Однією з причин, які цьому сприяють є зміни щодо електронних доказів до ГПК, ЦПК, КАС, які оминули КПК. Вони не поділяють такої позиції галузевого законодавства з огляду на неможливість застосування для виокремлення нового джерела доказів таких характеристик, як форма фіксації інформації, ознаки носія інформації чи спосіб відтворення даних. Однак, безумовно, враховуючи стрімкий розвиток ІТ, є перспектива створення такого формату електронної інформації (в тому числі способу перевірки її незмінності та цілісності без проведення експертного дослідження), що потребуватиме розширення джерел доказів –

електронними [213]. Схожої позиції дотримується Глібко В.М., який визначає «електронний документ» як один зі способів фіксації документа [88, с. 3-4].

З аналізу проведених досліджень можна зробити висновок про те, що науковці не можуть оминути проблему відсутності єдиного сталого визначення поняття «електронного документа», яке станом на сьогодні відсутнє у КПК. Однак, більшою проблемою є відсутність єдиного підходу до сутності електронного документа у доказуванні.

Існує декілька позицій науковців з даного приводу, наприклад: докази, виражені в електронному вигляді, вводяться в процес за допомогою їх віднесення до традиційних видів доказів. У кримінальному процесуальному праві «електронні докази» найчастіше відносять або до речових доказів, або до документів [159, с. 246].

Аналіз наукових праць різниць вчених та практиків показує, що зазвичай електронні документи відносять до різновиду документів, як джерел доказів [43, 91, 221, 257, 261, 266], речових доказів як джерел доказів [47, 132], документів або речових доказів, як джерел доказів [58, 59, 94, 105, 146, 149, 193, 211], самостійне джерело доказу [112, 124, 154], або вважають його лише способом фіксації інших доказів [88, 213, 214]. Зокрема, А.В. Столітній зазначає, що цифрова інформація залежно від умов, способу й суб'єкта створення, процедури отримання та закріплення може бути будь-яким із джерел доказів [214, с. 127].

З твердженнями науковців, які вважають що електронний документ є лише способом фіксації інших доказів ми не погоджуємось, з огляду на наступне:

Відповідно до ст. 103 КПК, процесуальні дії під час кримінального провадження можуть фіксуватися: у протоколі; на носії інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії; у журналі судового засідання. П.3 ч.2 ст.99 КПК передбачає, що до документів за наявності відомостей передбачених ч. 1 ст. 99 КПК, можуть належати складені в порядку, передбаченому КПК, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії. Згідно абз. 1, 2 ч. 2 ст. 104 КПК, у випадку фіксування

процесуальної дії під час досудового розслідування за допомогою технічних засобів про це зазначається у протоколі. Якщо за допомогою технічних засобів фіксується допит, текст показань може не вноситися до відповідного протоколу за умови, що жоден з учасників процесуальної дії не наполягає на цьому. У такому разі у протоколі зазначається, що показання зафіксовані на носії інформації, який додається до нього.

Аналіз зазначених статей дає можливість провести розмежування електронних документів як джерел доказів та як способу фіксації такого доказу.

По-перше, це час створення електронного документа. Електронний документ (листування, фотографії, відеозаписи, тощо) можуть бути створені будь-ким та в будь-який час. Натомість електронний документ, як спосіб фіксації проводиться лише в межах досудового розслідування (після внесення відомостей до ЄРДР) та під час судових засідань у порядку, регламентованому КПК.

Ю.Ю. Орлов та С.С. Чернявський зазначили, що «електронні документи» можуть бути складені виключно незалежно від кримінального провадження. При цьому вони містять опис події, яка стала предметом провадження (наприклад, результат моніторингу дій користувача, який здійснює шахрайство в комп'ютерній мережі), або є засобом вчинення злочину (наприклад, імітаційний сайт, призначений для здійснення Інтернет-маркетингу), або ж встановлюють окремі факти, обставини, що мають відношення до кримінального провадження (наприклад, трафіки з'єднань абонентів мобільного зв'язку, які можуть бути свідками події) [154, с. 18].

А.С. Запотоцький з цього приводу вважає, що «електронні документи» з'являються у кримінальному провадженні, так би мовити, в «готовому вигляді», а кримінальний процесуальний кодекс лише регламентує порядок їх збирання та дослідження, але не порядок складання. В той час, коли форма, обов'язкові реквізити та порядок складання протоколів, за результатами слідчих (розшукових) дій з метою дотримання достовірності доказів регламентовано у КПК. Протоколи є завжди письмовими документами, які складені згідно з вимогами КПК, тоді як «електронні документи» мають іншу форму [111, с. 9].

По-друге, здійснювати фіксацію доказу в електронній формі може лише уповноважений на те суб'єкт (слідчий, дізнавач, прокурор, секретар судового засідання), а створити електронний документ може будь-яка особа, або ж комп'ютерна система.

Електронний документ в Інтернет-середовищі може бути сформований не лише людиною, але й безпосередньо інформаційною системою (наприклад, трафіки з'єднань абонентів мобільного зв'язку, динамічні бази банківських проводок, білінгові системи, log-файли (визначення даних термінів у додатку Г) тощо). Отже, на відміну від «класичного» документа, «електронний документ» може не мати автора. Проте, створення «електронного документа» машиною відбувається внаслідок певних дій особи в інформаційній мережі (телефонування, перерахування грошей, відвідування сайтів тощо). Процес формування такого «документа» є подібним до процесу формування речового доказу, який містить сліди злочину: він формується природним (технічним) шляхом й незалежно від бажання людини, але внаслідок її дій [154, с. 15].

Збирати електронні документи можуть лише сторони кримінального провадження, наділені відповідними повноваженнями. Інші учасники кримінального провадження можуть бути залучені слідчим, дізнавачем, прокурором до проведення слідчих (розшукових) дій. Більш детально дане питання буде розглянуто у підрозділах 2.1. та 3.1.

По-третє, для формування електронного документа як доказу необхідно надати йому відповідну процесуальну форму. Така процедура здійснюється під час фіксації доказів. Електронний спосіб фіксацій є одним з різновидів фіксації доказів.

Електронний документ, який існує в електронному середовищі, тільки після належного фіксування буде мати доказове значення у кримінальному провадженні. Суб'єкт, який здійснює збирання електронних документів відтворює його, аналізує, описує, вилучає та копіює на новий технічний носій.

Натомість електронний спосіб фіксації це цілеспрямована діяльність суб'єктів збирання доказів, яка полягає у складанні протоколів процесуальних

дій та додатків до них. Електронний спосіб фіксації (повністю або частково) може здійснюватися як щодо електронних документів, так і до інших джерел доказів – речових доказів, показань учасників кримінального провадження. Спосіб фіксації визначає кінцевий вигляд доказу: повністю електронний (електронне процесуальне оформлення) чи змішаний (процесуальне оформлення на паперовому носії) [214, с. 120].

Таким чином, вважаємо що електронний документ не є штучно створеним інститутом кримінального процесу, а існує незважаючи на неврегульованість даного питання нормами КПК. Неоднозначне розуміння електронного документа серед науковців спричиняє відсутність єдиного комплексного підходу щодо дослідження даного питання та можливості використання цих знань у практичній діяльності.

Ми погоджуємось з думкою науковців, які вважають, що «електронний документ» слід віднести до окремого виду доказів. Зокрема, Н.А. Зігура та А.В. Кудрявцева слушно наголошують на тому, що комп'ютерна інформація повинна розумітися як окремий вид доказів з огляду на те, що вона має особливі специфічні властивості, що відрізняють її, з одного боку, від речового доказу, а з іншого боку – від документа [112, с. 30].

О.П. Метелев зазначає, що основними причинами виділення цифрової інформації, зафіксованої на машинних носіях, в якості самостійного і специфічного джерела відомостей, які не входять ні до складу речових доказів, ні до складу документів, є її особлива нематеріальна природа, природно-технічні особливості її створення, обробки, зберігання, передачі в часі і просторі, а також кримінально-процесуальні процедури і техніко-криміналістичні прийоми її пошуку та вилучення, доступу до неї, дослідження і перетворення її в форму, яку сприйматиме людина. У такому випадку необхідно оцінювати власне інформацію, а не матеріальний об'єкт на якому вона зафіксована. Крім того, для набуття доказового значення цифрова інформація повинна бути спеціальним чином перетворена із системи дискретних сигналів різної фізичної природи в форму, яку може сприймати людина. Так, наприклад, зміст документальної

інформації, яка міститься в електронних документах чи файлах баз даних, звукових файлів чи фонограм, може бути перетворений у візуальну інформацію, або шляхом її роздрукування на паперовий носій, або шляхом її виведення на екран монітора [145, с. 102-103].

Законодавець не врахував, що електронний доказ і речовий доказ не є тотожними поняттями, а тому дане положення повинно бути враховане у КПК. Ураховуючи вищевикладене, можемо стверджувати, що тенденції інформаційно-технологічного прогресу, які диктує нам час, потребують удосконалення інституту електронних доказів на законодавчому рівні. Погоджуючись із думкою більшості науковців, необхідно вирізнити «електронний доказ» серед інших видів доказів та надати йому окремий статус шляхом внесення змін до КПК, окремою нормою «електронні докази» з визначення змісту поняття, його ознак та різновидів [159, с. 246-247].

Більш детально про місце електронних документів у системі доказів КПК та відмінність електронних документів з документами і речовими доказами нами буде досліджено у підрозділі 1.2.

Вважаємо позитивним подання народними депутатами України законопроєкту «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів», реєстраційний №4004 від 01.09.2020 року [165]. У даному законопроєкті запропоновано використовувати поняття «електронних доказів», яким доповнити перелік процесуальних джерел доказів, проведено розмежування поняття електронного документу як різновиду електронного доказу та інших документів, які подаються в електронній формі. З метою підготовки зазначеного проєкту до попереднього розгляду нами надано пропозиції та зауваження, які наведені у додатку В дисертації.

Законодавче регулювання електронних доказів та науковий рівень дослідження проблем їх використання не відповідають вимогам практики. Зокрема, доцільно перестати робити акцент на матеріальному носії інформації документа. Оскільки, в такому випадку документом вважається фізичний носій

інформації, а не окремий файл, який міститься на ньому та має доказове значення. Крім того, на одному носії можуть міститись безліч файлів, а доказове значення у кримінальному провадженні мати лише один. Прив'язка документа до носія інформації, який існує в матеріальному вигляді також спричиняє проблему вилучення інформації з інтернет-серверів, які, зазвичай, можуть знаходитись віддалено та доступ до яких отримати дуже складно, або неможливо [121, с. 239].

До основних проблем також слід віднести складність процесу встановлення оригіналу та копії електронних документів, дослідження електронних документів, проведення експертизи, ідентифікації. Через велике навантаження працівників експертно-дослідних інститутів, час проведення експертизи може тривати від 1 до 6 місяців.

Відсутність базових знань у галузі ІТ (визначення терміну у додатку Г) та повноцінно сформованої методики збирання та використання таких доказів призводить до залучення спеціаліста, вилучення великої кількості обладнання, або ж витрачання багато часу на їх пошук та фіксацію. Окрім цього, відсутність засобів, котрі можуть бути використані слідчими, дізнавачами з цією метою самостійно (без участі спеціалістів), є ще однією перепоною ефективної роботи з електронними доказами. У більшості випадків дослідження такої інформації фактично відбувається у формі експертизи без участі слідчих при її проведенні.

Без елементарних знань принципів роботи мереж (локальних та Інтернет), файлових систем, протоколів роботи систем і підсистем, принципи формування log-файлів і загалом основ ІТ, ефективне використання означених засобів і їх глибинне дослідження не видається можливим [149, с. 317].

Місцеві суди м. Харкова і Харківської області, в узагальненні щодо використання електронних доказів (доказів вчинення злочину, які можна отримати в електронній формі) по кримінальних провадженнях, які перебували на розгляді у 2018 та 2019 роках відзначають, що під час дослідження електронних доказів з точки зору їх належності, допустимості, достовірності виникають труднощі, оскільки чіткої процедури збирання і дослідження таких доказів, порядку встановлення особи, яка розмістила певну інформацію,

законодавством не визначено. Інформація в електронній формі може бути змінена чи знищена до початку судового розгляду, що призводить до неможливості встановлення факту її існування раніше. Іншими проблемами є складність встановлення оригіналу та копії електронного доказу, відсутність спеціального обладнання та ліцензійних програм для роботи з електронними доказами. У деяких випадках, суду доводиться залучати спеціаліста для відтворення та дослідження електронного доказу, що впливає на строки судового розгляду [35].

Науковцями запропоновано виокремити не врегульовані та проблемні аспекти використання електронних документів у кримінальному судочинстві України:

- відсутність чіткого процесуального порядку їх збирання;
- відсутність критеріїв визнання електронних документів недопустимими;
- відсутність сформованої методики дослідження таких доказів;
- недостатність спеціальних знань роботи з комп'ютерними технологіями у слідчих, дізнавачів, оперативних працівників;
- відсутність закріплення на законодавчому рівні необхідної термінології [34, с. 248-249].

Д.М. Цехан зазначає, що ключовою перешкодою, що на сьогодні унеможливлює використання цифрової інформації в якості доказу, є відсутність експертних методик її ідентифікації та аутентифікації [258, с. 121].

Незважаючи на наведені недоліки, електронні документи мають беззаперечні переваги. До основних переваг можна віднести наступні:

- використання практично кожною особою щодня;
- електронний документ у вигляді фото-, аудіо- чи відео- запису дає змогу оцінити ситуацію чи подію більш комплексно та повно;
- простому користувачу складно внести зміни у технічні записи електронного документа, які здійснюються технічним пристроєм чи програмою;

- може мати дуже великий обсяг, що вимірюється гігабайтами інформації, однак зручний та економний у зберіганні.

За результатами опитування працівників підрозділів Національної поліції встановлено, що основі труднощі під час збирання та дослідження інформації в електронній формі виникали під час: призначення експертизи (складення переліку питань, направлення доказів, тривалість експертизи) – 18,8%; відсутність ліцензійного програмного забезпечення для копіювання, вилучення, транспортування, зберігання (у т.ч. операційних систем) таких доказів – 17,7%; відсутність технічних засобів для копіювання, вилучення, транспортування, зберігання таких доказів – 16,3%; відсутність достатньої кількості спеціалістів для залучення до проведення слідчих (розшукових) дій – 15,1%; складність процесу встановлення оригіналу, копії, дублікату інформації в електронній формі – 10,4% (додаток А).

Отже, завдяки аналізу рівня теоретичної розробленості проблематики з'ясовано, що окремі питання дослідження електронного документа недостатньо висвітлені в працях вітчизняних вчених.

Чимало положень, які по суті є дискусійними та потребують подальшого вдосконалення та розвитку, оскільки, по-перше, більшість досліджень «електронного документа», як джерела доказу було проведено в інших галузях права, по-друге, відсутнє комплексне кримінальне процесуальне та криміналістичне дослідження «електронного документа», що об'єктивно не може комплексно сприяти розв'язанню сучасних проблем використання електронного документа у доказуванні. Донині залишаються не дослідженими й актуальними і такими, що потребують розробки, питання поняття та змісту електронного документа, його основних ознак; класифікації електронного документа; оцінки електронного документа з точки зору допустимості, належності, достовірності та достатності; способи отримання та дослідження електронного документа та міжнародний досвід його використання. Вважаємо, що розв'язання цих питань сприятиме покращенню якості з доказування на всіх стадіях кримінального провадження.

1.2. Електронні документи в системі джерел доказів у кримінальному провадженні

Ч. 2 ст. 84 КПК чітко встановлює, що процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Цей перелік є вичерпним. При їх оцінці, джерела мають однакову юридичну силу, однак різні особливості своєї форми.

Показання, речові докази, документи, висновки експертів це процесуальні джерела, тобто матеріальна форма, у якій містяться і за допомогою якої передаються фактичні дані. Такі джерела гарантують отримання найбільш повних і достовірних фактичних даних, що є важливою умовою допустимості доказів [251, с. 11-12].

Разом з тим, під час виявлення доказу, який міститься в електронній формі у практичних працівників часто виникають труднощі, до якого з джерел доказів його відносити – речового доказу чи документа. Неправильне тлумачення норми спричиняє різні дискусії, неоднозначне застосування норми закону та перешкоджає вирішенню завдань кримінального провадження.

На нашу думку, з урахуванням норм чинного КПК, електронні документи в залежності від їх змісту, форми та мети створення у кримінальному провадженні можуть бути сформовані як речові докази або документи.

Документи на технічних носіях інформації за змістом і зв’язком із кримінальним правопорушенням можуть бути поділені на речові докази та документи. Перші – це докази використання ІТ під час вчинення «комп'ютерних» правопорушень. Сюди відносять програми зі слідами зміни команд або введення непередбачених команд, створення умов автозаміни програми, несанкціонованої зміни алгоритму і т.д. Другі – носії інформації про обставини, які мають значення для кримінального провадження, які в принципі не надто відрізняються від паперових документів – носіїв інформації [39, с. 164-165].

Ми вважаємо, якщо електронний документ, який був знаряддям вчинення кримінального правопорушення, зберіг на собі його сліди, або був об’єктом кримінально-протиправних дій то у таких випадках він буде речовим доказом.

Для такого різновиду речових доказів важливу роль відіграє матеріальний носій електронного документа, а інформація, яка на ньому міститься нерозривно з ним пов’язана. Так, О.О. Тушев та М.О. Назаров зазначають, якщо на комп’ютері (телефоні, інших електронних пристроях) збереглись сліди передачі якоїсь інформації, без її змісту, які мають значення для кримінального провадження, то даний електронний носій буде речовим доказом. Якщо ж доказову інформацію отримують зі змісту такого носія (текст, малюнок, графіки, формули і т.д), то їх слід відносити до документів [220].

Для того, щоб відрізнити електронний документ від речового доказу у формі електронного документа слід звернути увагу на те, що саме може бути використане як доказ факту чи обставин, що встановлюються під час кримінального провадження: інформація чи фізичний носій інформації. Саме ці ознаки є визначальними при розмежуванні.

У науці кримінального процесу під речовими доказами розуміють предмети, які через свої власні якості та зв'язок з іншими обставинами можуть служити засобом для встановлення обставин, що мають значення для кримінального провадження. При цьому ознака об’єктивності є ключовою та означає, що інформація, яку містить речовий доказ і яка має значення для кримінального провадження, формується незалежно від волі чи бажання будь-якої особи [101, с. 54-53].

Провівши аналіз теоретичних позицій та законодавчий підхід, С.О. Ковальчук відзначив, що зміст електронних доказів складають фактичні дані, на підставі яких можуть бути встановлені факти й обставини, що мають значення для кримінального провадження і підлягають доказуванню, та які існують в електронно-цифровій формі. До таких доказів можуть належати шкідливі програми, віруси, програми, які були об’єктом протиправних дій, комп’ютерні сліди, кошти та інші цінності в електронній формі, електронні документи та інші. Такі докази створені та існують об’єктивно, незалежно від волі правоохоронних органів та суду, містять доказову інформацію та не містять ознак предметності [124, с.121-122].

Розмежування документів і документів-речових доказів, як процесуальних джерел доказів також можливо за допомогою способу збереження та передачі відомостей про факти й обставини, які підлягають доказуванню у кримінальному провадженні. Традиційні документи письмової форми відображають обставини та факти, які мають доказове значення у своєму змісті, а в документах-речових доказах, такі дані містяться у його зовнішніх ознаках, властивостях предмета, формі. Звичайні документи можуть бути замінені копією, дублікатом, а речові докази завжди є незамінними [101, с. 65].

У монографії «Теорія і практика кримінального процесуального доказування» В.В. Вапнярчук відмітив, що при розгляді документів як самостійного процесуального джерела доцільно звернути увагу на їх розмежування з іншими процесуальними джерелами. Наприклад, матеріальний об'єкт, який містить певну інформацію, є документом у тому випадку, коли він важливий лише своїм змістом. Якщо ж для провадження мають значення його інші якості (зовнішній вигляд, сліди, матеріал з якого виготовлений, місце чи час його знаходження тощо), тоді він набуває статусу речового доказу [52, с. 305].

Особливістю документів-речових доказів, як процесуальних джерел також є їх зв'язок з подією кримінального правопорушення, оскільки існують випадки, коли річ не містить інформації, яка може бути доказовою. Наприклад, виявлення листа, фотокартки, блокнота під час огляду місця події, приміщення чи під час обшуку, виявлення раніше викрадених речей у підозрюваного, тощо надає таким предметам ознак речового доказу. Речі та предмети, походження яких невідоме (приміром, ніж з відбитками пальців підозрюваного чи аудіозапис із зізнанням у вчиненні злочину, підкинуті слідчому невідомими особами) не можуть набути статусу речового доказу, поки не буде з'ясована їх попередня історія. Таким чином, речовим доказом є не сама річ як така, а річ з її певними якостями і зв'язками з доказовими фактами [52, с. 296].

А.П. Запотоцький, аналізуючи КПК 1960 року, пропонує проводити розмежування документів – джерел доказів від документів – речових доказів за наступними критеріями: 1) відомості, які зафіксовані у документах – речових

доказах, відрізняються від інформації, що міститься в електронних документах, за своїм процесуальним статусом; 2) доказове значення у документах – джерелах доказів має лише зміст, а їх форма носить допоміжне значення. На відміну від них, документи – речові докази значущі у кримінальному провадженні не лише за змістом, а й за своїм зовнішнім виглядом, місцем, часом їх виявлення тощо; 3) документи – джерела доказів можуть бути замінними, у той час, як документи – речові докази внаслідок того, що зміни, які відбулися з ними, пов'язані з подією злочину, не можуть бути замінені на інші, оскільки сліди, що відобразились у них, є унікальними й існують в однині; 4) документи як джерела доказів можуть копіюватися з наступним процесуальним оформленням, що не зменшує їх доказового значення, а речові докази практично завжди унікальні і неповторювані; 5) документ – джерело доказів містить у собі відомості, які складаються з опису події злочину чи фактів його вчинення за допомогою письма або інших умовних знакових кодів тощо, на відміну від документа – речового доказу, що закріплює не опис матеріальних слідів злочину чи факту його скоєння, а самі сліди злочину, які збереглися на ньому [111]. Ці критерії дають чітке уявлення про розмежування документів та речових доказів як джерел доказів, та можуть бути використані й при розмежуванні електронних документів у кримінальному провадженні.

Вважаємо, що важливе значення має розмежування за тим, що саме має доказове значення: зміст чи форма. Якщо доказове значення має інформація, яка збережена в електронній формі, то це електронний документ. Наприклад, електронний лист на поштовій скриньці, отриманий через мережу Інтернет з інформацією, яка має значення для кримінального провадження.

Комп'ютерна програма, збережена на носії інформації, за допомогою якої відбулося несанкціоноване втручання в роботу комп'ютера буде речовим доказом. Носій інформації без вищевказаної комп'ютерної програми на ньому не має жодного доказового значення.

На нашу думку, віднесення електронного документа до певного різновиду джерел доказів не може забезпечити його правильне використання у доказуванні.

Так, С.О.Ковальчук зазначив, що на підставі норм КПК і сформованої слідчої та судової практики, електронні докази на сьогодні розглядаються як електронні документи, а їх матеріальні носії – як речові докази. Проте, з урахуванням їх існування в електронній формі та механізму залучення у кримінальне провадження, електронні докази, по аналогії з їх закріпленням в адміністративному, господарському і цивільному процесах, підлягають визнанню самостійним видом доказів у кримінальному процесі [124, с. 123].

Визнання електронного документа самостійним джерелом доказів, розроблення нормативно-правового забезпечення щодо їх виявлення, збирання, оцінки полегшить роботу практичних підрозділів та усуне законодавчі прогалини. Враховуючи вищевикладене, пропонуємо доповнити ч. 2 ст.84 КПК п’ятим процесуальним джерелом доказів – електронний документ.

Відсутність єдиного підходу до поняття електронного документа та єдиної практики його використання під час досудового розслідування спричиняє неоднозначне розуміння порядку використання та фіксації електронного документа під час доказування.

Слід зазначити, що за допомогою комп’ютерних технологій може бути вчинено безліч кримінальних правопорушень (загроза терористичного акту, виготовлення порнографічної продукції, фінансові правопорушення, тощо), це обумовлює необхідність проведення огляду комп’ютерної техніки, обшуку, який супроводжується специфічною процедурою фіксації, вилучення і дослідження електронних доказів. Відсутність чіткого законодавчого закріплення поняття електронних доказів, їх видів, джерел, допустимості спричинює низький рівень розкриття окремих видів кримінальних правопорушення та невизнання їх у суді [37, с. 123].

На практиці, зазвичай, слідчими, дізнавачами та прокурорами не надається належна оцінка електронних документів. Серед найбільш поширених помилок є прирівнювання роздруківки з електронним документом, збереженим на комп’ютері; копіювання електронних документів без спеціального програмного забезпечення та залучення спеціаліста; відсутність чіткого розуміння між

відеозаписом, який є електронним документом і який є речовим доказом та ін. Будь-яка помилка, допущена під час отримання електронного документа може спричинити визнання даного доказу недопустимим та, відповідно, не може використовуватися судом при прийнятті процесуальних рішень.

Як вважає Є.Г. Коваленко, не зважаючи на поширеність та частоту використання поняття «документ», він все одно залишається недостатньо дослідженим як на теоретичному, так і на практичному рівнях. Відсутність єдиного загальноприйнятого поняття документа, низькі знання у документоведенні впливають на здійснення практичної діяльності [123, с. 543]. Аналогічно можна сказати про поняття електронного документа.

Для дослідження поняття «електронного документа» виділимо основні поняття, які існують у законодавчій та науковій сферах.

Відповідно до Закону України «Про електронні документи та електронний документообіг», електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [169].

Згідно ДСТУ 7157:2010, затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 11 березня 2010 року № 8 «Інформація та документація. Видання електронні. Основні види та вихідні відомості», електронний документ – документ, інформація, в якому подана у формі електронних даних і для використовування якого потрібні засоби обчислювальної техніки [103, с. 2].

Відповідно до наказу Міністерства освіти і науки, молоді та спорту України від 01 жовтня 2012 року «Про затвердження Положення про електронні освітні ресурси» № 1060, електронний документ це документ, інформація в якому подана у формі електронних даних і для використання якого потрібні технічні засоби [171].

Енциклопедія державного управління пояснює, що документ електронний – документ, інформація в якому зафіксована у вигляді електронних даних,

включаючи обов'язкові реквізити документа, склад та порядок розміщення яких визначається законодавством [107, с. 142-144; 108, с. 126-127].

Великий енциклопедичний юридичний словник дає поняття електронного документа як матеріального носія відповідної інформації, зафіксованої у вигляді електронних даних, включаючи обов'язкові реквізити документа, без яких він не може бути підставою для його обліку і не матиме юридичної сили [57, с. 247].

У юридичній енциклопедії, електронний документ – це електронні копії документів з паперових оригіналів, а також деякі набори даних, спеціально підготовлених для зберігання, передавання і використання в електронному цифровому вигляді [270, с. 354].

На думку Є.С. Хижняка під електронним документом необхідно розуміти будь-яку інформацію, представлену в електронній формі, що має значення для розслідування кримінальних правопорушень, дослідження якої здійснюється за допомогою спеціальних програмно-технічних засобів [255, с. 81] .

Е.Кейсі пропонує поняття цифрового доказу, під яким розуміє будь-які дані, які можуть підтвердити вчинення злочину, або можуть встановити зв'язок між злочином та жертвою чи злочином і злочинцем [2, с. 7].

У ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» пропонується термін «цифровий доказ», під яким розуміють інформацію або дані, збережені або передані в бінарному вигляді, на які можна покладатися як на докази [104, с. 2].

Колектив авторів Національної академії прокуратури України, зазначають, що поняття «електронні докази» – це інформація, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах та відповідає вимогам ст. 84 КПК [102, с. 112.].

О.І. Котляревський та Д.М. Киценко пропонують використовувати поняття «електронні докази», під яким вони розуміють сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в

електронних засобах [127]. З даним визначенням погоджується В.В. Мурадов який зазначає, що воно є більш точним серед науковців [149, с. 316-317].

П.Д. Біленчук, А.П. Гель, Г С. Семаков зазначають, що електронні докази — це сукупність інформації, яка зберігається в електронному вигляді на всіх типах електронних носіїв і в електронних засобах [45, с. 451].

Н.М. Ахтирська вказує, що електронні докази – це дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій [38, с. 125].

О.В. Сіренко вважає, що електронні докази – це дані про обставини, що мають значення для кримінального провадження і існують у нематеріальному вигляді в межах технічного носія чи каналу зв'язку та сприйняття та дослідження яких можливо за допомогою технічних засобів та програмного забезпечення [201, с. 211].

На думку С.І. Хом'яченка та Т.О. Часової, електронний доказ – це інформація (відомості), що має електронну (цифрову) форму про обставини, які підлягають обов'язковому доказуванню у кримінальному провадженні [256, с. 178].

Деякі вчені відкидають поняття електронного документа та пропонують інші визначення. Так, наприклад, В.В. Лисенко відмітив, що окрім «електронного документа» автори використовують терміни «машинний документ», «документ, підготовлений з використанням електронно-обчислювальних машин», «комп'ютерна інформація» тощо. Сам В.В. Лисенко пропонує застосовувати термін «інформація, що міститься в електронному вигляді на будь-яких носіях» [137, с. 64]. Т.О. Кузубова вживає термін «електронний формат документа» як різновид документа [135, с. 161-162].

І. О. Крицька зауважує, що в науковому юридичному обігу зустрічаються і такі поняття, як «комп'ютерні докази», «комп'ютерні об'єкти» та ін. Утім, їх дефініції суттєво не відрізняються від визначення «цифрових доказів». Категорія «цифрові джерела доказової інформації» об'єднує програми (програмне

забезпечення), файли баз даних, аудіо-, відеозаписи тощо, джерелом яких, а отже, і формою існування, виступають засоби цифрової техніки – машинні носії, до яких належать оперативні запам'ятовуючі пристрої, постійні запам'ятовуючі пристрої, накопичувачі на жорстких магнітних дисках (вінчестери, дискети), переносні машинні носії (оптичні носії, флеш-карти), NAS-системи тощо [133, с. 302].

На думку Д.О. Алєксєєвої-Процюк та О.М. Брисковської у кримінальному провадженні не варто повністю ототожнювати поняття «цифрові докази», «комп'ютерні об'єкти», «кібердокази», «електронні документи», «електронне відображення», «цифрові джерела доказової інформації», «електронні докази». Адже цифрова інформація є формою передання електронної інформації. І хоча сьогодні весь світ переходить саме на цифрову інформацію, у КПК необхідно використовувати більш універсальний термін – електронні докази, під якими розуміти фактичні дані, які зберігаються в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах та які після обробки спеціальними технічними засобами та програмним забезпеченням стають доступними для сприйняття людиною [34, с.250]. Протилежною є думка у суддів Нововодолазького районного суду Харківської області, які вважають що терміни «електронні докази» та «цифрові докази» є тотожними поняттями [35].

Д.М. Цехан пропонує застосовувати визначення «цифровий доказ» під яким розуміти фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому, обов'язковою ознакою цифрового доказу є конвергентність – здатність одиничного доказу входити у сукупність інших доказів і набувати у зв'язку з цим доказового значення [257, с. 257]. Термін «цифровий доказ» також використовує О.П. Метелев, який розуміє під ним фактичні дані, отримані зі штучно створеного середовища та представлені у цифровій (дискретній) формі, зафіксовані на будь-якому типі електронних носіїв і які стають доступними для сприйняття людиною за допомогою комп'ютерного обладнання, які вилучені, зафіксовані, досліджені та збережені відповідно до

формалізованих процесуальних вимог, встановлюють наявність чи відсутність фактів та обставин, що мають доказове значення для кримінального провадження [146, с. 82].

Судді Куп'янського міськрайонного суду Харківської області розуміють поняття «електронні докази», як інформацію в електронній (цифровій) формі, яка містить дані про обставини, що мають значення для кримінального провадження та підлягають доказуванню. Судом використовуються, зокрема, такі електронні докази: електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (визначення терміну у додатку Г), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Перелік джерел інформації, які підпадають під поняття «електронний доказ», на думку суддів, не є вичерпним і законодавцем не надане належне поняття та порядок використання у кримінальному процесуальному законодавстві [35].

У Комсомольському міському суді Полтавської області вважають, що найбільш простим визначенням «електронних доказів» є фактичні дані, які зберігаються в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах та які після обробки спеціальними технічними засобами та програмними забезпеченнями стають доступними для сприйняття людиною. В той же час, судді вважають, що інформацію, яка зчитується ЕОМ, більш доцільно називати цифровою, а не електронною, так як вона пов'язана з кодуванням символів у цифри, з файлами, і поза ними існувати не може. [221].

Проблемою при формулюванні поняття «електронний документ» є двоєдина його сутність, тобто наявність двох складових: інформаційної (зміст документа) та технічної (специфічні процедури створення, підписування, передачі та зберігання електронного документу з використанням засобів електронно-обчислювальної техніки) [204, с. 32].

На нашу думку, використання терміну «електронний документ» є доцільним та необхідним у кримінальному процесуальному законі. По-перше, поняття «електронний» є ширшим ніж поняття «цифровий» та охоплює його.

«Цифровий» це уже у будь-якому разі «електронний». Комп’ютер – електронний пристрій, призначений для обробки інформації. Відповідно, він її оцифровує, тобто виражає інформацію у цифрах [183, с. 238]. Таким чином недоцільно використовувати прикметник «цифровий». По-друге, основною метою документа, як джерела доказу є збереження та передача інформації. Тому, до документів відносяться як текстові документи, так і фотографії, відео- та звукозаписи, вебсайти, голосові повідомлення та ін. Отже, так як головним у них є інформація, а не матеріальний носій, то відомості в електронній формі повинні визнаватись електронними документами. Вказане дає можливість використовувати електронні документи та не акцентувати на фізичному носії інформації як матеріальному об’єкті.

З урахуванням наведеного пропонуємо доповнити КПК ст. 99-1 під назвою «Електронні документи», а ч. 1 даної статті викласти у такій редакції: «Електронним документом є відомості в електронній формі які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження».

Використання законодавчо закріпленого у Законі України «Про електронні документи та електронний документообіг» визначення електронного документа неможливе у кримінальній процесуальній діяльності. Електронному документу притаманна наявність певних реквізитів, проте вона не є обов’язковою для усіх них. У порядку здійснення цивільно-правових відносин, ряд правочинів визнається недійсними й не мають юридичної сили без таких обов’язкових реквізитів документа (дата складання, сторони та умови угоди, електронний підпис). Проте всі інші електронні документи існують без основних реквізитів й можуть бути використані як джерело доказу [186, с. 91].

Електронні документи, які не регулюються Законом України «Про електронні документи та електронний документообіг» не мають реквізитів. Відсутність обов’язкових реквізитів не впливає на їх доказове значення у кримінальному провадженні.

Загальними ознаками, тобто такими, які присутні у кожному електронному документі є: формат і структура даних, які його складають, наявність (відсутність) певних реквізитів, візуальна форма представлення; окремими ознаками, які можуть існувати в деяких електронних документах є: конкретні електронні дані, програмні, програмно-апаратні і апаратні засоби, методи його підготовки, створення, передачі, перевірки цілісності; параметр криптографічного алгоритму формування електронного цифрового підпису, який відомий лише конкретній особі [266, с. 14].

С.Й. Гонгало зазначив, що основними ознаками документа завжди є: а) інформація, б) носій (матеріал документа), та в) письмо (символи, знаки) [91, с. 22]. Однак, у таких електронних документів є свої особливості, які необхідно враховувати.

Серед загальних ознак електронних документів фахівці вказують такі:

– існують у нематеріальному вигляді;

– створюються людиною, або комп'ютерною системою;

– не можуть існувати поза межами фізичного носія або каналу зв'язку;

– не мають нерозривного зв'язку з матеріальним носієм;

– вільно переміщуються в електронній мережі;

– сприйняття та дослідження таких документів може здійснюватися лише з використанням спеціальних програм та пристроїв;

– потребують спеціального порядку збирання, перевірки й оцінки;

– мають здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати своїх характеристик;

– можливість дистанційного внесення змін до них та їх знищення [34, с. 252].

На думку А.Ю. Каламайко до ознак електронного документа слід віднести наступні:

– неможливість безпосереднього сприйняття інформації, що обумовлює необхідність використання технічних та програмних засобів для одержання відомостей;

– наявність технічного носія інформації, який може бути використаний багаторазово;

– специфічний процес створення та зберігання інформації, який надає можливість легко змінювати носій без втрати змісту і навпаки, надає можливість внесення змін до змісту без залишення слідів на носієві;

– відсутність поняття «оригіналу» електронних засобів доказування в силу повної ідентичності електронних копій;

– наявність специфічних «реквізитів», так званих метаданих — інформації технічного характеру, яка закодована всередині файлів [118, с.50].

На нашу думку, до основних особливостей електронного документа, в першу чергу, слід віднести обов'язкову складову будь-якого електронного документа – метадані.

«Метадані» це термін, який походить від англійського слова «metadata» (*meta, грец. – «після», data, англ. – «інформація», «відомості», «дані»)* означає дослівно «дані про дані».

Е. Кейсі пояснює, що усі електронні документи у тій чи іншій формі містять метадані. Електронний документ повинен мати метадані для того, щоб інтерпретувати мету створення такого документа. Метадані можуть автоматично створюватися програмним забезпеченням, за допомогою якого створюється електронний документ, або вноситися особисто людиною, яка створила такий документ. До такої інформації входить: коли і як був створений документ (час і дата), тип файлу, назва автора (хоча це не завжди правдиво), місце з якого файл був відкритий або збережений, дата та час останньої зміни, друку та іншу інформацію[2, с. 27; 181, с. 81]. Даний перелік є необмеженим та залежить від типу файлу, програми-створювача документа, тощо.

Під час проведення комп'ютерно-технічної експертизи експерти часто використовують термін «метадані», однак у Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої Наказом Міністерства юстиції України №53/5 від 08 жовтня 1998 року [114] такого терміну не передбачено. Під час проведення комп'ютерно-технічної експертизи,

на розгляд експерту покладаються питання щодо технології та хронології створення електронного документа, атрибутів файлу тощо [181, с. 81].

На нашу думку, необхідно використовувати термін «метадані», та додати можливість його дослідження в перелік орієнтованих питань експертизи. Даний термін відповідає сучасним досягненням науки та використовується у міжнародній практиці.

Серед нормативно-правових актів України визначення поняття «метадані» зустрічається у постанові КМУ №833 від 10.11.2017 року «Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі», відповідно до якого метадані – структуровані дані, які містять відомості про подію, зафіксовану технічними засобами, що дають змогу здійснювати фотозйомку або відеозапис подій, що містять ознаки адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху, в автоматичному режимі (далі – технічні засоби), характеристики зафіксованого транспортного засобу, необхідні для його ідентифікації, параметри функціонування цих технічних засобів, а також інші дані для обліку, пошуку, оцінки та управління цими відомостями [175].

Метадані мають велике значення під час досудового розслідування та можуть бути використані для перевірки електронного доказу на його повноту і цілісність з однієї сторони та допустимість, належність – з іншої.

Наприклад, вироком Тячівського районного суду Закарпатської області, докази визнано недопустимими, у зв'язку з тим, що відповідно до висновку комплексної експертизи відео-звукозапису та комп'ютерної техніки стверджується, що відеограма 1 та відеофонограма 2 піддавались комп'ютерній обробці, про що свідчать записи «VirtualDub build 35491/release» у метаданих файлів [83].

З однієї сторони простому користувачу внести зміни до таких системних записів неможливо, що практично унеможливлює підробку такої інформації про документ [186, с. 92]. З іншої – метадані не є надійним джерелом інформації. Збій чи дефект програми, комп'ютерний вірус чи інша проблема, пов'язана з

технічним пристроєм може вплинути на зміну чи видалення метаданих. Для досвідчених програмістів не є проблемою вплинути та видозмінити цю інформацію. На даний час кількість хакерів збільшується, а інформація про спосіб зміни IP-адреси (визначення терміну у додатку Г) є у вільному доступі у мережі Інтернет. Тому, використовувати лише метадані як визначальну інформацію про електронний документ не цілком вірно. Особливо, якщо такий електронний документ виступає доказом кримінального правопорушення, пов'язаного з незаконним втручанням електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку чи іншими злочинами пов'язаними з використанням комп'ютерної техніки [181, с. 81].

Так, наприклад, Ленінський районний суд м. Севастополя дійшов висновку, що метадані графічних файлів (EXIF) можуть бути піддані редагуванню без порушення цілісності зображення, через що вони не дозволяють з необхідною достовірністю ідентифікувати автора або фотокамеру, за допомогою якої зображення було виготовлено [188].

У іншому рішенні, Індустріальний районний суд м. Дніпропетровська зазначив, що встановити значення точного часу створення файлів не представляється можливим через те, що фахівцеві невідомі настройки часу і часового поясу телефону, встановлені в момент проведення зйомки, а також суб'єктивності установок і налаштувань, виконаних користувачем телефону [69].

У зв'язку з цим, пропонуємо авторське визначення, метаданих електронного документа – структуровані закодовані дані, які характеризують електронний документ та мають доказове значення у кримінальному провадженні.

Другою особливістю електронного документа є його форма. Не слід зосереджувати увагу лише на матеріальній стороні електронного документа. Матеріальний носій – тільки спосіб збереження та передачі інформації. Окрім того, електронний документ може також зберігатися у мережі Інтернет (онлайн).

Основну роль в електронному документі відіграє інформація та її зміст. Аналогічної думки дотримується О.С. Гиляка, який вважає, що суть документа полягає в інформації, а не у його носії [87, с. 34]. Д.М. Цехан зазначає, що необхідно оцінювати власне інформацію, а не матеріальний об’єкт на якому вона зафіксована [257, с. 257].

Якщо вважати, що первинне значення має носій, то до таких документів не може бути віднесено документ, в якому інформація не може існувати окремо від матеріального носія. Це неминуче тягне за собою виключення з ряду документів будь-яких документів, переданих і отриманих з використанням електронних засобів зв'язку. Такі документи (наприклад, електронні повідомлення) самі по собі вже є матеріальними об'єктами, незалежно від того, на який носій вони записані після отримання з використанням електронних засобів зв'язку: дискети або компакт-диски. Для того, щоб їх можна було кваліфікувати як документи, матеріальний носій не має суттєвого значення [110, с. 41].

Інформація, яка поширюється через мережу Інтернет, існує на носії інформації може бути доказовою. Як свідчить слідча практика, досить часто виникає можливість виявляти правоохоронним органам ознаки вчинення кримінального правопорушення певними особами, переглядаючи відкриті офіційні сайти інших держав. Наприклад, державний службовець, який за законодавством України не має права бути підприємцем, закордоном зареєстрований як власник комерційної структури. Джерелом у цьому випадку є офіційний реєстр органу виконавчої влади іноземної держави. В такому випадку правоохоронні органи ставлять слушне запитання, чи варто ускладнювати процедуру притягнення до відповідальності особи за вчинення корупційного правопорушення надсиланням запиту до іноземної держави про надання письмового варіанту документа (виписки з Реєстру підприємців), чи достатньо електронної інформації, яку можна одержувати з відкритих іноземних джерел [38, с. 124].

Носієм інформації є матеріальний об'єкт, призначений для запису, передачі та зберігання інформації. Носії інформації поділяються на: паперові (рукописні,

друковані), з магнітним або оптичним записом (магнітні стрічки та диски, оптичні CD та DVD диски, магнітооптичні компакт-диски), електронні (карта пам’яті, флеш пам’ять, сервер та ін.). Наявність різних видів носіїв інформації не виключає їх взаємоіснування, а лише доповнює можливості їх використання [195, с. 412].

Д.М. Цехан зазначає, що ІТ характеризуються високою здатністю до інтеграції і створення абсолютно нових техніко-соціальних середовищ, наприклад, об’єднання персональних комп’ютерів у мережу і, як наслідок, виникнення Інтернету. У науковій літературі для позначення техніко-соціального середовища, яке створене на базі високих ІТ, використовується термін «кіберпростір» [258, с. 30]

Електронний документ за своїм змістом є двійковим комп’ютерниим кодом, який створений з використанням технічних засобів та існує на фізичних носіях інформації. Він існує у нематеріальній формі. Специфічна форма електронного документа визначає технологічні особливості таких документів, які необхідно враховувати при їх використанні в різних сферах.

З однієї сторони відсутність матеріальної форми існування зумовлює нерозривний зв'язок електронного документа із технічним носієм, на якому такий документ зберігається. Електронний доказ не може існувати поза межами технічного носія. Проте, разом з цим, електронний документ не має нерозривного зв’язку із певним технічним носієм, може вільно переміщуватися в електронній мережі без технічного носія та існувати одночасно на кількох технічних носіях [255, с. 81].

Електронна форма представлення інформації – спосіб документування інформації, що означає створення, запис, передачу або збереження інформації у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних або інших засобів, здатних до відтворення, передачі чи зберігання інформації. Електронною формою представлення інформації вважається документування інформації, що дає змогу її відтворювати у візуальній формі, придатній для сприйняття людиною [170].

Відтворення електронного документа у візуальній формі за допомогою програмного забезпечення з використанням технічних пристроїв є ще однією особливістю. Без розкодування комп’ютером, інформація буде лише набором незрозумілих чисел, символів. Вивчення і дослідження електронного документа можливе лише після його сприйняття людиною.

Як зазначає Т.Е. Кукарникова, представлений на екрані або роздрукований документ кардинально відрізняється від вихідного електронного, хоча і сформований комп'ютером на його основі. Єдиний по структурі паперовий документ в електронному вигляді може зберігатися у вигляді декількох окремих компонентів: графічних, текстових, бази даних, електронних таблиць і т.д. Документ виходить їх комбінацією [136, с. 56].

Візуалізація електронного документа полягає у використанні спеціальних пристроїв технічних програм для відтворення на екрані відео, аудіо файлів, зображень, тексту, тощо.

Таким чином, до особливих ознак, притаманних електронному документу як доказу у кримінальному провадженні можна віднести наступні:

— наявність метаданих, що характеризують документ та є його обов’язковим елементом;

— існування в нематеріальній електронній формі;

— використання спеціального програмного забезпечення та технічних засобів для візуалізації.

Отже, на даний час, з урахуванням норм КПК електронний документ може бути різновидом документа або речового доказу. У зв’язку з відсутністю єдиного законодавчо-закріпленого терміну «електронного документа» в науці існує велика кількість варіантів як щодо самого терміну, так і визначень даного поняття.

1.3. Класифікація електронних документів у кримінальному провадженні

Потреба в класифікації доказів у кримінальному провадженні диктується складністю процесу доказування, формуванням доказів та їх процесуальних

джерел. Сукупність доказів допомагає швидко, повно і неупереджено встановити усі обставини лише в тому випадку, коли вона утворює систему доказів, яка здатна встановити усі елементи предмету доказування.

Класифікація доказів – це їх поділ з метою дослідження складових частин цієї системи. Окрім теоретичного, класифікація доказів має і практичне значення. Завдяки їй з'ясовуються особливості збирання, перевірки та оцінки доказів, їх значущість для доведення тих чи інших обставин, що входять до предмета доказування. Таке багатопланове значення класифікації доказів свідчить, що провести поділ доказів за однією ознакою чи властивістю неможливо [211, с. 17].

Теоретичне та практичне значення класифікації електронних документів полягає у тому, що вона допомагає правильно використовувати їх як докази, сприяє збиранню, перевірці (дослідженню їх для встановлення наявності чи відсутності ознак втручання) та оперуванню ними в процесі доказування в ході розслідування та судового розгляду кримінальних проваджень [89, с. 33].

Найбільш поширеною серед науковців є така класифікація доказів: залежно від відношення до обставини, що підлягає доказуванню: прямі та непрямі; залежно від обставин, що обтяжують чи пом'якшують відповідальність: обвинувальні та виправдувальні; за джерелом відомостей (за цією обставиною класифікуються як докази, так і їх джерела): первинні та похідні [123, с. 39-40].

У практиці використовуються різні класифікації документів. Так, за способом виконання розрізняють рукописні, машинописні документи, документи, виконані поліграфічними способами, виготовлені за допомогою комп'ютерних принтерів, різних розмножувальних апаратів і т. п., за джерелом – офіційні та приватні, за способом передачі інформації – відкриті та кодовані, за юридичною природою – справжні та підроблені. Підроблений документ у кримінальному провадженні завжди фігурує як речовий доказ, тоді як справжній документ може таким бути, а може і не бути [39, с. 164].

Одним з перших почав досліджувати проблематику нетрадиційних засобів доказування проф. О.Т. Боннер. Хоча вчений не проводить чіткої класифікації сучасних джерел інформації, що можуть слугувати доказами в суді, проте вказує

на окремі найбільш поширені їхні види. До таких автор відносить: 1) аудіо- та відеозаписи; 2) електронні документи; 3) відомості, отримані з глобальних інформаційних систем (зокрема, мережі Інтернет); 4) електронну пошту; 5) свідчення (показання) спеціальних технічних засобів (напр., прилади обліку витрат електроенергії, води, газу, тепла; прилади визначення швидкості транспортного засобу чи ступеня алкогольного сп'яніння водія тощо); 6) засоби «електронного судочинства» (зокрема, відеоконференції, офіційні вебсайти судових органів, листування з судовими органами за допомогою електронної пошти, автоматизовані судові інформаційні системи та ін.) [51, с. 46-48].

О.В. Шведова пропонує поділяти електронні документи на дві групи. До першої групи слід відносити документи, які можуть бути перенесені на фізичний носій інформації та не мають юридичної сили. До другої групи слід віднести документи, які мають юридичну силу без їх перенесення на фізичний носій та мають електронний цифровий підпис, який надає можливість ідентифікувати особу, яка створила документ [266].

Гонгало С.Й. вважає, що з точки зору використання електронного документа як доказу, то його можна поділити на дві групи – юридичні та технічні. Юридичні документи містять передбачені законом реквізити, складаються уповноваженою на те особою та мають юридичну силу. До технічних документів слід відносити документи, які не мають юридичної сили [90].

Ми погоджуємося з таким поділом електронних документів та вважаємо, що його доцільно використовувати при обранні нормативно-правових актів, якими регулюються використання електронного документа.

Враховуючи основні терміни та принципи, визначені Законом України «Про електронні документи та електронний документообіг» [169] та Законом України «Про електронну комерцію» [170], усі електронні документи, створені на основі цих законів мають юридичну силу. Проте, якщо організаційно-правові засади використання таких електронних документів встановлено, то у технічних електронних документів немає законодавчого врегулювання та закріплення. Під

час здійснення досудового розслідування саме технічні електронні документи використовуються найчастіше.

До так званих технічних електронних документів, що не мають юридичної сили можна віднести: фотографії та зображення, відео- та аудіозаписи, вебсайти, облікові записи у соціальній мережі, дані геолокації, голосові, мультимедійні та інші повідомлення, історія вхідних та вихідних викликів, записи, що містяться у нотатках, диктофоні, чернетках й навіть відмітки у календарях, у випадку якщо вони можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До юридичних електронних документів належать договори, різного виду звіти, акти, свідоцтва, витяги, протоколи, електронні платіжки та інші документи, які створюються в порядку електронного документообігу між державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності [186, с. 93-94].

Ми погоджуємося з думкою С.Й. Гонгало про те, що ***за стадіями виготовлення електронні документи поділяються на оригінали, дублікати, копії та витяги.*** Однак не вважаємо, що цей поділ є досить умовним [89, с. 34], оскільки в деяких випадках можливо встановити оригінал електронного документа.

Встановлення оригіналу чи копії електронного документа необхідне для дотримання безпосередності дослідження показань, речей та документів, як однієї із засад КПК.

У ст. 7 Закону України «Про електронні документи та електронний документообіг» передбачено, що оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис». Оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис». У разі

надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу [169].

Оригінал електронного документа повинен: давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії. Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Правовий статус електронного документа визначений у ст. 8 Закону України «Про електронні документи та електронний документообіг». Електронний документ є допустимим доказом, не зважаючи на його електронну форму та має встановлену юридичну сили [169].

Таким чином, Законом України «Про електронні документи та електронний документообіг» встановлено, які юридичні документи є оригіналами, а які є копіями, порядок виготовлення витягу, зберігання, передавання таких документів.

Складнішим є питання визначення оригіналу та копії технічних електронних документів. Для того, щоб встановити яким саме повинен бути оригінал технічного електронного документа слід врахувати засади кримінального процесуального закону та вимоги щодо належності, допустимості, достатності та достовірності доказів.

Згідно з ч. 3 ст. 99 КПК, оригіналом та дублікатом документа. Відповідно оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке ж значення, як документу.

Оригіналом електронного технічного документа є той, який створений та зберігається на первинному носії інформації. Наприклад, оригінал відеозапису з камер відеоспостереження зберігається на носії інформації, на який записується

відео. Копією такого відеозапису є його переміщення на інший носій інформації. Однак, у деяких випадках встановити оригінал чи копію електронного документа неможливо, оскільки інформація може повністю дублюватися під час копіювання, та відрізнятися лише датою та часом створення, що може становити труднощі під час визначення оригіналу. *Так, Верховний Суд зазначив, що відповідно до ст. 7 Закону України «Про електронні документи та електронний документообіг», у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа [162].* У такому випадку, вважаємо що доцільно визнавати оригіналом той електронний документ, який має найбільш ранні дату та час створення та копіювання.

З урахуванням вищенаведеного, пропонуємо викласти ч. 3 ст. 99-1 КПК наступного змісту: Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал електронного документа на фізичному носії інформації. Оригіналом електронного документа є його відображення, яке зберігається на первинному фізичному носії інформації. Якщо один і той самий електронний документ зберігається на кількох носіях інформації, то оригіналом є електронний документ, дата створення або дата копіювання якого є більш ранньою.

Відповідно до ч. 4 ст. 99 КПК, дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

Вважаємо, що термін «дублікат» для електронного документа використовувати недоцільно, оскільки, в більшості випадків, слідчий, дізнавач, прокурор за участі спеціаліста здійснюють копіювання інформації за допомогою спеціального програмного забезпечення, а не ідентичним до створення способом. Тому, пропонуємо викласти ч.4 ст.99-1 КПК наступним чином: Копія

електронного документа, виготовлена слідчим, дізнавачем, прокурором за участі спеціаліста визнається судом як оригінал електронного документа.

На нашу думку, роздруківка веб-сторінки, частини відео, фото чи іншого файлу не може бути визнана ні оригіналом, ні копією електронного документа та самостійно не може бути використана як доказ.

Для дублювання інформації, яка міститься в мережі Інтернет, виготовлення копії електронного документа з комп'ютера чи іншого пристрою необхідно залучати спеціаліста. Візуалізована у паперовій формі сторінка може бути використана лише як додаток до проведеної слідчої (розшукової) дії. Правильне виготовлення копії електронного документа забезпечує його допустимість під час перевірки доказів у суді.

Наприклад, Зарічний районний суд м. Суми визнав роздруківки місця знаходження радіоелектронного засобу неналежними і недопустимими доказами. В обґрунтуванні суд зазначив, що відсутність первинних носіїв та вказаних відомостей в роздруківці та протоколі ставить під сумнів достовірність інформації, що міститься в них, та дає суду підстави стверджувати, що втручання у приватне спілкування гр. П. відбулось не у спосіб, що встановлений КПК. Всупереч зазначеним вимогам кримінального процесуального закону, у цьому випадку, на виконання доручення прокурора було надано не протокол, а роздруківку у формі таблиць, складених у довільній формі, в яких відсутня: інформація про володільця (оператора чи провайдера, з мереж якого було знято інформацію); відомості щодо технічних засобів, що застосовувались для зняття інформації, а також первинні носії, на яких повинна зберігатися знята з телекомунікаційних мереж інформація, що зберігаються до набрання вироком суду законної сили; дата самої роздруківки та прізвище, ім'я, по батькові, посада і підпис особи, яка виготовляла роздруківку; відомості про наявність ухвали слідчого судді про надання дозволу на зняття інформації з транспортних телекомунікаційних мереж та дата, номер і зміст доручення прокурора, на виконання якого здійснювались негласні слідчі (розшукові) заходи. Суд визнав гр. П. невинуватим у пред'явленому обвинуваченні у зв'язку з

недоведеністю його вини у вчиненні кримінальних правопорушень та виправдав [67].

У іншій справі, Апеляційний суд м. Києва зазначив, що не можуть бути джерелом доказування та є недопустимими доказами фотокартки та скріншоти, отримані внаслідок моніторингу сторінок користувачів, яких орган досудового розслідування ототожнює з представниками ДНР, у соціальних мережах «Вконтакте» і «Одноклассники», оскільки достовірність інформації, яка в них міститься, викликає обґрунтовані сумніви та вони отримані у спосіб, не передбачений кримінальним процесуальним законом [222].

У абз. 10 п. 46 Постанови Пленуму Вищого Господарського суду України №12 «Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності» від 17.10.2012 року передбачено, що роздруківки Інтернет-сторінок (веб-сторінок) самі по собі не можуть бути доказом у справі [168].

Відповідно до ч. 3, ч.4, ст. 99 КПК сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції, узагальнення документів, які незручно повністю досліджувати в суді, а на вимогу суду – зобов’язані надати документи у повному обсязі.

Оскільки електронний документ може містити великий обсяг інформації, то доцільно створювати витяги, узагальнення, компіляції. Витягом, компіляцією чи узагальненням електронного документа є копіювання та виділення за допомогою технічних пристроїв частини інформації, яка встановлює наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Витяг із електронного документа — це певна частина змісту електронного документа, яка може підтверджувати чи спростовувати відомості, які підлягають доказуванню. У витязі з електронного документа, частина інформації та зміст ідентично відтворюються з основного документа.

Узагальнення та компіляція електронного документа, на нашу думку, необхідна тоді, коли уся інформація є важливою та не підлягає окремому виділенню частини. Обсяг та форма такого виокремлення інформації чітко не встановлені та фактично визначаються за внутрішнім переконанням особи, яка її проводить. Головним завданням є відсіяти інформацію, яка не є суттєвою та виявити інформацію, яка має значення під час доказування. Наприклад, вирізання частини звукозапису чи відеозапису, збільшення частини фотографії чи зображення, узагальнення змісту сторінки вебсайту тощо. Ця дія є суб'єктивною, тому оцінити правильність складання скороченого чи узагальненого електронного документа може лише суд. Таким чином, якщо зроблено витяг, компіляцію чи узагальнення електронного документа, то його разом із повним за обсягом і змістом оригіналом необхідно долучати до матеріалів кримінального провадження.

На підставі викладеного, пропонуємо викласти ч. 6 ст. 99-1 КПК у наступній формі: Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції, узагальнення електронного документа, які незручно повністю досліджувати в суді разом з електронним документом у повному обсязі.

Одним із найскладніших є спосіб ***класифікації електронних документів за комбінацією метаданих,*** тобто характеристиками технологічних процесів, які необхідні для візуалізації. Такі складнощі пов'язані з великою кількістю різноманітних структур, типів і форматів даних, у тому числі з їх взаємозв'язками в межах одного документа. Для класифікації зазвичай пропонують поділ електронних документів залежно від комбінації метаданих: однорангові – документи, які складаються з ідентичного один одному типу електронних даних, об'єднаних в одну структуру, записаних в один файл наперед визначеного формату, наприклад: *.wav, *.gif; 2) дворангові – це документи, що складаються з кількох типів даних, об'єднаних в одну структуру та записаних в окремий файл наперед визначеного формату; 3) три ранговими називають документи, які не лише складаються з кількох типів даних і об'єднані кількома структурами, а й

записані в один файл; 4) чотири рангові ж складаються з кількох типів, які об'єднані в кілька структур і записані в певну кількість структур наперед відомого загального формату, наприклад: БД Phara DOX; 5) п'ятирангові документи — це саме ті документи, що мають декілька типів, об'єднаних у певну кількість структур, записаних файлами у різних форматах. Яскравим прикладом п'ятирангового документа є гіпертекст [92, с. 96].

За доступом до метаданих електронних документів можна поділити на відкриті та приховані. До відкритих метаданих можна віднести ті, які звичайний користувач створює самостійно або може побачити за допомогою перевірки властивостей документа. Наприклад, до них можна віднести дату та час створення, зміни, якщо це електронний лист, то ім'я адресата, дату надсилання документу тощо. Приховані метадані доступні користувачеві лише за допомогою використання спеціального технічного забезпечення та програм. Встановлення прихованих метаданих під час проведення експертизи електронного документа дозволяє встановити так звані «електронні сліди» створення, редагування, видалення чи його зміни [178, с. 44].

За ступенем захисту електронні документи можна поділити на відкриті та закриті. Для захисту електронних документів існує велика кількість спеціальних засобів: електронний цифровий підпис шифрування поштових відправлень і мережевого трафіку, різноманітні системи захисту від несанкціонованого доступу в мережах, а також установка пароля на документі тощо [136, с. 73].

За джерелом походження виділяють електронні документи, які створені фізичною особою та електронним середовищем [118, с. 10; 136, с. 69]. Автоматично створюються кеш-файли, cookie-файли, метадані за замовчуванням налаштувань програми тощо. Більшість електронних документів створюються користувачем шляхом введення інформації особисто.

Пошук інформації у мережі Інтернет здійснюється за допомогою браузера (визначення терміну у додатку Г). Відвідані вебсайти, їх вміст, який було переглянуто, зображення, відеозаписи зберігаються у тимчасових кешах

(визначення терміну у додатку Г). Головне завдання кешу – це прискорення перегляду раніше відвіданих вебсайтів. Таким чином, після повторного відкриття вебсайту, який раніше відвідувався – браузер завантажує дані безпосередньо з жорсткого диску комп'ютера, а не з мережі. Деякі версії програмного забезпечення зберігають таку інформацію в більш ніж одній локальній папці комп'ютера.

Наприклад, одним із важливих доказів, збережених на мобільних телефонах марки «iPhone», є останні налаштування GPS (визначення терміну у додатку Г), які зберігаються в кеші, коли GPS включений. Недосвідчений експерт може запустити додаток «Google Maps» на пристрої для відновлення адрес, за якими здійснювався пошук, випадково активувати GPS, знищити останні GPS налаштування й замінити їх поточними. Ці, здавалося б, не шкідливі дії також завантажать графічні зображення карти відносно поточної позиції, що перезапише дані в кеш. Внаслідок цього буде знищена уся інформація по GPS, а інші карти, що залишились, можуть бути визнані недопустимими та відхилені під час дослідження доказів у суді.

Також, браузер «Safari» перезавантажує сторінки, які були раніше завантажені, у будь-який раз, коли завантажується додаток. Якщо одна зі сторінок належала до сторінок певного форуму або іншого вебсайту для окремої спільноти людей, кеш може стати важливим місцем зберігання корисних доказів. Але запуск «Safari» може перезавантажити сторінку та переадресувати експерта до головної сторінки сайту, а отже перезаписати дані кешу, які містили докази [144, с. 92].

Перевірка кешу на наявність файлів та даних найчастіше використовується експертами під час дослідження електронних документів. Ця інформація дає можливість встановити які вебсайти відвідувались, які файли були завантажені та вирішити інші питання, які були поставлені експерту слідчим, дізнавачем чи судом.

Окрім кеш-файлів, браузер також може зберігати cookie-файли (визначення терміну у додатку Г). До таких файлів можна віднести збереження паролю та

логіну особистої сторінки, вподобань користувача [178, с. 45]. Таким чином, інтернет-магазини вивчають вподобання відвідувачів вебсайту та пропонують відповідні послуги, товари для замовлення.

Збереження cookie-файлів дає можливість отримати доступ до облікового запису, електронної сторінки, вебсайту без подолання логічного захисту (логіна та пароля) та застосування спеціального програмного забезпечення.

У клопотаннях про тимчасовий доступ до речей та документів слідчі обов'язково мають вказати перелік документів, тимчасовий доступ до яких планується отримати (п.3 ч.2 ст.160 КПК). При аналізі судової практики, слідчі, за погодженням з прокурором звертаються до суду для отримання інформації про дані з cookie-файлів, що зберігаються на пристрої, в тому числі ідентифікатори і налаштування cookie-файлів [240, 241], cookie-файли для користування поштовою скринькою [225, 246] тощо.

Особливість обміну електронними документами полягає в тому, що інформація копіюється і повторюється на безлічі носіїв. Наприклад, електронний лист створюється на комп'ютері користувача, потім при відправці він зберігається на сервері вихідної пошти компанії, в якій працює користувач, потім потрапляє на сервер вхідних повідомлень адресата, потім безпосередньо в комп'ютер адресата. Як наслідок, електронні документи набагато більш стійкі до пошкодження або знищення, ніж паперові. Видалення документа користувачем операційної системи в кошик зовсім не означає його остаточного зникнення. Інформація зберігається в іншому вигляді й при необхідності може бути відновлена як вихідний документ.

Класифікацію електронних документів можна здійснити за їх місцем розташуванням: комп'ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер за своєю природою є різновидами комп'ютера. Інформація про місцезнаходження електронного документа необхідна під час отримання санкціонованого доступу до нього та встановлення його особливостей, які створюються внаслідок існування на певному технічному носії інформації.

В.В. Білоус вказує, що завдяки компактності, полі функціональності, придатності для інсталяції великої кількості зручних і корисних додатків та сукупності інших конкурентних переваг смартфонів, протягом 20 останніх років, обсяги постачань цих інноваційних засобів зросли. Це призвело до витіснення з обігу традиційних (аналогових та цифрових) фотокамер і мобільних телефонів й домінування у мережі Інтернет аудіовізуальних матеріалів, відзнятих з використанням саме смартфонів [46, с. 135]. Як показує звіт «DIGITAL 2021: Global Digital Overview», кількість користувачів мобільних пристроїв станом на січень 2021 року становить 5,22 млрд осіб, або дорівнює 66,6% усього населення світу (7,83 млрд осіб) [6].

У сучасному смартфоні зберігається інформація про час і тривалість дзвінків, приймання та відправлення текстових повідомлень, номери телефонів абонентів, фотографії, відеозаписи, аудіозаписи створені користувачем, отримані від іншого користувача або збережені з іншого пристрою (у т.ч. Інтернет-мережі), історія користування веб-браузером тощо. Популярні додатки до смартфонів дають можливість спілкуватись з іншими користувачами таких додатків за допомогою дзвінків, обміну повідомленнями, зображень, відео-, аудіофайлів використовуючи при цьому ресурси Інтернет-мережі, а не мобільного зв'язку.

Наприклад, старший слідчий, обґрунтовуючи клопотання про тимчасовий доступ до речей та документів, вказав, що погодження злочинних дій відбувалося і за допомогою здійснення листування у програмах з функціями відправлення текстових повідомлень, зображень та відеозображень: Skype, Viber, WhatsApp, ooVoo, Line, GoogleTalk, Facebook Messenger, iMessages, ChatOn, ICQ, Mail@Агент, GaduGadu, Однокласники, Вконтакте, Microsoft Outlook, а також за допомогою особистої електронної пошти та інших подібних програм[238].

Ми не погоджуємося з думкою Т.Е. Кукарникової, яка вважає що не існує відмінностей в електронних документах, якими можна було б обґрунтувати виділення будь-яких електронних документів (наприклад, аудіо- та відеозаписи)

в самостійний підвид, через те, що абсолютно байдуже, яка інформація (текст, відеозапис, аудіозапис і т. п.) записана на машинному носії [136, с. 63].

За формою електронні документи можна поділити на відеозаписи, аудіозаписи, електронні повідомлення, вебсайти та інформацію у електронній формі [118, с.10].

Згідно з опитуванням, під час досудового розслідування працівникам підрозділів Національної поліції найчастіше зустрічались наступні електронні документи: цифрові фотографії та зображення – 28,2%, відеозаписи – 25,8%, аудіозаписи – 19,1%, вебсайти – 12,5%, електронні повідомлення (у т.ч. електронна пошта, соціальні месенджери) – 11,3%, дані геолокації – 2,5% (додаток А).

Відеозапис як електронний документ містить візуальні дані різного характеру з аудіозаписом, або без нього. Перегляд якісного відеозапису дає можливість слідчому, дізнавачу, прокурору, суду та іншим учасникам кримінального провадження більш повно встановити обставини події, які відбувались [50, с. 80-81].

У звукозаписах доказова інформація виражається звуковою формою. Особливістю звукозаписів є те, що вони можуть містити відомості не тільки про доказувані дії чи бездіяльність, але й про дії, які передували їм, а також про розмови, які їх супроводжували та інші компоненти (музика, вигуки, інші супутні звуки та шуми).

Однією з особливостей відео- та звукозаписів є їх динамічність. Відбувається безперервне відображення, збереження та наступне відтворення, а також зорове та слухове сприйняття учасниками процесу обставин дійсності в якісних, кількісних та просторових змінах, що відбувались з людьми та предметами матеріального світу протягом певного проміжку часу. Саме фіксація в динаміці всіх відомостей про обставини кримінального правопорушення надає можливість отримати найповнішу інформацію про них слідчому, дізнавачу, суду та іншим особам, які беруть участь у кримінальному провадженні.

У письмових та речових доказах інформація про обставини кримінального правопорушення зазвичай наявна у статичному вигляді, адже під час їх дослідження учасниками кримінального провадження необхідно здійснити інтелектуальну діяльність, застосувати уяву для відтворення обставин кримінального правопорушення у власній свідомості. На відміну від показань, відтворення звуко- та відеозаписів дозволяє встановити обставини кримінального правопорушення в точній послідовності, в якій вони мали місце, що забезпечує сприйняття подій слідчим, дізнавачем, прокурором, судом, без суб'єктивного сприйняття та відтворення іншими особами (свідками, потерпілими та ін.).

Іншими словам, звуко- та відеозаписи, на відміну від показань чи речових доказів, володіють точністю, тобто вони надають можливість слідчому, суду та особам, які беруть участь у провадженні, безпосередньо сприйняти в динаміці обставини, які мали місце в минулому. Сприйняття інформації про обставини кримінального правопорушення в обсязі, наближеному до того, який би ці особи отримали, якби були безпосередніми спостерігачами подій, створює особливий психологічний вплив, результатом якого може стати впевненість, що учасники процесу стали «майже очевидцями», а досліджувані події дійсно мали місце. Саме завдяки вищенаведеному, очевидно, що інформація, зафіксована у звуко- та відеозаписах, під час дослідження може мати особливо переконливий вплив на суд та осіб, які беруть участь у провадженні [50, с. 69-71].

Фотографії, зображення в електронному вигляді також мають безліч позитивних властивостей під час доказування. Зображення зафіксоване статично дає можливість оцінити інформацію, яка має доказове значення у кримінальному провадженні. Сприйняття доказу особисто покращує розуміння ситуації, обстановки та обставин події, які відбулись. Під час огляду фотографії є можливість збільшити, зменшити зображення та привернути увагу до важливих на ній деталей. Метадані, що містяться у файлі цифрової фотографії дають можливість встановити час та дату фотографування та технічний пристрій, за допомогою якого проводилось фотографування.

До однієї з форм електронних документів слід віднести електронні повідомлення. Прикладами електронних повідомлень є СМС-повідомлення, електронні листи з використанням електронної пошти, листування в мобільних додатках тощо. Такі повідомлення, також, можуть бути виділені на підвиди: текстові, голосові та мультимедійні повідомлення [158, с. 83].

До іншої інформації в електронній формі можна віднести інформацію про місцеперебування пристрою. Більшість мобільних телефонів, планшетів, ноутбуків та інших пристроїв обладнані GPS-трекерами. Інформація, яку передає GPS є теж електронним документом [180, с. 351-352].

Місцеперебування пристрою може автоматично зберігатися при використанні певних програм, під час користування картами, здійснення відео та фотозйомки та залежить від налаштувань самого пристрою. Оператори мобільного зв'язку зберігають інформацію про дату, час та тривалість з'єднань в зоні дії базових станцій. Отримання інформації про всіх абонентів, які перебували в зоні дії базових станцій можуть підтвердити чи спростувати місце перебування особи, яка є користувачем пристрою.

Інформація про геолокацію (якщо вона буде в метаданих) може допомогти з максимальною точністю встановити місце запису. Водночас наявність даних про геолокацію залежить від декількох факторів. По-перше, від пристрою, яким була створена фотографія. У деяких камерах або мобільних пристроях може не бути GPS-датчика, який фіксує координати. По-друге, в залежності від бажання користувачів мобільних пристроїв – вони можуть відключити геолокацію з міркувань приватності або зменшення навантажень на акумулятор. По-третє, наявність таких даних залежить від ресурсу, на якому фотографія була опублікована. Соціальні мережі «Facebook», «Twitter» або «Instagram» видаляють метадані з фотографій під час їх завантаження на свої сервери. Але в той же час вони можуть безпосередньо показувати інформацію про місцезнаходження автора фотографії (а також поста/твіти), якщо він дав доступ до GPS-датчика свого мобільного пристрою [150].

Інформація про місце перебування особи може використовуватися як обвинувальний або виправдувальний (алібі) доказ. Однак, слід ретельно перевіряти такі відомості, адже однієї геолокації недостатньо для підтвердження того, що особа перебувала в іншому місці під час події кримінального правопорушення.

Наприклад, для приховування вчинених кримінальних правопорушень та створення собі можливого алібі, гр. М. вжив ряд заходів. Розуміючи, що особа, яку він незаконно позбавив волі, є публічною особою та активним користувачем соціальних мереж, з метою маскування своєї злочинної діяльності та введення правоохоронних органів в оману, щодо часу та місця зникнення потерпілого 05.03.2016 року на його сторінці Фейсбук зробив запис «гуляем)) спасибо что приняли», а о 23.27 год. – запис «вечер удался» з геолокацією у м. Одеса та додав фотографію потерпілого, зроблену на його мобільний телефон раніше.

06.03.2016 року о 12.49 год., продовжуючи маскування свої злочинної діяльності з наведених мотивів гр. М. зробив ще один запис на сторінці потерпілого «накрылась зарядка на связи буду завтра».

09.03.2016, перебуваючи на території м. Шарм-ель-Шейх республіки Єгипет, гр. М., продовжуючи маскування свої злочинної діяльності о 19.34 год. на сторінці потерпілого зробив ще один запис «Простите, что подвел вас мои друзья. Пришлось уехать с Украины, не по своей воле! Зато я в безопасности! Не знаю когда вернусь, по возможности, буду отвечать вам.очень хочу обратно на Родину.» та 13.03.2016 року о 13.49 год. на сторінці потерпілого виклав фото торговельного центру «Genena City» у м. Шарм-ель-Шейху, республіки Єгипет та запис «У меня все хорошо, скоро вернусь.извините что подвожу вас!)» [242].

Окрім цього, GPS-трекер може використовуватись як окремий пристрій (годинник, браслет, підвіска, ошийник) для того, щоб відстежити місцеперебування дитини, домашнього улюбленця, встановити місцеперебування транспортного засобу у випадках його викрадення чи незаконного заволодіння. Власник (користувач) такого пристрою може у будь-

який час встановити місцеперебування трекера і, відповідно, особу чи річ, місце перебування яких його цікавить.

Так, правоохоронними органами під час оглянуто інтернет-ресурсу http://server1.gsm-gps.com отримано дані щодо GPS-модуля , яким облаштований автомобіль «Daewoo Lanos», яким раніше користувався померлий та встановлено місцезнаходження автомобіля. На момент огляду автомобіля у ньому перебував гр. Щ, який був затриманий [81].

Електронна пошта досить часто використовується для офіційного листування юридичними та фізичними особами. Також, для передачі повідомлень можуть використовуватись соціальні мережі. За даними опитування компанії «Research & Branding Group», в Україні станом на січень 2020 року 58% від усієї кількості опитаних користується соціальною мережею Facebook, 41% - Youtube, 28% - Instagram, 14% - Telegram, 7% - Вконтакте, 6% - Одноклассники [31]. За допомогою листування, правопорушники мають можливість домовлятися про спільне вчинення кримінального правопорушення, уточнювати деталі, розробляти план його вчинення та приховування. Окрім цього, листування може свідчити про конфліктні відносини, висловлювання образ, шантажу, погроз, приниження честі та гідності.

Обліковий запис може надати фото та інші особисті дані користувача, інформацію про його знайомих, інтереси, захоплення, вивчити особисті якості, погляди, життєві цінності. Надалі така інформація може бути використана під час доказування у кримінальному провадженні [185, с. 97].

Веб-сторінка також може бути доказом і у кримінальних провадженнях. Наприклад, веб-сторінка та/чи обліковий запис може створюватися ймовірним правопорушником для розповсюдження зображень порнографічного характеру (ст.301 КК) [72], шахрайства (ст.190 КК) [79], збуту наркотичних засобів, психотропних речовин або їх аналогів (ст.307, ст.311 КК) [77], укладення домовленості про надання сексуальних послуг, звідництво тощо.

З урахуванням наведеного, пропонуємо викласти ч. 2 ст. 99-1 КПК наступного змісту: до електронних документів можуть належати: текстові

документи, фотографії та інші зображення, аудіо- та відео- записи, електронні повідомлення (смс-повідомлення, електронна пошта, голосові повідомлення), кеш-файли, cookie-файли, вебсайти, дані геолокації та інші відомості в електронній формі.

Отже, підбиваючи підсумок викладеного матеріалу, електронні документи з точки зору використання як доказу, у цьому підрозділі пропонуємо розділити на дві групи юридичні та технічні. За стадіями виготовлення: оригінали, копії та витяги. За комбінацією метаданих: однорангові, дворангові, трирангові, чотирирангові, п’ятирангові. В залежності від доступу до метаданих: з відкритими та прихованими метаданими. За ступенем захисту: відкриті та закриті. За джерелом походження: документи, які створюються користувачем та комп’ютерною системою. За місцем знаходження: комп’ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер, тощо. За формою: відеозаписи, аудіо записи, електронні повідомлення, вебсайти та інформацію в електронній формі.

Висновки до першого розділу

Узагальнення та аналіз нормативно-правових актів, досліджень науковців, наукової літератури дали змогу зробити певні висновки:

1. Встановлено, що електронний документ, як джерело доказу не був предметом комплексного дослідження науковцями та не регламентований на належному рівні у КПК чи інших підзаконних актах. Вказане підтверджує актуальність та вагоме значення проведеного дослідження для розвитку кримінальної процесуальної та криміналістичної науки, покращення роботи слідчих та судових органів.

2. Науковці пропонують різні визначення електронного документа, обґрунтовують необхідність використання відмінних термінів від електронного документа та розглядають електронний документ як різновид речового доказу або документа. Доведено, що у зв’язку з суттєвими відмінностями від речових

доказів та документів, електронний документ повинен бути самостійним джерелом доказів. Наголошено на тому, що електронні документи мають такі особливості, як наявність метаданих, електронна форма, необхідність візуалізації за допомогою спеціальних програм та пристроїв.

3. Проведено узагальнення існуючих класифікацій та запропоновано класифікувати електронні документи за стадіями виготовлення; за комбінацією метаданих; в залежності від доступу до метаданих електронного документа; за ступенем захисту; за джерелом походження; за їх місцем розташування; за формою.

РОЗДІЛ 2
КРИМІНАЛЬНІ ПРОЦЕСУАЛЬНІ ОСНОВИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У ДОКАЗУВАННІ

2.1. Належність електронних документів у кримінальному провадженні

Однією із обов’язкових елементів характеристики доказів є їх належність.

Згідно із ст. 85 КПК, належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів.

М.М. Стоянов визначає належність доказів як властивість доказу, що характеризує зв’язок відомостей, які становлять його зміст, із обставинами, що підлягають доказуванню у кримінальному провадженні [215, с. 9].

О.С. Степанов зазначає, що належність доказів – це один із критеріїв оцінки доказів, що виражає об'єктивний зв'язок будь-яких відомостей, що пов’язані з обставинами конкретного кримінального провадження, а точніше – з обставинами, що входять до предмета доказування [212, с. 10].

Належність доказів – це їх внутрішня властивість, внаслідок якої вони здатні встановити обставини, необхідні для повного і правильного вирішення кримінального провадження.

Під належністю розуміється також наявність зв’язку доказу за змістом із предметом доказування або допоміжними фактами, що слугують для його встановлення [100, с. 53].

Належність відповідає, з одного боку, на питання про наявність зв’язку між змістом і фактом, який підлягає встановленню, з іншого – визначає, наскільки точно встановлено необхідний факт, тобто належний доказ має визначену доказову силу; неналежний – її не має.

За результатами аналізу поглядів процесуалістів і практиків належність доказу – це його можливість встановлювати обставини, що є предметом доказування, через логічний зв'язок між отриманими фактичними даними й тим, що потрібно доказувати. Тільки визначивши, які саме обставини кримінального провадження необхідно встановити, можна вирішити питання про належність конкретних фактичних даних до кримінального провадження, а саме їх належність для вирішення конкретного завдання. Тобто обставини, що підлягають доказуванню, є критерієм належності доказів [100, с. 55].

Як указує О.С. Степанов, практичне значення розкриття змісту поняття належності доказів полягає в тому, що створюється очевидна можливість забезпечити досить повне і всебічне встановлення обставин і фактів, що мають істотне значення у провадженні. З урахуванням критеріїв належності створюється можливість не захаращувати матеріали провадження даними, що не мають відношення до предмета доказування, а отже не ускладнювати розслідування і розгляд в суді кримінального провадження [212, с. 10].

В основу належності доказів покладені об'єктивні зв'язки (причинно-наслідкові, умовно-обумовлені, просторово-часові тощо) між предметами і явищами дійсності. Властивість належності становить логічне відображення будь-якого роду зв'язків. Це – здатність одержуваної інформації бути аргументом у ланцюзі умовиводів, що обґрунтовують наявність або відсутність шуканих фактів. Встановлення належності доказів – не одномоментний акт. На початковому етапі досудового розслідування у слідчого, дізнавача обмаль доказової інформації, тому основний зміст їх діяльності полягає в висуненні та перевірці версій та імовірнісному виведенні належності фактичних даних. На цьому етапі можуть бути зібрані такі відомості про факти, котрі надалі не будуть використані під час прийняття рішень як докази саме через відсутність у них властивості належності. З накопиченням доказів, з'ясування кола обставин, котрі необхідно встановити у кримінальному провадженні, встановлення належності доказів має більш конкретний характер і під час прийняття та обґрунтування рішень повинен бути встановлений безумовний зв'язок доказу з предметом

доказування. Неналежними будуть докази, що містять відомості не про досліджувану подію, а про інший факт, що не входить до обставин, які підлягають доказуванню. Докази будуть неналежними не тільки тоді, коли з'ясується відсутність їх зв'язку з розслідуваною подією, але і коли вони є несправжніми або помилково прийнятими за ті, які підлягають дослідженню [129, с. 185].

Отже, головним для визнання доказу у провадженні має вирішення питання про те, чи належать обставини та факти, для встановлення котрих він використовується, до кола тих, котрі мають істотне значення для правильного розгляду і вирішення кримінального провадження, а отже, підлягають доказуванню. Якщо належать, то відповідають вимозі належності, а якщо не належать, то такій вимозі не відповідають і тому доказуванню не підлягають. При цьому, для визнання доказу у провадженні не має значення, чи входять обставини й фактичні дані, ними встановлені, у коло тих компонентів предмета доказування, що передбачені у КПК, чи сформульовані вони в інших статтях КПК, або належать до числа так званих «проміжних» фактичних даних і обставин, на підставі котрих можуть бути встановлені компоненти предмета доказування, оскільки всі вони у підсумку складають предмет доказування [123, с. 42-43].

Належність документів як доказів визначається як їх змістом, тобто можливістю встановлювати (або спростовувати) факти, котрі мають значення для провадження, так і складанням в належній формі (наприклад, окремі документи повинні бути нотаріально засвідчені, інші, зокрема електронні документи, містити електронно-цифровий підпис) і т.д., що зближує цей критерій доказу з його допустимістю [136, с. 16].

Як зазначає В.В. Вапнярчук, зміст доказу повинен підтверджувати хоча б одну з трьох видів обставин, а саме:

– входять до загального предмета доказування (ст. 91 КПК);

– мають значення доказових фактів (тобто використовуються як аргументи, логічні посилки для встановлення перших);

– мають значення допоміжних фактів, зокрема тих, що стосуються достовірності чи недостовірності, допустимості чи недопустимості отримання інших доказів (приміром, неналежність понятих, які знаходилися під час проведення слідчої (розшукової) дії) [52, с. 242].

Висновок про належність доказу не завжди можна зробити вже при збиранні цього доказу. Зв'язок між змістом доказу та обставинами предмета доказування чи їх відсутністю лише міркується у свідомості суб'єкта доказування [265, с. 67-68].

І справді, справжня належність чи неналежність доказу з'ясовується в той час, коли буде встановлено остаточний предмет доказування. Предмет доказування може змінюватися, і тоді змінюється й належність доказів [265, с. 68]. Як слушно вказує Д.Б. Сергєєва, «тільки визначивши, які саме обставини кримінального провадження необхідно встановити, можна вирішити питання про належність конкретних фактичних даних до кримінального провадження» [196, с. 236].

Прямий доказ перевіряється лише в частині допустимості та достовірності, а в частині належності – не перевіряється, оскільки його змістом і є обставини предмета доказування. Натомість під час перевірки непрямих доказів обов'язковим є з'ясування наявності об'єктивного чи неправдиво приписуваного зв'язку між доказовим фактом, який встановлюється цим не прямим доказом, та обставиною предмета доказування [265, с. 76].

Наприклад, розслідування здійснюється щодо кримінального правопорушення, у якому можливе укладення угоди про визнання винуватості. Якщо такого не станеться, то належними будуть одні докази та їх сукупність, а якщо прокурор та підозрюваний все ж укладуть угоду – то інші, адже предмет доказування вже інший. При цьому подія кримінального правопорушення одна і та ж [265, с. 68-69].

Згідно із ч.1 ст. 91 КПК у кримінальному провадженні підлягають доказуванню наступні обставини:

– подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

– винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

– вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат;

– обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом’якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження;

– обставини, що є підставою для звільнення від кримінальної відповідальності або покарання;

– обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов’язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення;

– обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру [130].

Електронні документи можуть підтверджувати чи спростовувати обставини, які підлягають доказуванню.

Зокрема, з аналізу судових вироків можна зробити висновок, що прямими доказами у кримінальних провадженнях, пов'язаних з незаконним поширенням наркотиків можуть бути: листування в соціальній мережі «Telegram» щодо замовлення наркотичних засобів, психотропних речовин і прекурсорів [64, 66, 71,

73, 78, 82, 84], замовлення наркотичних засобів, психотропних речовин і прекурсорів через інтернет-магазин [65, 75, 76, 82], отримання інформації про «закладку»(схованку) – адреса, фото місця та координати, опис, тощо [65, 73, 75, 76, 78, 84], отримання фото квитанції відправлення через «Нову пошту» [66], збут наркотичних засобів, психотропних речовин і прекурсорів через соціальну мережу «Telegram» [61, 64, 80], надсилання інформації про «закладку» (схованку) – адреса, фото місця, координати, опис, тощо [61, 80] [184, с.81].

Наркоторгівля є одним з найпоширеніших злочинів, який вчиняється за допомогою Інтернету. Зокрема, у 2020 році виявлено 1175 кримінальних правопорушень щодо збуту наркотичних засобів, психотропних речовин або їх аналогів, а також отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів із використанням всесвітньої мережі Інтернет. Ця кількість зросла практично втричі у порівнянні з 2019 роком (421 кримінальне правопорушення), та майже у шість разів більше ніж у 2018 році (196 кримінальних правопорушень) (додаток Б). При цьому, варто відзначити, що у ЗМІ ці показники подаються як кількість виявлених груп, які збували наркотичні засоби з використанням Інтернету [86, с. 114].

Згідно стану боротьби з наркозлочинністю протягом вересня 2019 року – серпня 2020 року кількість виявлених інтернет-ресурсів з продажу наркотичних засобів і психотропних речовин збільшилась втричі у порівнянні з аналогічним періодом минулих років. Зокрема, викрито 1154 осередки, які поширювали наркотики в Інтернеті (з вересня 2018 року до серпня 2019 року було викрито 448 таких осередків) [199]. У грудні 2020 року Департамент боротьби з наркозлочинністю спільно зі слідчими м. Києва виявили та припинили діяльність понад 100 магазинів у Інтернет-мережі з продажу наркотичних речовин та викрили 3 гуртових постачальників [151].

Для блокування телеграм-каналів, через які здійснюється продаж наркотичних засобів, факультет кіберполіції Харківського національного університету внутрішніх справ створив безплатний чат-бот «СтопНаркотик» і

«Mriya». Необхідно зазначити, що вже з моменту презентації чат-бота є позитивні результати роботи [148].

На сьогодні соціальні мережі є істотним інструментом руйнівного психологічного впливу, з метою маніпулювання людиною та певними соціальними групами, суспільством, а також – полем інформаційного протиборства.

Паралельно з цим набуває розвитку в мережах використання специфічних маніпулятивних технологій. Серед великого різноманіття способів інформаційних впливів, які реалізуються в інформаційному просторі або через нього, можна виділити такі: поширення спеціально підібраної інформації (дезінформації). Цей спосіб впливів здійснюється у формі розсилки e-mail (електронних листів); організації новинних груп у соціальних мережах; створення сайтів з елементами інтерактивної взаємодії їх відвідувачів (чати, онлайн голосування); розміщення інформації на приватних за змістом веб-ресурсах: у блогах, соціальних мережах.

В умовах реальної інформаційної війни, пов’язаної з подіями на Сході України, маніпулювання інформацією, що реалізується через Інтернет і, безпосередньо, через соціальні мережі, є серйозною загрозою як головним засадам розбудови демократичного суспільства й зміцненню незалежності України, так і національній інформаційній безпеці держави. Інформаційне маніпулювання із застосуванням різноманітних технологій інформаційно-психологічного впливу в сучасних умовах стає загрозливішим. Сугестивні технології активніше використовуються в інтернет-просторі і набувають масштабів, співмірних з найсуттєвішими загрозами для національного інформаційного простору [205, с. 256].

Кримінальні правопорушення проти основ національної безпеки активно вчиняються у соціальних мережах, а тому основними доказами у таких провадженнях є відомості з аккаунтів: публікації, дописи, коментарі, особисте листування. Такі відомості можуть зберігатись у комп’ютерній техніці, мобільному телефоні, на сервері, в мережі Інтернет чи інших місцях.

Наприклад, суд задовольнив клопотання слідчого про надання тимчасового доступу та можливість копіювання (роздруку) необхідних відомостей у кримінальному провадженні, внесеного до ЄРДР за ознаками кримінального правопорушення, передбаченого ч.2 ст.109 та ч.1 ст.114-1 КК.

В обґрунтування свого клопотання, слідчий зазначив, що продовж січня-квітня 2016 року гр. Д. та гр. О., бувши в складі, так званих, об'єднаних анархістів радикальної організації «Чорний світанок» здійснювали адміністрування радикально налаштованої Інтернет-спільноти. Гр. О. виступав активним учасником та організатором масових акцій громадянської непокори. Окрім того, вказані особи, шляхом керування та наповнення електронної групи проводили агітаційну роботу серед активістів громадських та незалежних медійних Інтернет-форумів, формували деструктивні погляди та думки інших учасників спільноти, направлені на шкоду конституційному ладу, територіальній цілісності та державному суверенітету України [227].

В такому випадку листування гр. О. з іншими учасниками групи підтверджує адміністрування радикальної спільноти, участь в ній уже відомих співучасників та дає можливість встановити осіб, які також причетні до вчинення цих кримінальних правопорушень. Приватна бесіда між співучасниками дає можливість встановити мотив, мету, роль учасників кримінального правопорушення та іншу інформацію, що є предметом доказування.

Ще одним прикладом визнання належними доказами листувань у соціальних мережах між обвинуваченими та іншими особами є рішення Колегії суддів судової палати з розгляду кримінальних справ Львівського апеляційного суду за обвинуваченням гр. Ж. у вчиненні кримінальних правопорушень, передбачених ч.1 ст. 109 КК, ч.2 ст.28 ч.1 ст.263 КК, гр. Г. у вчиненні кримінальних правопорушень, передбачених ч.2 ст. 345 КК, за ч.2 ст.28 ч.1 ст.263 КК, гр. К. у вчиненні кримінальних правопорушень, передбачених ч.2 ст.28 ч.1 ст.263 КК. Суд зазначив, що у ході судового розгляду знайшло своє підтвердження обвинувачення гр. Ж. в частині наявності змови про вчинення дій з метою насильницького захоплення державної влади. На наявність в діях

обвинувачених ознак складу кримінального правопорушення вказували предмети, які були в них вилучені, їхнє особисте листування в соціальній мережі, документи з розподілом ролей учасників змови, які зберігались на їхніх персональних комп'ютерах та носіях інформації, тощо [235].

Окрім, злочинів у сфері обігу наркотиків та проти основ національної безпеки, поширеним явищем є шахрайство в Інтернеті – обман покупців в інтернет-магазинах, обман осіб та отримання конфіденційної інформації: термін дії платіжних карток, CVV, PIN, паролі і ін. Так, згідно з даними Департаменту кіберполіції Національної поліції України протягом 2020 року отримано 41 568 звернень громадян, з них понад 80 % щодо шахрайства в мережі Інтернет, заблоковано 28 559 шахрайських інтернет-посилань [157]. У таких провадженнях, доказуванню обов’язково підлягає вид і розмір шкоди, завданої кримінальним правопорушенням.

Якщо внаслідок шахрайства невідома особа здійснила переказ певної суми коштів, то відповідний платіж, транзакція може бути доказом як події кримінального правопорушення, так і розміру завданої шкоди. Водночас розрахунки за допомогою систем дистанційного обслуговування здійснюються відповідно до глави 10 Інструкції про безготівкові розрахунки в Україні в національній валюті, затвердженої постановою Правління Національного банку України від 21 січня 2004 року № 22 (далі – Інструкція № 22).

Згідно з п. 10.1 Інструкції № 22 клієнт може обслуговуватись дистанційно за допомогою систем «клієнт-банк», «клієнт-Інтернет-банк», «телефонний банкінг», «платіжний застосунок» та інших систем дистанційного обслуговування.

Пунктом 10.5 Інструкції № 22 визначено, що під час здійснення розрахунків за допомогою систем «клієнт-банк», «клієнт-Інтернет-банк» тощо застосовуються електронні розрахункові документи. Якщо це передбачено договором між банком та клієнтом, то використання клієнтом системи не виключає можливе оброблення банком документів клієнта на паперових носіях.

Реквізити електронного розрахункового документа, що використовується в системах «клієнт-банк», «клієнт-Інтернет-банк», визначаються договором між банком та клієнтом, але обов'язково цей документ має містити визначені реквізити.

Тому, усі платежі, проведені через «Інтернет-банкінг» (Приват 24, Ощад 24 та інші) та роздруковані електронні квитанції, які містять обов'язкові реквізити електронного розрахункового документа, визначені п. 10.5 Інструкції № 22, – є підтвердним документом понесених платником податку витрат та печаткою банку вона не завіряється [109].

Таким чином, платіжний документ, який здійснений за допомогою інтернет-банкінгу та збережений на технічному пристрої є електронним документом. Під час досудового розслідування кримінальних проваджень, вважаємо, за необхідне долучати роздруковану електронну квитанцію, яка не потребує завірення у відділенні банку. Огляд електронної квитанції може бути проведений лише за необхідності. Наприклад, якщо електронна квитанція була предметом злочинних дій (підробки, тощо).

Водночас крадіжка криптовалюти, титульних знаків чи іншої електронної валюти через відсутність офіційного правового статусу і легальної торговельної площадки для її обігу становить проблему під час кваліфікації кримінального провадження, визначення розміру завданої шкоди та здійснення досудового розслідування.

Зокрема, мною, під час проведення досудового розслідування кримінального провадження, пов'язаного з несанкціонованими переказами у електронній системі «WebMoney» спільно з Департаментом кіберполіції Національної поліції України було проведено наступні дії: отримано інформацію про особу-правопорушника з вебсайту «Webmoney»; подано запит та отримано офіційну відповідь від представника «Webmoney» в Україні про обліковий запис особи-правопорушника; встановлено місце проживання особи-правопорушника; подано запит та отримано відповідь від провайдера, яким підтверджено IP-адресу з якої здійснювались транзакції; проведено обшук житла правопорушника, під

час якого вилучено мобільний телефон потерпілого. Незважаючи на те, що особа повністю визнавала вчинене ним кримінальне правопорушення та було зібрано достатньо доказів, неможливо було встановити розмір завданої шкоди та відповідно встановити усі елементи складу крадіжки, оскільки титульні знаки, які були переведені правопорушником не є предметом крадіжки. Переведення отриманих у злочинний спосіб титульних знаків зі свого гаманця в електронній системі «Webmoney» на власний банківський рахунок ПАТ КБ «Приватбанк» у вигляді грошей (конвертація) та зняття їх у терміналі стало належним доказом завдання потерпілому матеріальної шкоди та встановлення її розміру. За вчинення даного кримінального правопорушення особу було визнано винною за ч. 1 ст.185 КК та ч. 1 ст. 361 КК [70].

Зазвичай, внаслідок вчинення кримінальних правопорушень з використанням високих ІТ завдається великий матеріальний збиток. Наприклад, протягом 2017-2020 рр. загальна установлена сума збитків становить 163 млн 734 тис. грн., а сума відшкодованих збитків, з урахуванням накладеного арешту та вилученого майна становить 77 млн 583 тис. грн. (додаток Б).

Електронні документи, які містяться на мобільних телефонах та інших пристроях можуть бути прямими доказами вчинення кримінального правопорушення особою, яка повністю заперечує його вчинення.

Наприклад, суд дослідив зібрані у провадженні докази, зокрема: мобільні телефони, де в розділі «Контакти» вказаних телефонів були номери телефонів та листування в додатку «Viber», котрі мають відношення до сутенерства, проституції, секс туризму та фінансових питань щодо грошових коштів, отриманих від зайняття проституцією. Також в листуваннях були фотознімки, а саме: фотографії з Туреччини, фотографії жінок-повій разом з клієнтами та обвинуваченим в орендованому будинку та в басейні, еротичні фото дівчат, скріншоти грошових переказів за допомогою додатку «Приват 24». Фотографії у мобільних пристроях автоматично відсортовані за датою та місцем їх виготовлення – в Туреччині та у м. Дніпро; в ході огляду мобільного телефону марки «Iphone-6» встановлено наявність фотографій із зображенням

обвинуваченого та жінок-повій, а також листування останніх з обвинуваченим. Суд зазначив, що зафіксовані дані із вилучених телефонів, знайдених за місцем обшуку, а саме листування та наявність фотографій у додатках, а також показання потерпілих, зокрема, неповнолітньої на час учинення злочину обвинуваченим, неповнолітніх свідків, які повідомили суду, що обвинувачений, який мав фотокопії паспортів дівчат, було достеменно відомо про їхній вік, та попри факт неповноліття, останній влаштував їх на роботу з надання послуг інтимного характеру особам чоловічої статі, а також пропонував їм займатись проституцією на території Турецької Республіки.

Враховуючи вищевказане, суд не взяв до уваги твердження обвинуваченого та критично поставився до його показань, оскільки вищевказані докази підтверджували, що останній втягував, вербував та примушував потерпілих займатись проституцією, а також підтверджували факт застосування до них погроз, та враховуючи їхній уразливий стан – шантажу [68].

Відомості з електронних документів також можуть бути непрямими доказами або мати допоміжне значення для складання версій, їх перевірки, встановлення можливих місць вчинення злочину та можливих учасників, тощо.

Зокрема, у справі щодо притягнення до кримінальної відповідальності гр. Р. за ч. 2 ст. 258-2, ч. 1 ст. 161, ч. 1 ст. 258-3 КК, суд під час розгляду справи встановив, що за допомогою сайту «Миротворець», «Центр досліджень ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку» (https://psb4ukr.org/criminal/) оглянуто пошуковий сервіс баз даних осіб, що причетні до протиправної діяльності на шкоду національній безпеці України. Протоколом огляду встановлено, що за даними сайту «Миротворець» місце роботи гр. Т. – «Новороссия ТВ, Народний телеканал, Донецьк, Технічний директор». Окрім того, на сайті «Миротворець» здійснено збереження розміщуваних особою фото у соціальних мережах, в т.ч. й місць бойових дій, чи таких, що містять заклики на підтримку терористичної діяльності терористичної організації ДНР. Під час подальшого проведення огляду відкрито сайт «TERROR.IN.UA» (http://terror.in.ua/) на якому також

здійснюється збір даних стосовно осіб, що причетні до протиправної діяльності на шкоду національній безпеці України. Отримано інформацію в розділі «Террористы в розыске» стосовно гр. Т.

Також, під час дослідження сторінки гр. Т. у соціальній мережі «Вконтакте», стало відомо, що останній вказав місце роботи «Новороссия ТВ, Народный телеканал, Донецьк, Технічний директор», а гр. Р. перебуває у нього в друзях [60].

Вищевказані відомості є непрямими доказами, однак в сукупності з документуванням змісту особистих листувань між гр. Р. та гр. Т щодо налаштування та здійснення трансляцій каналу «Новороссия ТВ», встановлення факту численних з'єднань за номерами телефонів гр. Р та гр. Т та інших доказів, суд визнав гр. Р. винним.

Непрямі докази повинні утворювати у своїй сукупності систему, в якій докази не тільки узгоджені між собою, але і підкріплюють одне одного. Тому між непрямими доказами повинен існувати зв'язок [120, с. 31].

Як зазначає В.В. Вапнярчук, залишається невирішеним питання визнання належними доказів, які стосуються версії, яка не знайшла свого підтвердження. Одні науковці вважають, що належність доказів, зазвичай, визначається ймовірно, і якщо надалі їх зв'язок з розслідуваним діянням не підтвердиться, вони втрачають цю властивість і перестають бути доказами. Інші вважають, що докази, котрі призвели до відкидання певної версії (наприклад, алібі) залишаються такими й не втрачають властивості належності.

Ми погоджуємось з думкою В.В. Вапнярчука, що правильною є друга точка зору, оскільки, по-перше, головне, щоб докази мали значення для кримінального провадження, інакше з-поміж доказів потрібно буде виключати майже всі виправдувальні докази, позаяк зазвичай вони відкидають версію сторони обвинувачення; по-друге, такі докази можуть мати значення і для непрямого підтвердження версії, яка залишилась, тобто встановлювати якісь доказові факти; по-третє, версії, які відпали, є такими лише для конкретної стадії процесу, адже вони завжди можуть бути перевірені й оцінені вищими інстанціями [52, с. 243].

Різні учасники кримінального провадження висувають різні версії кримінального правопорушення, а тому оцінка належності доказу може суттєво відрізнятися. Тобто, вирішення питання про належність доказу, з одного боку, ґрунтується на положеннях норм закону, зокрема, ст. ст. 85, 91 КПК, з іншого – на суб'єктивному сприйнятті особи – суб'єкта доказування, що ґрунтується на його уявленні про логічний зв'язок фактичних даних, що становлять зміст доказу та обставин, які підлягають доказуванню у кримінальному провадженні, передбачених ст. 91 КПК [196, с. 237].

Під час розслідування кримінального правопорушення, передбаченого ст. 115 КК за допомогою електронних документів можуть бути висунені та перевірені різні слідчі версії. Наприклад, у Японії молоді жінки діляться своїми суїцидальними намірами в мережі Інтернет, шукають однодумців і домовляються про дату і час смерті [55]. Перевірка особистих записів потерпілого може надати можливість встановити його думки про суїцид, приналежність до так званих «груп смерті», які існують у соціальних мережах. Також, доволі часто самогубці ведуть щоденники, або блоги в електронному, онлайн-форматі, діляться своїми думками, переживаннями у постах, коментарях, групах, під час листування з різними людьми. Такі відомості можуть мати доказове значення у кримінальному провадженні.

У судовій практиці також наявні випадки, коли електронні документи можуть бути неналежними доказами у кримінальних провадженнях з різних підстав.

Наприклад, під час досудового розслідування кримінального провадження за ч. 1 ст. 258-3 КК, в ході обшуку за місцем проживання свідка гр. В. оглянуто його комп'ютер, в якому у соціальній мережі виявлено листування між ним та обвинуваченим гр. Б. Згідно з цим листуванням гр. Б. надсилав гр. В. ряд фотографій з коментарями до них, а саме: фото нагороди, що виглядає у виді хреста з написом «Доброволец», «Донбасс», фото, на якому гр. Б. на площі з підписом - «награждение в Севастополе было», фото, на якому гр. Б. зі зброєю у військовій формі та шевроном та підписом до нього «на посту», а також у

листуванні гр. Б. зауважував, що: «война многому учит». Також, проведено огляд сторінки гр. Б. у соціальній мережі «Вконтакте», на основному фото якого гр. Б. на танку (БТР). У даних про рідне місто зазначено Слов'янськ. На сторінці наявні фотографії за 2014-2015 рр. Фото зображення наявні та сторінки датовані 2014-2015 роками, на яких наявні особи у військовій формі з шевронами «Новоросії» та зі зброєю, серед яких є гр. Б. [63].

В окремій думці судді Кофанова А.В., який входив до колегії суддів, що розглядали дане провадження, зазначено, що достатньо сумнівними та неналежними як докази слід визнати роздруківки та фотографії з так званих соціальних інтернет-мереж, що були вилучені протоколом обшуку. Зі змісту цих документів вбачається, що вони були розміщені на так званих неавторизованих сторінках, тобто джерело та обставини походження цих документів є невідомим, про що обґрунтовано вказав захисник обвинуваченого. У цьому випадку саме застосування поняття «оригінал документу» є неможливим, а отже, зазначені роздруківки та фотографії не можуть вважатися доказами [153].

Також, в ухвалі Кіровського районного суду м. Кіровограда у задоволені клопотання слідчого про дозвіл на обшук відмовлено з мотиву визнання поданих доказів неналежними та недопустимими. Для підтвердження факту підпільного виробництва незаконного виготовлення одягу під відомими торговельними марками, серед яких: «ADIDAS», «NIKE», «PUMA», «Tommy Hilfiger» та збуту готової продукції у торговельній мережі «Садко», слідчий додав фотографії контрафактної продукції та зовнішнього вигляду магазинів «Садко». Суд у своєму рішенні зазначив, що фотографії контрафактної продукції та магазинів «Садко», додані до клопотання як докази подані без зазначення дати виконання фото та місця виконання фотографії. Фотографії магазинів зовні взагалі не є належними доказами [234].

У обох випадках електронні документи (роздруківки з огляду соціальних мереж та фотографії контрафактної продукції і магазинів) є неналежними доказами через неможливість встановлення взаємозв'язку даних документів з

предметом доказування та тісно пов’язані з порушенням вимог допустимості доказів.

Водночас неможливо ототожнювати належність та допустимість доказів, оскільки належність стосується змісту доказу (ч. 1 ст. 84 КПК), а допустимість – його форми (ч. 2 ст. 84 КК). Тому, ми не погоджуємось з думкою В.В. Маркова та Р.Р. Савченко, які зазначають, що допустимість відноситься до принципів належності електронних доказів, отриманих із мобільних пристроїв [144, с.92]. В.В. Вапнярчук вважає, що належність і допустимість це властивості, які визначаються за різними критеріями і між собою жодним чином не зв’язані. Адже, неналежні докази, якщо вони отримані в порядку передбаченому законом, є цілком допустимими (наприклад, фотографія, яка не встановлює обставин кримінального правопорушення), і навпаки належний доказ може виявитися недопустимим (знаряддя кримінального правопорушення, вилучене з порушенням КПК) [54, с. 365].

Отже, належність є властивістю електронного документа, яка полягає у його здатності встановлювати факти, які підлягають доказуванню у кримінальному провадженні. Електронні документи можуть прямо чи непрямо встановлювати обставини, що підлягають доказуванню у кримінальному провадженні, а також допомагати у складенні і перевірці версій розслідувань, встановленні можливості чи неможливості використання інших доказів.

2.2. Допустимість електронних документів у кримінальному провадженні

Сторони кримінального провадження мають рівні права на збирання та подання до суду речей, документів, інших доказів, клопотань, скарг, а також на реалізацію інших процесуальних прав, передбачених КПК.

Під час збору доказів слідчий, дізнавач, прокурор, повинен дотримуватись основних вимог, що стосуються доказів: належність, допустимість, достатність, достовірність.

Визнаватися допустимими та використовуватися як доказ в кримінальному провадженні можуть тільки фактичні дані, одержані згідно з вимогами КПК.

Оцінка доказів на предмет їхньої допустимості є однією з гарантій забезпечення прав і свобод людини та громадянина в кримінальному процесі, прийняття законного і справедливого рішення. Аналіз положення ч. 3 ст. 62 Конституції України «обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом» дає підстави для висновку, що обвинувачення у вчиненні кримінального правопорушення не може бути обґрунтоване фактичними даними, одержаними в незаконний спосіб, тобто: з порушенням конституційних прав і свобод людини і громадянина; з порушенням встановлених законом порядку, засобів, джерел отримання фактичних даних, не уповноваженою на те особою тощо [210].

Згідно зі ст. 19 Конвенції про захист прав людини і основоположних свобод, обов’язок Європейського суду з прав людини полягає в забезпеченні дотримання Договірними державами їхніх зобов'язань за Конвенцією. Зокрема, до його функцій не належить розгляд помилок, яких нібито припустився національний суд при вирішенні питань факту чи права, якщо – і тією мірою, якою – такі помилки не становлять порушення гарантованих Конвенцією прав і свобод.

Хоча ст. 6 Конвенції про захист прав людини і основоположних свобод гарантує право на справедливий судовий розгляд, вона не встановлює ніяких правил стосовно допустимості доказів як таких, бо це передусім питання, яке регулюється національним законодавством [208].

Так, згідно ч.1 ст.86 КПК, допустимість доказу означає отримання доказу у порядку визначеному КПК.

Торкаючись питання правової регламентації допустимості доказів, необхідно відзначити, що кримінальне процесуальне законодавство України містить визначення поняття допустимості доказів (ст. 86 КПК), але не виділяє, за винятком випадків істотного порушення прав та свобод людини (ст. 87 КПК), критерії вирішення питання про недопустимість доказів. Крім того, висновок про визнання за доказами цієї невіддільної ознаки постає з положень класичної теорії доказів, зі змісту ч. 3 ст. 62 Конституції України (норма про неможливість

обґрунтування обвинувачення на доказах, отриманих незаконним шляхом) та ч. 1 ст. 84 КПК (легальне поняття доказів). У цілому норми, що прямо або опосередковано стосуються допустимості доказів, хаотично розташовані в тексті КПК [216, с. 246-247].

Аналіз дискусійних питань про зміст кожного критерію дозволяє зробити висновок про те, що вчені-процесуалісти встановлюють різні критерії дослідження доказів із точки зору їх допустимості. Водночас майже всі фахівці називають серед умов допустимості доказів у кримінальному провадженні такі складові елементи: належний суб'єкт, належний спосіб, належне джерело, належна форма закріплення відомостей про факти [216, с. 245].

Для дослідження електронного документа в частині допустимості, на нашу думку, доцільно проаналізувати кожен його елемент:

1. Належний суб'єкт збирання електронних документів.

Вимога про те, що доказ має бути отриманий належним суб'єктом, означає одержання його учасником кримінального процесу, правомочним здійснювати це провадження (конкретну процесуальну дію).

Зокрема, належним суб'єктом, який уповноважений на проведення досудового розслідування є слідчий, дізнавач:

– визначений керівником органу досудового розслідування для здійснення конкретного кримінального провадження (ч. 1 ст. 214 КПК);

– якому із заяви, повідомлення чи інших джерел стало відомо про обставини, які можуть свідчити про вчинення кримінального правопорушення, розслідування якого не віднесено до його компетенції (підслідності), він проводить розслідування доти (тобто є належним слідчим, дізнавачем у цьому кримінальному провадженні), доки прокурор не визначить іншу підслідність (ч. 2 ст. 218 КПК).

– якому постановою слідчого іншого органу досудового розслідування іншої територіальної юрисдикції чи прокурора доручено проведення слідчих (розшукових) і негласних слідчих (розшукових) дій (ч. 6 ст. 218 КПК);

– який входить до складу слідчої групи (ч. 2 ст. 38 КПК);

– який на час провадження конкретних слідчих (розшукових) чи інших процесуальних дій, в результаті яких були отримані докази, перебував на посаді слідчого й виконував свої трудові обов'язки (зокрема, не знаходився на лікуванні, не перебував у відпустці тощо) [52, с. 246-247].

Відповідно до п. 17 ч. 1 ст. 3 КПК, слідчим є службова особа відповідного органу досудового розслідування, уповноважена в межах компетенції, передбаченої КПК, здійснювати досудове розслідування кримінальних правопорушень.

Згідно п.4-1 ч.1 ст. 3 КПК, дізнавач – це службова особа підрозділу дізнання, уповноважена особа іншого підрозділу зазначених органів, які уповноважені в межах компетенції, передбаченої КПК, здійснювати досудове розслідування кримінальних проступків [130].

Це доводить, що відповідна службова особа має право здійснювати досудове розслідування за одночасної наявності двох умов:

1) вона є службовою особою органу досудового розслідування чи підрозділу дізнання, до компетенції якого відноситься розслідування відповідного кримінального провадження;

2) вона є уповноваженою у передбачений законом спосіб на здійснення досудового розслідування.

Дотримання умови щодо призначення слідчого, дізнавача на проведення досудового розслідування можливе лише при правильному визначенні органу досудового розслідування, підрозділу дізнання до компетенції якого відноситься таке розслідування.

Постанова прокурора про визначення підслідності (в порядку ч. 7 ст. 214 КПК) чи доручення проведення досудового розслідування кримінального правопорушення іншому органу досудового розслідування (в порядку ч. 5 ст. 36 КПК) з порушенням вимог підслідності не уповноважують орган досудового розслідування на проведення будь-яких дій.

Керівник органу досудового розслідування, який не може проводити досудове розслідування кримінального провадження згідно зі ст. 216 КПК, не

може й уповноважувати слідчого, дізнавача на такі дії. Прийняте рішення керівника органу досудового розслідування про призначення слідчого, дізнавача у кримінальному провадженні всупереч вимогам підслідності не має жодного юридичного значення [247].

Слідчий, дізнавач, прокурор можуть доручати збирання доказів оперативним працівникам. Після винесення доручення оперативні працівники наділяються правом проводити слідчі (розшукові) дії та негласні слідчі (розшукові) дії в кримінальному провадженні.

Залучення осіб до кримінального провадження здійснюється слідчим, дізнавачем, прокурором шляхом винесення відповідної постанови, або прийняття рішення про проведення відповідної процесуальної дії. В окремих випадках, особа може бути залучена до кримінального провадження після написання заяви про залучення її до кримінального провадження (наприклад, залучення потерпілого).

У будь-який момент підозрюваний, обвинувачений, потерпілий, свідок та інші учасники кримінального провадження мають право користуватись правовою допомогою захисника, відповідно, захисник наділяється правами та обов’язками учасника, інтереси якого він представляє. За вимогами КПК, захисником може бути лише адвокат, відомості про якого внесені до Єдиного реєстру адвокатів України, має свідоцтво про право на зайняття адвокатською діяльністю та доручення, укладену угоду чи ордер на надання правової допомоги. Якщо в особи відсутні такі документи чи його діяльність зупинена, або припинена то він не має право збирати та подавати докази, бути присутнім під час проведення слідчих (розшукових) дій та судових засідань.

Так, ухвалою Голопристанського районного суду Херсонської області від 07.04.2020 року слідчий суддя відмовив у задоволенні заяви захисника у зв’язку з тим, що заява подана неуповноваженою особою. Суд зазначив, що згідно з листом Секретаріату Національної асоціації адвокатів України відомості стосовно захисника в Єдиному реєстрі адвокатів України відсутні і адміністратором першого рівня бази даних ЄРАУ не вносились [228].

Таким чином, вичерпний перелік осіб, які можуть здійснювати збирання доказів та умови їх призначення, залучення визначені КПК.

2. Належний спосіб збирання електронних документів.

Основним способом збирання електронних документів слідчим, дізнавачем, прокурором у кримінальному провадженні є проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій. Їх перелік визначений Главами 20 та 21 КПК. Окрім того, сторона обвинувачення та сторона захисту можуть подавати запити до підприємств, установ та організацій чи витребовувати електронні документи.

З метою досягнення дієвості кримінального провадження сторона обвинувачення може звертатись із клопотанням про застосування заходів забезпечення кримінального провадження.

Так, тимчасовий доступ до електронного документа є одним із заходів забезпечення кримінального провадження і полягає у наданні особою, у володінні якої знаходяться такий електронний документ, стороні кримінального провадження можливості ознайомитися з ним, зробити копії та вилучити його (здійснити виїмку). Цей захід не є слідчою (розшуковою) дією, а одним зі способів отримання доступу до інформації і має проводитися лише у випадку, коли особа (володілець) відмовляється надати інформацію добровільно, або інформація становить охоронювану законом таємницю. У випадку, якщо існує загроза безповоротної зміни, знищення електронного документа проводити тимчасовий доступ недоцільно, слід одразу проводити обшук.

КПК допускає звернення з клопотання про тимчасовий доступ до речей і документів не тільки стороною обвинувачення, але й захисту. У випадку відмови підприємства, установи, організації у наданні електронного документа сторона захисту може отримати дозвіл суду на такий доступ. Однак, як показує практика, деякі суди не задовольняють клопотання сторони захисту про тимчасовий доступ у зв’язку з необхідністю використання усіх законних процесуальних можливостей для отримання запитуваних відомостей без звернення до суду [239]. В першу чергу, це звернення до слідчого, дізнавача чи прокурора з відповідним

клопотанням. Вважаємо, що такі рішення є незаконними та суперечать засадам змагальності, рівності сторін в частині збирання доказів.

Отримання доступу до фізичного носія електронного документа без подальшого огляду файлів, які на ньому збережені, на нашу думку, є порушенням правил збирання доказів. Тобто, тимчасовий доступ надає можливість отримати певний пристрій, носій інформації, на якому знаходиться електронний документ. Отримання (фіксація) самого змісту електронного документа здійснюється за допомогою його огляду.

У КПК відсутнє право огляду доказів, у тому числі електронного документа стороною захисту, адже ст. 237 КПК зазначає вичерпний перелік осіб, які можуть проводити огляд. Тому, сторона захисту має право надати електронний документ слідчому, дізнавачу чи прокурору для огляду та долучення його до матеріалів кримінального провадження [182, с. 37]. Більш детально про огляд електронного документа буде розглянуто у розділі 3.1 дисертації.

Під час аналізу судових рішень встановлено випадки неправильного розуміння способу отримання електронного документа у кримінальному провадженні. *Наприклад, у судовому засіданні стороною захисту заявлено про недопустимість диску із відеозаписом камер спостереження хостелу як речового доказу, де було зафіксовано факт затримання правопорушників. Відеозапис був добровільно наданий адміністрацією хостелу та визнаний речовим доказом. Сторона захисту зазначала, що для отримання такого відеозапису слідчий мав попередньо отримати дозвіл слідчого судді на тимчасовий доступ до відеозаписувальної апаратури, та лише потім робити копію запису у встановленому законом порядку.*

У своєму рішенні суд зазначив, що заходи забезпечення кримінального провадження застосовуються з метою досягнення дієвості кримінального провадження. У цьому випадку, слідчий отримав копії відеозапису камер спостереження у відповідь на його запит та у добровільному порядку, при цьому права інших осіб порушено не було. У задоволенні клопотання сторони захисту суд відмовив [231].

У вищевказаному прикладі, вважаємо, що слідчий отримав відеозапис законно, адже згідно з ч.2 ст.93 КПК він має право збирати докази за допомогою витребування, отримання, проведення інших процесуальних дій передбачених КПК. Застосування тимчасового доступу до документів чи проведення обшуку вимагає втручання в права людини, тому застосовується лише у передбачених випадках, коли в інший спосіб неможливо отримати докази.

Проте, слід дотримуватись наступного порядку дій: перш за все необхідно оглянути відеозапис з першоджерела (комп'ютера хостелу) у присутності володільця (користувача) відеозапису (власника, адміністратора, працівника хостелу), далі створити копію відеозапису та записати її на носій інформації, після цього зобов'язати працівників хостелу зберегти відеозапис події до закінчення судового процесу. У таких випадках, доцільно залучати спеціалістів для допомоги при роботі з електронними документами та з метою недопущення втрати важливої інформації [185, с. 99].

Отже, під час збирання електронних документів сторона обвинувачення повинна правильно розмежовувати слідчі (розшукові) дії та заходи забезпечення кримінального провадження залежно від ступеня втручання у права та свободи громадян та можливостей отримання доказів. Слідчий, дізнавач може збирати електронні документи шляхом:

– надання його добровільно учасником кримінального провадження (отримання);

– витребування доказів;

– проведення тимчасового доступу до електронного документа (як заходу забезпечення);

– проведення слідчих (розшукових) дій (огляд, обшук);

– проведення негласних слідчих (розшукових) дій.

Після отримання електронного документа на носії інформації, слідчий, дізнавач зобов'язаний оглянути його.

В свою чергу, сторона захисту, потерпілий та його представник згідно ст. 93 КПК збирає електронні документи шляхом:

1) витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок

2) отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок;

3) ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій;

4) здійснення інших дій.

Якщо говорити про право сторони захисту, потерпілого на ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, то в цьому випадку учасники виступають лише ініціаторами, а суб'єктами збирання, у випадку задоволення клопотання, буде слідчий чи дізнавач [263, с. 63].

Проте, якщо для сторони обвинувачення існує виключний перелік законних способів збирання доказів, то натомість докази, у тому числі електронні документи, зібрані стороною захисту, у невизначений законом спосіб, чи з певними порушенням не можуть бути визнані одразу недопустимими, а повинні досліджуватись з іншими доказами на предмет можливості їх використання для доведення невинуватості.

Як зазначає Верховний суд у постанові від 29.09.2020 року, законодавець застосовує «асиметричний» підхід щодо збирання доказів сторонами у кримінальному провадженні. У ч. 3 ст. 17 КПК передбачено, що обвинувачення не може ґрунтуватися на доказах, отриманих незаконним шляхом, однак дана норма не містить подібної категоричної заборони щодо доказів, які надаються на спростування обвинувачення і свідчать на користь сторони захисту. Якщо доказ отримано і надано суду стороною обвинувачення, суд має бути вкрай обережним, оцінюючи вплив формальних порушень під час отримання доказу на

можливість його використання для спростування обвинувачення. Правила оцінки доказів, особливо вимога дотримуватися передбаченого законом порядку при отриманні доказів, мають за мету запобігання неправомірному втручанню держави та заохочення доброчесної поведінки правоохоронних органів. Вимога визнати докази, отримані з порушеннями, недопустимими спрямована на те, щоб сторона, що допустила порушення, не могла скористатися його результатами. Використання цих правил на шкоду стороні, яка жодним чином не відповідальна за порушення процесуальних правил, суперечить їх меті [163].

Більш детально про способи збирання електронних документів сторонами буде розглянуто у підрозділі 3.1 дисертації.

3. Належне джерело отримання електронних документів.

Допустимим електронним документом буде лише той, який отриманий з належного процесуального джерела. У підрозділі 1.2 дисертації нами обґрунтовано необхідність виокремлення електронного документа як окремого самостійного джерела доказу. Враховуючи законодавче закріплення лише чотирьох джерел доказів, ми вважаємо, що електронний документ на цей час може бути документом або речовим доказом. Для того, щоб розрізнити електронний документ від речового доказу в електронній формі, слід звернути увагу на те, що саме може бути використане як доказ факту чи обставин, що встановлюються під час кримінального провадження: інформація чи матеріальний об’єкт.

Якщо доказове значення має інформація, яка збережена в електронній формі, то це електронний документ, наприклад, електронний лист отриманий у мережі Інтернет з інформацією, яка має значення для кримінального провадження. У цьому випадку, комп’ютер, мобільний телефон чи інший пристрій є лише засобом отримання інформації. Копіювання листа на інший носій інформації, знімок з екрана є похідним джерелом доказу, оскільки оригінал листа зберігається на Інтернет-сервері [182, с. 40].

Оскільки порядок отримання і зберігання речових доказів та документів є різним, регламентується окремими статтями КПК, то необхідно правильно визначати яким джерелом доказу є електронний документ.

У попередньому прикладі [231], де нами проаналізовано порядок отримання слідчим відеозапису від працівника хостелу допущено порушення при фіксації факту отримання запису з камер відеоспостереження.

Перш за все, слідчий неправильно оцінив яким саме джерелом доказу є відеозапис. У кримінальному провадженні відеозапис може бути визнаним як речовим доказом, так і документом в залежності від своїх ознак.

Як пояснює А.П. Запотоцький, доказове значення у документах – джерелах доказів має лише зміст, натомість у документах–речових доказах має значення не лише зміст, але і форма, місце та час їх виявлення тощо [111, с. 8]. Тому, у конкретному випадку відеозапис є електронним документом.

Найскладніша проблема з оцінки належності джерела електронного документа, як критерію допустимості, виникає тоді, коли він розміщений на віддаленому сервері. Наприклад, складно отримати доступ до сервера соціальної мережі «Facebook», який знаходиться у Сполучених штатах Америки, або до сервера соціальної мережі «Вконтакте» – в Російській Федерації. В такому випадку, огляд облікового запису, відеозапису, вебсайту, без вилучення інформації з сервера може бути визнаний недопустимим доказом.

Для уникнення неоднакового розуміння правил розмежування електронних документів – документів та речових доказів слід виокремити електронний документ окремим процесуальним джерелом доказів, що нами було обґрунтовано у підрозділі 1.2. та регламентувати можливість використання як оригіналу доказу відомостей з електронного документа, якщо його фізичний носій не має доказового значення для кримінального провадження. Тому, пропонуємо викласти ч. 5 ст. 99-1 КПК у такому вигляді: Електронний документ визнається допустимим доказом, якщо отримати зміст його відображення можливо без доступу до фізичного носія інформації, або такі відомості перебувають у вільному доступі (вебсайти). Для підтвердження змісту електронного документа

можуть бути визнані допустимими й інші відомості, якщо: 1) оригінал електронного документа втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає; 2) оригінал електронного документа не може бути отриманий за допомогою доступних правових процедур; 3) оригінал електронного документа знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.

Отже, важливо правильно встановлювати джерело доказу електронного документа, проводити фіксацію і дотримуватись правил зберігання такого доказу відповідно до визначених норм КПК.

4. Належна форма закріплення відомостей про факти.

Для виконання умови допустимості необхідно також дотримуватись порядку оформлення отриманих доказів. Належна форма закріплення відомостей про факти гарантує їх правильне сприйняття. До цього критерію відносяться форми проведення слідчих та негласних слідчих (розшукових) дій, заходів забезпечення, їх процесуальне закріплення у відповідних протоколах, додатках до них.

Як зазначає І.Л. Чупрікова Відповідно до правил допустимості, для того, щоб предмет матеріального світу отримав процесуальний статус «речового доказу», він повинен не лише містити на собі сліди, а й бути належним чином зафіксованим, оформленим, залученим до справи тощо [264, с. 268].

Відповідно до ст.103 КПК процесуальні дії під час кримінального провадження можуть фіксуватися: у протоколі; на носії інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії; у журналі судового засідання.

Порядок складання протоколу і додатків, ведення журналу судового засідання, створення носія інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії, їх обов'язкові реквізити та вимоги до них передбачені Главою 5 КПК.

На практиці, слідчі, дізнавачі часто допускають помилки під час фіксації доказів, зокрема електронних документів, що тягне за собою визнання такого доказу недопустимим. *Так, Бершадський районний суд Вінницької області визнав недопустимим доказом відеозапис огляду місця події у зв'язку з тим, що даний відеозапис збережений на СД-диску, який долучено до провадження, однак ідентифікаційних даних відеокамери на який він здійснювався у протоколі не зазначено. У зв'язку з цим неможливо встановити чи є наданий відеозапис оригіналом.*

Для перевірки відеозапису з точки зору допустимості суд допитав слідчого, який пояснив, що флеш-носій є первинним носієм інформації. Проте, на вимогу суду відеокамеру, якою проводився відеозапис не надано.

Оскільки СД-диск, який містить відеозапис огляду місця події, не є первинним носієм інформації, суд перед початком огляду даного доказу повинен встановити походження даного диску, спосіб його запису та технічний засіб, на який було зафіксовано відеозапис (первинний носій інформації). При цьому, ні на диску, ні в протоколі огляду місця події відсутні ідентифікуючі ознаки технічного засобу на який було проведено відеозапис цієї слідчої (розшукової) дії. Вказані обставини дають суду підстави для визнання даного відеозапису, відображеному на СД-диску, недопустимим доказом, оскільки не вдалось встановити джерело його походження.

Таким чином, Бершадський районний суд Вінницької області визнав недопустимим доказом відеозапис огляду місця події, відображений на СД-диску та виключив можливість його дослідження в судовому засіданні [223].

Слідчим допущено ряд порушень норм, що стосується фіксації доказів, а саме електронного документа. Зокрема, не зазначено у протоколі точні ідентифікуючі ознаки технічного засобу за допомогою якого було проведено відеозапис, не надано суду оригінальних примірників, не здійснено відкриття матеріалів досудового розслідування відповідно до положень ст. 290 КПК.

Отже, відеозапис огляду місця події, як додаток до огляду місця події визнано недопустимим доказом у зв'язку з неналежним оформленням та

забезпеченням проведення слідчої (розшукової) дії, порушенням порядку ознайомлення з матеріалами кримінального провадження. Звичайно, як наслідок, суд не може використовувати даний відеозапис як доказ у кримінальному провадженні.

Носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії хоча і не можуть бути використаними без протоколу слідчої (розшукової) дії, проте його значення є важливим для більш повного і об'єктивного сприйняття реальних обставин події, отримання детального уявлення ситуації, оцінки фактичних даних, отриманих під час доказування.

До протоколу проведення слідчих (розшукових) дій також можуть додаватись роздруківки чи скріншоти екрану як додатки. Роздруківка Інтернет-сторінки, файлу полягає у друці їх вмісту на папері. Паперова роздруківка, окрім інформації про зміст електронного документа може також містити дату, час роздруку, інтернет-адресу сторінки, кількість друкованих сторінок, їх нумерацію, тощо.

В українському законодавстві відсутній термін «скріншот» (з англ. Screenshot – «screen» - екран, «shot» - знімок), однак він широко використовується у повсякденному спілкуванні. Скріншот дозволяє зафіксувати зображення екрану у певний момент часу та зберігає його у вигляді фотографії на пристрої, екран якого фіксувався. Після цього, він також може бути роздрукованим у паперовому вигляді [179, с. 93].

На практиці слідчі, дізнавачі часто вважають, що самої роздруківки чи роздруківки скріншоту достатньо для підтвердження чи спростування певного факту та нехтують необхідністю складення протоколу огляду, що надалі призводить до визнання таких роздруківок недопустимими.

Роздруківка не може самостійно визнаватись доказом, оскільки передає лише частину електронного документа, яка відображена у доступній для користувача формі. Решта інформації є прихованою та може бути виявлена та відображена лише відповідними спеціалістами [179, с. 93]. Також виключається

можливість ідентифікації документа, його перевірки на втручання у зміст, тощо [29, с. 118].

Аналогічно, це стосується відеозапису, аудіозапису та інших додатків, які фіксують хід проведення слідчої (розшукової) чи негласної слідчої (розшукової) дій. Як зазначають Р.М. Шехавцов та С.С. Кудінов, носії інформації, отриманої під час проведення негласних слідчих (розшукових) дій шляхом застосування відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, є додатками до протоколів даних негласних слідчих (розшукових) дій відповідно до положень п. 3, 4 ч. 2 ст. 105 КПК України. Визнавати їх речовими доказами є невірним [267, с. 189].

Слід зазначити, що порушення одного з критеріїв допустимості електронного документа у кримінальному провадженні має наслідком визнання його та всіх доказів, зібраних на його основі недопустимими.

В таких випадках застосовується концепція «отруєного дерева» (або «ефект доміно»), яка знайшла своє відображення у чисельних рішеннях Європейського суду з прав людини, зокрема у справі «Яременко проти України» рішення у справі від 30.04.2015 р., заява № 66338/09, згідно якого визнання одного доказу недопустимим має наслідком невизнання доказами всіх фактичних даних, одержаних на його підставі («отруєне дерево дає отруйні плоди») [209].

На підставі викладених положень нами виділяються наступні рекомендації для визнання електронного документу допустимим доказом:

1. Збирання електронних документів повинно проводитись належними суб'єктами доказування. Перш за все, це слідчий та дізнавач який уповноважений відповідно до рішення керівника органу досудового розслідування згідно з правилами, визначених ст.216 КПК. Інші учасники кримінального провадження для збирання електронних документів повинні бути залученими до кримінального провадження у встановленому КПК порядку та володіти процесуальною правосуб’єктністю.

2. Електронні документи можуть бути надані: добровільно, на підставі запиту, витребувані, отримані під час проведення тимчасового доступу до речей

та документів, або під час огляду місця, обшуку. Вибір процесуальної дії залежить від володільця якого знаходиться електронний документ та виду інформації, яку він містить. У будь-якому випадку, огляд електронного документа є обов'язковою слідчою (розшуковою) дією. Єдина слідча (розшукова) дія, яка може зафіксувати зміст електронного документа є огляд.

3. Правильне розмежування електронного документа як речового доказу та документа впливає на порядок його вилучення та фіксації.

4. Фіксація факту і порядку отримання електронних документів здійснюється за допомогою проведення слідчих (розшукових) дій, таким чином, необхідно дотримуватись визначених форми протоколу та додатку до нього. Огляд електронного документа слід проводити за участі спеціаліста, з копіюванням такого документу на додатковий фізичний носій.

2.3. Встановлення достатності та достовірності електронних документів у кримінальному провадженні

Встановлення достовірності існування фактів, яким надається значення доказів – один з найголовніших елементів дослідження доказів [71, с. 58].

Факт це об'єктивна реальність, яка не залежить від сприйняття її слідчим чи дізнавачем, її пізнання та проникнення в її сутність. Факт не може бути недостовірним, тому що достовірність – не властивість факту, а властивість знань про факт [40, с. 58].

Про достовірність доказів можна говорити лише умовно, розуміючи під цим достовірність джерела доказів і наших відомостей про докази. Тому, перевірка доказів – перевірка достовірності їх існування і достовірності наших відомостей щодо його змісту. Саме так пояснює поняття достовірності Р.С. Бєлкін [40, с. 59].

С.О. Ковальчук розглядає достовірність як процесуальну властивість, що відображає відповідність їх змісту об'єктивній дійсності та придатність на основі такої відповідності використовуватися для встановлення фактів й обставин, які

мають значення для кримінального провадження і підлягають доказуванню [124, с. 133].

Ю. М. Грошевий, О. В. Капліна та О. Г. Шило зазначають, достовірність доказів є правильністю відображення в них фактів об'єктивної дійсності, яка є предметом досудового розслідування або судового розгляду. Іншими словами – це відповідність доказу дійсності [99, с. 190].

Під достовірністю доказу Ю.І. Лозинська розуміє його властивість, яка одержує свій вираз у формі судження, сформульованого в результаті оцінки доказу для виявлення внутрішніх або зовнішніх протиріч з іншими доказами у кримінальному провадженні, в якому констатована повна відповідність конкретних відомостей реальним фактам, котрі є предметом кримінального провадження [141, с. 165]

Достовірність означає істинність. Тому, якщо в одному джерелі доказів підтверджується те, що заперечується в іншому, то один з них достовірний, а інший ні [40, с. 59].

Достовірність доказу в кримінальному провадженні є його ознакою, яка характеризується повною відповідністю одержаних відомостей про факти реальним подіям, що відбувалися. Достовірність як ознака доказів виникає, встановлюється та існує в межах системи доказів. Визначення доказу як достовірного відбувається в результаті оцінки доказу для виявлення внутрішніх суперечностей (наприклад, в обстановці на місці події немає слідів, які мали б залишитися під час учинення кримінального правопорушення певним способом, особа під час допиту змінює свої показання стосовно тих чи інших обставин, які є предметом допиту), та супутніх їх одержанню проявів в актах поведінки та показаннях осіб дисимуляції (утаювання чогось), які спостерігаються в ході процесуальних дій як такі, що не узгоджуються із встановленими фактичними даними про конкретну подію і потребують дослідження з метою встановлення їх походження та суті виявлених неузгодженостей; та зовнішніх суперечностей, тобто неузгодженостей з іншими доказами, зібраними у провадженні. Така оцінка кожного доказу повинна розпочинатися з аналізу для виявлення внутрішніх, а

далі зовнішніх суперечностей. У випадку виявлення суперечностей не слід автоматично визнавати відомості як недостовірні. Природа (тобто, чи є такі дані результатом протидії кримінальному провадженню або ж помилки) та зміст виявлених суперечностей підлягають обов'язковому з'ясуванню й оцінці щодо їх впливу на систему зібраних доказів у кримінальному провадженні.

Отже, достовірність доказу – це властивість фактичних даних, що становлять зміст доказу, встановлювати наявність чи відсутність обставин, що мають значення для кримінального провадження, заснована на внутрішньому переконанні суб'єкта доказування, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження [100, с. 57-58].

Дана властивість доказів є самостійною відносно розглянутих вище належності та допустимості.

Однак, якщо щодо належності можна говорити про відсутність між ними зв'язку (належний доказ може бути як достовірним, так і ймовірним; і навпаки достовірний доказ може бути як належним, так і не належним), то щодо допустимості варто констатувати її безсумнівний зв'язок з достовірністю. Адже, окремі вимоги допустимості спрямовані гарантувати достовірність доказів. В таких випадках доказ буде недопустимим саме через сумніви в його достовірності, які не можуть бути усунуті. Однак, це не означає неможливість розмежування цих властивостей. Допустимість оцінюється по формальних ознаках, прямо передбачених в законі; достовірність же підлягає змістовній оцінці [95]. Якщо сумніви в достовірності є наслідком прямого порушення закону, доказ недопустимий. Коли ж такі сумніви виникають з інших причин (наприклад, неякісно проведене експертне дослідження), доказ буде недостовірним) [54, с. 366].

Яким би сумнівним не видавався доказ, він повинен бути зафіксований і підлягає перевірці й оцінці на загальних засадах. І лише наприкінці дослідження, на якомусь заключному етапі, він повинен бути мотивовано відкинутий. При цьому визнання доказу недостовірним одним суб'єктом доказування не

передбачає обов'язковість цього рішення для інших суб'єктів. Так, у випадку визнання судом недостовірними доказів, на яких ґрунтувалось обвинувачення і винесення, скажімо, виправдувального вироку в той час, коли слідчий і прокурор чи дізнавач і прокурор вважали зібрані у провадженні докази достовірними й обґрунтовували ними обвинувачення. Тобто достовірність доказів завжди визначається лише на якомусь завершальному етапі оперування ними кожним наступним суб'єктом доказування. На підставі аналізу перевірки доказів, які входять до цієї сукупності, і робиться висновок про достовірність чи недостовірність якогось конкретного доказу, причому висновок про недостовірність будь-якого доказу має бути мотивованим, обґрунтованим. Тобто діє принцип «презумпції достовірності доказу» – зібраний у кримінальному провадженні доказ вважається достовірним доти, доки в результаті його перевірки не буде встановлено протилежне – конкретний доказ недостовірний. Необхідно звернути увагу, що достовірність може бути встановлено двома шляхами: по-перше, невстановленням фактичних даних, які б вказували на недостовірність конкретного доказу (у цьому разі такий доказ необхідно вважати достовірним відповідно до принципу «презумпції достовірності доказу»; по-друге, з'ясуванням фактичних даних, які прямо або опосередковано підтверджують достовірність конкретного доказу [96, с. 70].

Встановлення достовірності чи недостовірності електронного документа може здійснюватись шляхом його зіставлення з іншими наявними доказами, або під час збирання інших доказів у кримінальному провадженні. Так, сторона обвинувачення може допитувати свідків, призначати проведення експертизи, клопотати про надання тимчасового доступу до речей і документів та проводити його, проводити обшуки, огляди тощо.

Наприклад, під час проведення досудового розслідування кримінального провадження за ознаками злочину, передбаченого ч. 2 ст. 191 КК, слідчий клопотав суд про надання тимчасового доступу до речей та документів, що містять інформацію, яка перебуває у володінні оператора мобільного зв`язку ПрАТ «Київстар», шляхом витребування електронних документів за номером

абонента. Клопотання було мотивовано необхідністю перевірки достовірності інформації, опублікованої на сайті про публічні закупівлі України «Prozorro» щодо укладання договору на виконання робіт з реконструкції спортивного майданчика на території Старомайданської філії ОЗЗСО Стрибізької ЗОШ І-ІІІ ступенів Житомирської області з влаштуванням міні-футбольного на загальну вартість 719 060 грн. [248].

У цьому випадку, відомості, які потребували перевірки на достовірність були електронними документами у вільному доступі в мережі Інтернет. Отримання інформації, яка перебуває у володінні оператора мобільного зв`язку ПрАТ «Київстар» у даному провадженні теж є електронним документом. Отже, електронний документ як доказ може також бути перевірений на достовірність за допомогою зіставлення з іншим електронним документом.

Оскільки доказ, є органічною єдністю фактичних даних та їх джерела, то й перевірка доказу в частині його достовірності має два аспекти. Перший – накопичення знань про ті ж обставини, які підтверджує чи спростовує доказ, що перевіряється, тобто, перевірка фактичних даних, другий – перевірка надійності (добротності, доброякісності) процесуального джерела. Зазначені два аспекти здебільшого реалізуються судом та іншими суб'єктами доказування одночасно: «паралельно» відбувається як накопичення знань про ті ж обставини, які підтверджує чи спростовує доказ, що перевіряється, так і перевірка надійності процесуального джерела [265, с. 94].

Науковці пропонують наступні етапи визначення достовірності фактичних даних:

– визначення достовірності джерела;

– визначення достовірності методу отримання фактичних даних;

– визначення достовірності з урахуванням інших матеріалів кримінального провадження [100, с. 59].

Встановлення достовірності електронного документа як джерела доказу може полягати у перевірці технічної справності носія технічної інформації, встановленні інформації про власника вебсайту, облікового запису у соціальній

мережі, встановлення місцезнаходження технічного пристрою у період, який становить інтерес, тощо. Наприклад, на відеозаписі (відеокамер системи зовнішнього чи внутрішнього відеоспостереження, нагрудної камери патрульного поліцейського, відеореєстратора автомобіля) може бути невірно зазначені або ж зовсім відсутні дата та час. Така неточність може з різних причин: у зв'язку неправильним функціонуванням технічного пристрою, неналаштуванням відповідних даних, внаслідок переходу з літнього на зимовий час і навпаки. У випадку, якщо пристрій був технічно несправним, то відомості, отримані з такого джерела доказу скоріш за все будуть недостовірними. Якщо збій у налаштуваннях часу не пов'язаний з технічними причинами, то достовірність такого доказу може бути підтверджена показаннями свідків (власників технічних пристроїв, учасників події), іншим відеозаписом (з іншого пристрою), електронними документами (наприклад, під час події, яка зафіксована на відео проводилась оплата через термінал банку, телефонний дзвінок, тощо), документами (які підтверджують налаштування та правильну роботу відеокамери, останньої повірки, тощо), то отримання таких відомостей в сукупності можуть підтвердити достовірність відеозапису та усунути неточності дати та часу.

Визначення достовірності методу отримання фактичних даних з електронних документів пов'язане з характеристиками та налаштуваннями інструментарію, який використовується під час огляду електронного документа (комп'ютерні програми, браузери, додатки тощо), а під час дослідження висновку експерта – характеристики заснованої ним методики аналізу.

Визначення достовірності електронного документа з урахуванням інших матеріалів кримінального провадження полягає у його перевірці з використанням уже зібраних доказів. Як зазначає Г. М. Рєзнік, остаточна достовірність окремого доказу встановлюється оцінкою не всіх існуючих доказів, а тільки тих, що стосуються одного й того ж факту [187, с. 11].

Водночас електронний документ може допомогти учасникам досудового розслідування та судового розгляду встановити достовірність чи недостовірність інших раніше зібраних доказів.

Наприклад, під час проведення досудового розслідування кримінального провадження за ознаками кримінального правопорушення, передбаченого ч.2 ст.189 КК, слідчий звернувся з клопотанням про надання тимчасового доступу до охоронюваної законом таємниці, із можливістю ознайомлення та вилучення документів та інформації, що перебуває у володінні гр. Л., а саме з електронної пошти, що перебуває в його користуванні, з адресою: інформація 1 з іменем поштової скриньки інформація 2 та доменним іменем поштового серверу інформація 3 в частині його листування з директором ПП «Західний Буг» гр. Ж., інформація 4, за період з 01.01.2018 року по час виконання даної ухвали. Своє клопотання слідчий обґрунтовував необхідністю встановлення документів та інформації, наявних у гр. Л., оскільки вона має істотне значення для встановлення обставин у цьому кримінальному провадженні і полягає у тому, що їх встановлення та вилучення надасть можливість перевірити достовірність його показів, спростувати або підтвердити їх, надасть інформацію необхідну для розслідування вказаного провадження [226].

У іншому випадку, Вищий антикорупційний суд під час встановлення достовірності показань свідка досліджував надані стороною захисту докази: роздруківка із сайту статті ОСОБА_54 ІНФОРМАЦІЯ_2, роздруківка із сайту статті Цензор.Нет «Рекордний хабар для ОСОБА_38 передав широковідомий позаштатний агент НАБУ ОСОБА_39», роздруківка з соціальної мережі «Facebook» сторінки ОСОБА_40, роздруківка із сайту http://moygrad.kiev.ua*, роздруківка із мережі інтернет та DVD-R диск, відтворений у судовому засіданні, на якому містяться файли: 1) ОСОБА_41 про обставини затримання... 2) ОСОБА_42 про НАБУ 1, ОСОБА_42 про НАБУ 2, 3) НАБУ проводить розслідування; 4) пряма лінія на КП ...1, пряма лінія на КП .2; 5) Цензор ОСОБА_39 (інтерв'ю ОСОБА_40, інтернет виданню Цензор.Нет).*

У вироці суд зазначив, що ці матеріали, здебільшого, містять публікації у засобах масової інформації, особисті погляди окремих осіб (авторів) та не можуть бути перевіреними з точки зору їхньої достовірності та об'єктивності. Більше того, в основному вони відображають громадянську позицію самого свідка ОСОБА_3 і не мають відношення до достовірності його показань та їх не спростовують. Інших показань, документів, які підтверджують репутацію свідка, зокрема, щодо його засудження за завідомо неправдиві показання, обман, шахрайство або інші діяння, що підтверджують нечесність свідка, стороною захисту не надано, а судом не встановлено [62].

Слід зауважити, що хоч обов'язок доказування в більшості випадків покладено на слідчого, дізнавача та прокурора, проте сторона захисту, потерпілий також здійснюють оцінку доказів, оскільки вона є необхідним та невід'ємним елементом процесу доказування. Тобто сторона захисту, так само, як і слідчий, дізнавач, прокурор повинна попередньо оцінити кожен поданий до суду доказ із позицій його належності, допустимості й достовірності [197, с. 107]. Сторона захисту може підтверджувати чи спростовувати достовірність електронних документів шляхом подання інших доказів, ініціювати проведення слідчих (розшукових) дій чи інших процесуальних дій через подачу клопотань та заяв, брати участь у проведенні слідчих (розшукових) дій.

Визначення достатності є найбільш складним етапом оцінювання доказів. Всі попередні етапи здійснюються саме для нього, є його передумовою. Кожний доказ, якщо його не відсіяно за якоюсь ознакою, входить до сукупності і відіграє в ній певну роль [96, с. 72].

Оцінювання достатності доказів має свої особливості. По-перше, оцінюванню достатності підлягає тільки сукупність доказів, по-друге, питання про достатність повинно вирішуватись у тісній взаємодії з питанням про значущість (силу) кожного доказу окремо та всіх у сукупності. Так, в одному кримінальному провадженні для висновків буде досить і десяти доказів, а в іншій і на підстави двадцяти не можна зробити конкретного висновку. Кількісна характеристика сукупності доказів не буде відігравати вирішального значення.

Головною тут стає змістовна характеристика наявної сукупності доказів [96, с. 72].

В.В. Вапнярчук зазначав, що достатність – це властивість, яка, на відміну від інших властивостей, характеризує не один, окремо взятий доказ, а їх сукупність. Достатність доказів означає, що на підставі певної сукупності може бути зроблений певний висновок (ймовірний чи достовірний) та прийнято відповідне процесуальне рішення в кримінальному провадженні (проміжне або кінцеве) [52, с. 290; 54, с. 372].

М.В. Дєєв сформулював визначення достатності доказів як таку властивість сукупності доказів у справі, яка викликає у суб'єкта доказування внутрішню переконаність у вірогідному встановленні наявності або відсутності обставин предмету доказування, необхідних прийняття правильного рішення у справі [97, с. 7].

Достатність доказів – це можливість суду чи органу досудового розслідування покласти їх сукупність або ж один із них в основу процесуального рішення. Цю ознаку доказів застосовують тільки до певної їх сукупності. Достатність сукупності доказів передбачає попередню оцінку кожного доказу з точки зору допустимості належності та достовірності. Докази, які не відповідають цим критеріям, не можуть бути використаними для обґрунтування будь-яких висновків, відповідно їх і не беруть до уваги під час оцінки сукупності доказів в цілому [100, с. 61].

Зовсім не обов'язково збирати всі докази, які відносяться до провадження. Збирання доказів припиняється після того, як встановлений предмет доказування в необхідних у провадженні межах. Подальше збирання доказів може спричинити невиправдане збільшення строків досудового розслідування, штучне ускладнення матеріалів, не потрібне використання часу, сил та засобів [40, с. 91-92].

Для розгляду питання достатності доказів, Р.С. Бєлкін вважає, що необхідно зупинитись на дослідженні обов'язкових доказів і джерелах доказів.

Під обов’язковими розуміють такі джерела доказів та докази, за відсутності яких неможливо зробити висновок про повне і неупереджене розслідування кримінального правопорушення, а зібрані докази – визнати достатніми. Обов’язковість наявності у провадженні тих чи інших доказів і джерел доказів в одних випадках визначається законом, в інших – теорією і практикою досудового розслідування [40, с. 91-92].

Обов’язковими джерелами доказів і доказами у провадженні по суті типові при розслідуванні тих чи інших видів кримінальних правопорушень. Це необхідно враховувати під час розробки методики розслідування окремих видів кримінальних правопорушень та включати вказівки на коло типових джерел доказів і доказів у конкретні методики [40, с. 92-93].

У зв’язку з занадто широким розумінням достатності доказів, наведеним у законі, під час прийняття процесуального рішення на практиці досить часто для прийняття найбільш важливих процесуальних рішень поняття достатності доказів зводиться до їх звичайного арифметичного обрахунку за схемою: чим більше окремих процесуальних джерел доказів (показань, речових доказів, документів, висновків експертів), тим краще. Водночас, в окремих випадках, під час розслідування кримінальних правопорушень, показань чи документів може взагалі не бути, у висновках експертів можуть бути відсутні категоричні (ствердні) відповіді на поставлені запитання, а основні сліди кримінального правопорушення збережені на речових доказах. Водночас, іноді такого доказу достатньо для прийняття, наприклад, рішення про притягнення особи для кримінальної відповідальності та застосування запобіжного заходу, однак його не достатньо для формулювання обвинувачення та складання обвинувального акту, а тому отримані такі докази необхідно використати для їх перевірки шляхом проведення відповідних слідчих (розшукових) дій [269, с. 112].

Встановлення достатності сукупності доказів здійснюється суб’єктом доказування перед ініціюванням та проведенням слідчих (розшукових) дій, негласних слідчих (розшукових) дій, інших процесуальних дій, прийняттям рішень. Достатність доказів визначається на підставі внутрішнього переконання

того чи іншого суб'єкта доказування. Одна й та ж сукупність доказів може бути визнана як достатньою (наприклад, судом першої інстанції), так і недостатньою (наприклад, судом апеляційної інстанції) [52, с. 290; 54, с. 372].

Під час досудового розслідування кримінального правопорушення можуть виникати ситуації, коли первинна кваліфікація не відповідає та не доводиться сукупністю зібраних доказів. Наприклад, сторона обвинувачення за заявою потерпілого кваліфікувала кримінальне правопорушення за ч. 2 ст. 190 КК (шахрайство, вчинене за попередньою змовою групою осіб) та почала збирати докази відповідно до предмета, котрий підлягає доказуванню у цьому кримінальному правопорушенні. Однак, на певному етапі досудового розслідування, після збирання доказів та їх оцінки встановлено, що в цій ситуації відбулась крадіжка за попередньою змовою групою осіб, яка кваліфікується за ч.2 ст.185 КК. В цьому випадку, змінюється кваліфікація кримінального правопорушення, та, відповідно, змінюється предмет доказування, а тому і сукупність необхідних доказів (обов'язкові докази та джерела доказів) для встановлення їх достатності буде іншою.

Якщо недостатність доказів буде встановлена під час судового розгляду, то суд може виправдати обвинуваченого, у зв'язку з недоведеністю вини у вчиненні кримінального правопорушення. *Наприклад, суд присяжних Шевченківського районного суду м. Києва у справі №761/10306/15-к виніс вирок, яким визнав гр. Д. винним у вчиненні злочину, передбаченого п. 13 ч. 2 ст. 115 КК, та виправдав у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 185 КК України [143]*. У даному випадку, суд виключив докази, які були визнані ним неналежними та недопустимим і через відсутність достатньої сукупності доказів виправдав особу.

Т. Руда зазначає, що при оцінці достатності доказів було б помилково орієнтуватися виключно на критерії належності, допустимості та достовірності. Достатність доказів не може встановлюватися лише шляхом механічного додавання належних за змістом, допустимих за формою та достовірних доказів. Адже подані у провадженні докази можуть бути належними і цілком

достовірними, але їх може виявитися недостатньо для того, щоб суд зміг зробити висновок про те, що певний факт дійсно мав місце (а отже, для того, щоб ухвалити рішення на користь тієї чи іншої сторони) [190, с. 107-108].

Внутрішньому переконанню під час визначення доказів достатніми належить найбільша роль. Так, визначаючи докази достатніми для прийняття рішення, вони, насамперед, повинні бути оцінені з точки зору належності допустимості та достовірності. Провівши оцінку вже наявної сукупності доказів на відповідність зазначеним критеріям, слідчий, дізнавач, прокурор керуючись саме внутрішнім переконанням повинні вирішити, чи цих доказів достатньо для прийняття відповідного процесуального рішення, чи взаємодоповнюють ці докази один одного, чи відсутні між ними будь-які суперечності, чи достатньо таких доказів для обґрунтування єдино можливого, який став ціллю (об'єктом) доказування та прийняття відповідного процесуального рішення, а також чи достатньо цих доказів для спростування інших висновків, які найбільш подібні до того, який став підставою для прийняття процесуального рішення, а також протилежного висновку тому, що був зроблений [269, с. 113].

Достовірність електронного документа перевіряється шляхом його зіставлення з раніше зібраними доказами та доказами, які необхідно зібрати в подальшому у кримінальному провадженні: допит, проведення експертизи, обшук, огляд тощо. Електронний документ також може надати можливість перевірити на достовірність інші зібрані у кримінальному провадженні докази. Встановлення достатності доказів стосується усієї зібраної сукупності доказів та залежить від наявності обов'язкових джерел доказів та доказів під час розслідування тих чи інших кримінальних правопорушень. Оцінка сукупності доказів з точки зору достатності здійснюється усіма суб'єктами доказування на підставі внутрішнього переконання.

Висновки до другого розділу

Узагальнення наукових поглядів щодо властивостей електронних документів та критеріїв їх оцінювання дає змогу зробити такі висновки:

1. Електронний документ може бути належним доказом, якщо його зміст: а) входить до предмета доказування; б) має значення доказових фактів; в) має значення допоміжних фактів.

2. Дослідження електронного документа з точки зору допустимості проводиться з урахуванням таких критеріїв допустимості, як належний суб'єкт, належний спосіб, належне джерело, належна форма закріплення відомостей про факти. Слідчий, який збирає електронні документи повинен бути уповноваженим на проведення досудового розслідування керівником підрозділу, а орган досудового розслідування, у провадженні якого перебуває кримінальне провадження, повинен відповідати вимогам підслідності.

3. До належних способів отримання електронного документа, як обов'язкового елементу допустимості, можна віднести: а) отримання добровільно; б) витребування; в) проведення слідчих (розшукових) дій; г) проведення негласних слідчих (розшукових) дій; д) проведення заходів забезпечення кримінального провадження. Обов'язкова слідча (розшукова) дія, за допомогою якої фіксується зміст електронного документа є огляд.

4. Перед збиранням електронних документів слід враховувати яким саме джерелом доказу він виступає – речовим доказом чи документом та, в залежності від цього, обирати спосіб збирання, вилучення, фіксації, зберігання. Під час отримання електронних документів, відповідна процесуальна дія повинна проводитись за участі спеціаліста та фіксуватись у протоколі і додатку до нього, оформлених згідно з вимогами КПК.

5. Оцінка електронного документа на достовірність здійснюється шляхом його зіставлення з іншими доказами, які в подальшому будуть зібрані у кримінальному провадженні, або уже наявні у ньому; перевірки технічного пристрою, за допомогою якого створювався електронний документ, на відсутність пошкоджень; перевірки програмного забезпечення та інших налаштувань; проведенням експертизи, тощо. За допомогою електронного документа може бути перевірена достовірність інших, раніше зібраних доказів.

6. Сукупність зібраних доказів може бути визнана достатньою, якщо ними встановлюється предмет доказування. Основні джерела доказів та докази, які повинні бути зібрані під час досудового розслідування встановлюються нормативно-правовими актами, методикою розслідування певного виду кримінального правопорушення з урахуванням особливостей кожного провадження.

РОЗДІЛ 3
КРИМІНАЛІСТИЧНІ ОСНОВИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

3.1. Способи збирання електронних документів у кримінальному провадженні

Враховуючи те, що нормотворча та правозастосовна практика електронного доказування в Україні перебуває на шляху становлення, відсутня чітка законодавча регламентація порядку подання, збирання, забезпечення та процесу оцінки судами електронних доказів [36].

Збирання доказів у кримінальному провадженні є важливим етапом досудового розслідування та може здійснюватись як стороною обвинувачення так і стороною захисту.

Р.В. Малюга під час дослідження суті збирання доказів, наведених різними науковцями, зазначив, що одні вважають, що це діяльність з виявлення, фіксації, вилучення і збереження різних доказів. Інші розуміють його як виявлення, збирання, фіксацію і дослідження доказів. Існує точка зору, яка полягає в тому, що пошук і виявлення доказів, а також їхнє закріплення (фіксація) складають самостійні стадії доказування. У діяльності зі збирання доказів також включають їх виявлення, збирання і закріплення. Збирання доказів розглядають як виявлення доказів, їх розгляд та процесуальне закріплення. Під збиранням доказів розуміють пошук, виявлення доказів і отримання інформації, яка в них міститься, або як пошук сприйняття і закріплення доказової інформації.

На думку Р.В. Малюги виявлення доказів полягає в їх пошуку, у зверненні уваги на ті чи інші сліди, обставини, фактичні дані, які можуть мати значення для вирішення справи. Це є початковим етапом їхнього збирання. Виявлення доказів зазвичай відбувається під час проведення слідчих (розшукових) дій. Відповідно до теорії відображення, вони виступають як сліди кримінального правопорушення, подія якого залишила їх у навколишньому середовищі [143, с. 281].

Вважаємо, що збирання доказів, джерелом яких є електронний документ, за своїм змістом полягає у виявленні і закріпленні (фіксації) його фізичної (матеріальної) частини (за можливості), або доступ до хмарного сховища, серверу, Інтернету, що і є збиранням доказів у цьому випадку.

Згідно з ч.2 ст. 93 КПК, сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених КПК.

Сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, відповідно до ч.3 ст. 93 КПК здійснює збирання доказів шляхом витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок; ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів.

Вибір способу збирання певного доказу обумовлюється передусім слідчою ситуацією і тактичним завданням, зокрема: характером наявної інформації і динамічним розвитком слідчої ситуації у конкретному кримінальному провадженні, невідкладністю, рекомендаціями методики розслідування вказаної категорії злочинів та іншими чинниками, які так чи інакше випливають із зазначених вище і їх деталізують. Нормативне закріплення їх усіх не можливе. З точки зору невідкладності, визначаючи, які докази слід отримати першочергово і якими способами доказування, передусім необхідно проводити слідчі (розшукові) дії, спрямовані на: фіксацію фактичних речових даних, які перебувають під загрозою зникнення (огляд місця події, освідування і особистий обшук затриманого тощо); попередження спроб приховати, знищити або

викривити відомості, що мають доказове значення; отримання речових доказів (обшук), що можуть мати більш повний та достовірний характер відомостей щодо встановлюваних обставин [119, с. 84].

Як зазначалось у підрозділі 2.1 дисертації, слідчий, дізнавач, прокурор може збирати електронні документи шляхом:

– надання його добровільно учасником кримінального провадження (отримання);

– витребування доказів;

– проведення тимчасового доступу до електронного документа (як заходу забезпечення);

– проведення слідчих (розшукових) дій (огляд; обшук);

– проведення негласних слідчих (розшукових) дій.

З урахуванням предмета дослідження, у даному підрозділі нами буде розглянуто основні особливості збирання електронних документів.

Надання добровільно учасником кримінального провадження. Добровільність видачі електронного документа полягає у свідомому волевиявленні, рішенні особи надати технічний носій з електронним документом, або доступ до змісту електронного документа (у т. ч. шляхом надання даних логічного захисту) стороні обвинувачення та можливе лише за відсутності ознак зовнішнього примусу.

Слідчий та дізнавач може отримати електронний документ внаслідок добровільної видачі під час проведення огляду, обшуку, або на підставі заяви чи клопотання учасника кримінального провадження. В обов’язковому порядку, особі, в якої проводиться обшук, роз’яснюється її право на добровільну видачу речей та документів, які зазначені в ухвалі на обшук. Якщо добровільно видача здійснюється під час обшуку, то недоцільно відмовлятись від проведення подальшого обшуку, оскільки слідчому та дізнавачу не завжди відомі усі обставини кримінального правопорушення, епізоди, а особи можуть приховувати чи зберігати інші предмети та речі, які можуть мати значення для кримінального провадження [259, с. 119].

Якщо сторона захисту чи потерпілий користуються своїм правом подавати докази слідчому, то, по-перше, йдеться не про докази, а про речі та документи, а, по-друге, суб'єктом одержання (збирання) доказів є слідчий або дізнавач [131, с. 244].

У КПК та інших нормативно-правових актах не наведено порядок долучення таких доказів, форму та зміст відповідного документа про долучення. Відсутність інформації про долучення, отримання, чи інший спосіб збирання доказів може спричинити визнання такого доказу недопустимим. *Наприклад, суд визнав протокол огляду предмету (фотографій) недопустимим доказом в розумінні положень ст. 86 КПК України. У даному випадку у матеріалах справи відсутні відомості про те, яким чином ці фотографії з'явилися в володінні слідчого [74]*.

З аналізу параграфів 2-5 Глави 3 КПК, можна зробити висновок, що збирати і подавати слідчому, дізнавачу, прокурору, слідчому судді докази можуть підозрюваний; обвинувачений; виправданий; засуджений; законний представник підозрюваного, обвинуваченого; захисник; потерпілий; представник потерпілого; законний представник потерпілого; представник юридичної особи, щодо якої здійснюється провадження; третя особа, щодо майна якої вирішується питання про арешт; представник третьої особи, щодо майна якої вирішується питання про арешт. Право свідка на подачу доказів у КПК не врегульоване, однак жодних обмежень також не містить.

В.В. Рогальська зазначає, що речі та документи, які мають значення для кримінального провадження та не містять охоронювану законом таємницю оформлюється протоколом про добровільне отримання речей чи документів, який треба складати відповідно до ст. 104 КПК з посиланням на ч. 3 ст. 93 КПК та ч. 2 ст. 100 КПК. Такий порядок отримання речей і документів найбільш спрощений серед усіх і відповідає КПК, що виключає в подальшому ухвалення суддею рішення про недопустимість доказів, отриманих у такий спосіб [189, с. 129].

Поширеною є практика подачі доказів учасниками кримінального провадження під час проведення допиту чи інших слідчих (розшукових) дій. Зокрема, в описовій частині протоколу допиту учасник зазначає, що у нього наявні певні електронні документи, які він має та хоче додати на підтвердження своїх показань. Т.О. Кузубова відмітила, що слідчі і прокурори нерідко отримують копії документів, що мають доказове значення, оформлюючи їх додатками до протоколу допиту. При цьому метою такого допиту може бути саме отримання копій документів, а не показань [135, с. 49-50]. На нашу думку зазначення факту добровільної видачі лише у протоколі огляду чи обшуку може призвести до визнання такого доказу недопустимим. Електронний документ слід долучати на підставі заяви чи клопотання про долучення електронного документа на фізичному носії інформації до матеріалів провадження учасником та фіксуватися за допомогою відеозапису (якщо видача здійснюється під час огляду чи обшуку де проводиться обов'язкова відеозйомка).

У зв'язку з необхідністю закріплення порядку подачі електронних документів за допомогою клопотань, пропонуємо доповнити абзац 2 ч. 3 ст. 93 КПК, та викласти його у такій редакції: Ініціювання стороною захисту, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, проведення слідчих (розшукових) дій *та подання доказів* здійснюється шляхом подання слідчому, прокурору відповідних клопотань, які розглядаються в порядку, передбаченому статтею 220 КПК. Постанова слідчого, прокурора про відмову в задоволенні клопотання про проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій може бути оскаржена слідчому судді.

Клопотання повинне містити дані слідчого або дізнавача, номер кримінального провадження, інформацію про учасника, який пише заяву чи клопотання, його статус у кримінальному провадженні, коротко інформацію про електронний документ, який долучається (що саме він може підтвердити чи спростувати), добровільність надання цього документа, перелік додатків (матеріальних носіїв, що додаються) підпис та дату. Після отримання такого

клопотання, слідчий, дізнавач повинен винести обґрунтоване рішення про задоволення або відмову у задоволенні. Тобто сам факт добровільної видачі електронного документа не означає його безумовне визнання доказом.

Наприклад, Дніпровський районний суд м. Дніпродзержинська Дніпропетровської області під час розгляду скарги потерпілої на скасування постанови про закриття кримінального провадження встановив, що нею, як потерпілою стороною слідчому було надано для долучення до матеріалів кримінального провадження аудіо-фонограми її розмов з гр. Ю. та гр. К., які підтверджували те, що гр. Ю., зловживаючи їхніми родинними стосунками, шляхом умовлянь та інших дій маніпулятивного характеру, ввівши її в оману, примусив надати йому можливість переоформити на нього квартиру, а її залишив без житла. Проте, надані потерпілою аудіо-фонограми слідчим, в порядку, передбаченому КПК, не були оглянуті та не були визнані доказами [229].

У випадку задоволення клопотання чи заяви про долучення документа до матеріалів кримінального провадження та винесення відповідної постанови, слідчий, дізнавач повинен оглянути електронний документ (його зміст) та визнати його доказом. Якщо у долученні електронного документа відмовлено, або сторона обвинувачення ігнорує подане клопотання, то учасник має право оскаржити рішення чи бездіяльність в порядку ст.303 КПК. Також, є можливість повторно звернутись з відповідною заявою чи клопотанням.

Винесення постанови про долучення чи відмову у долученні доказу пов’язана тим, що часто виникають випадки цілеспрямованого завантаження провадження непотрібними та неналежними доказами. Наприклад, долучення відеозапису тривалістю 10 год., потребує проведення подальшого його огляду, тривалість якого перевищуватиме тривалість відеозапису. В той же час, такий відеозапис може не мати жодного значення у кримінальному провадженні.

Доцільно надати слідчому, дізнавачу, прокурору можливість виготовлення будь-якої постанови в електронній формі на офіційному бланку з її засвідченням кваліфікованим електронним підписом. Така пропозиція була надана Комітету

правоохоронної діяльності Верховної Ради України в межах законопроєкту «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» (реєстр. №4003 від 01.09.2020 р.) [166] (додаток В).

Добровільно видати будь-який доказ, у тому числі електронний документ, під час досудового розслідування, учасник кримінального провадження може лише слідчому, дізнавачу, прокурору та у будь-якому випадку в межах кримінального провадження. *Зокрема, суд касаційної інстанції погодився з висновком апеляційного суду, що диск відеозапису з камер спостереження магазину, який суд першої інстанції поклав в основу обвинувального вироку, був отриманий від потерпілого не уповноваженою на те посадовою особою органу досудового розслідування – оперативним працівником, до внесення відомостей в ЄРДР без дотриманням вимог кримінального процесуального закону, а тому доводи сторони обвинувачення щодо їх допустимості є такими, що не ґрунтуються на вимогах закону [160]*.

До електронних документів, які можуть бути добровільно видані учасником кримінального провадження можна віднести відеозапис (з камер відеоспостереження, нагрудної відеокамери патрульного поліцейського, відеореєстратора автомобіля, цифрового фотоапарату, мобільного телефону, планшету, ноутбуку, тощо), цифрові фотографії (з мобільного телефону, фотоапарату, відеокамери, планшету, ноутбуку, тощо), аудіозаписи телефонних розмов, листування за допомогою смс-повідомлень, голосових повідомлень, у чаті, соціальній мережі чи іншими каналами зв'язку (з мобільного телефону, планшету, ноутбуку, тощо), відомості про вхідні-вихідні дзвінки зроблені за допомогою мобільних операторів чи інтернет-зв’язку (з мобільного телефону, планшету, ноутбуку, тощо), дані з облікових записів сторінок соціальних мереж, тощо.

Отже, добровільна видача електронного документа є реалізацією права учасників кримінального провадження на збирання і подання доказів. У зв’язку з відсутністю чіткої процедури добровільної видачі документа та відсутності

усталеної практики, можуть виникати певні труднощі під час фіксування цієї дії. Вважаємо, що заява або клопотання учасника кримінального провадження про добровільну видачу електронного документа відповідає вимогам КПК та є гарантією допустимого збирання доказів.

Під час досудового розслідування слідчий, дізнавач та прокурор можуть витребовувати електронні документи у органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб з метою збирання доказів.

В.В. Рогальська зазначає, що витребування речей та документів доречно використовувати лише тоді, коли речі та документи не містять охоронювану законом таємницю і є підстави вважати, що знищення чи зміна необхідних для кримінального провадження речей або документів не відбудеться. Наприклад, якщо володільцем речей і документів є сторона захисту, то витребування не є дієвим способом збирання доказів, оскільки в багатьох випадках особа або відмовиться від надання, або знищить такі докази [189, с. 129].

В.В. Вапнярчук зазначає, що якщо конкретизувати перелік суб'єктів у котрих можуть бути витребувані та отримані докази то, ними можуть бути:

– сторони та інші учасники кримінального провадження, які надають доказову інформацію з метою реалізації своєї процесуальної функції та впливу на напрямок пізнавальної діяльності, що відповідає їх інтересам.

– державні органи, підприємства, установи, організації (в тому числі й правоохоронні органи, зокрема, що здійснюють оперативно-розшукову діяльність), які, відповідно до закону (це може бути закон, який регламентує їх правовий статус), зобов'язані надавати доказову інформацію;

– інші особи (в тому числі й сторонні), які можуть надавати доказові матеріали (однак це не є їх обов'язком згідно із законом, а швидше за все їх моральною повинністю) [53, с. 86-87].

Ми погоджуємось з думкою Т.О. Кузубової про те, що на відміну від тимчасового доступу до речей та документів, витребування та отримання сторонами кримінального провадження речей, документів та їх копій має

фактично декларативний характер. Пояснюється це тим, що процесуальний порядок їх застосування стороною обвинувачення взагалі не регламентовано в КПК. Означене на практиці призводить до того, що вимога слідчого, прокурора, на адресу органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб не сприймаються ними як законна, що є цілком обґрунтованим з їх точки зору. В таких випадках замість інформації, речей, документів або їх копій, сторона обвинувачення отримує на свою вимогу лист про згоду видати вказане, але лише на підставі ухвали слідчого судді, суду про тимчасовий доступ до речей і документів [135, с. 53-54].

КПК та підвідомчі нормативно-правові акти не визначають форми документа, який дає можливість витребувати документи, речові докази. Поширеною є практика направлення вимоги (запиту) з проханням надати певні документи у вигляді запитів до відповідних суб'єктів [224, 232, 237, 244].

Натомість, В.В. Вапнярчук вважає, що відповідно до ч. ч. 3 і 2 ст. 110 КПК, всі рішення слідчого, прокурора приймаються у формі постанови, а судові рішення – у формі ухвали, то саме цими процесуальними документами й необхідно оформлювати витребування доказів [53, с. 87]. Існує і така практика слідчих у підготовці та направленню відповідним органам постанов про витребування документів, однак в більшості випадків вони також залишаються без відповіді, або у наданні документів відмовляють [233, 236, 243, 249].

Вважаємо, що слідчий повинен витребовувати електронні документи чи інших документи, речові докази шляхом надсилання вимоги про витребування документів та речових доказів, яка повинна бути складена на офіційному бланку, обґрунтована та направлена до відповідного органу супровідним листом. Доцільно запровадити строки розгляду такої вимоги стороною, у якої витребовуються документи та санкції у випадку необґрунтованої відмови чи неповного надання відповіді.

Тому, пропонуємо доповнити КПК ст.110-1 «Вимога про витребування документів та речових доказів» та викласти її у такій редакції: 1. Слідчий,

дізнавач, прокурор звертається з вимогою про витребування документів та речових доказів до органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб з метою збирання доказів. 2. Вимога про витребування документів та речових доказів виготовляється на офіційному бланку та підписується службовою особою, яка прийняла відповідне процесуальне рішення. 3. Вимога про витребування документів та речових доказів повинна бути складена відповідно до ч.2 ст.160 КПК. 4. До вимоги про витребування документів та речових доказів додається витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, в рамках якого подається клопотання. 5. У вимозі повинно бути зазначено строк на її виконання, який не може бути меншим 10 днів. 6. У випадку відмови в наданні документів та речових доказів, несвоєчасного або неповного надання документів та речових доказів, надання документів та речових доказів, які не відповідають дійсності на вимогу про витребування документів та речових доказів, слідчий, дізнавач, прокурор має право звернутись до суду з клопотанням про тимчасовий доступ до речей і документів.

Таким чином, витребування електронних документів є способом збирання доказів, однак не забезпечує його ефективність. Зазвичай, вимоги слідчого, дізнавача у наданні доказів ігноруються, або надається формальна відповідь про необхідність звернення до суду. Витребування електронних документів повинне здійснюватись у формі вимоги про витребування документів та речових доказів з дотримання вимог КПК та надсилатись до належного суб'єкта супровідним листом.

Тимчасовий доступ до електронних документів може проводитись, якщо наперед чітко відомі назва й такі характеристики електронного документа, що дають можливість виокремити її або його із числа подібних, відомий її чи його володілець. У такому випадку існує передумова для використання поза слідчими (розшуковими) діями таких способів збирання доказів, як тимчасовий доступ до речей і документів [119, с. 85].

Ми погоджуємось з думкою Д.Б. Сєргєєвої та О.В.Шаповал, що виходячи із розуміння, сутності та призначення, тимчасовий доступ до речей та документів є процесуальною дією, що має виключно забезпечувальний характер, оскільки в результаті її провадження слідчий, дізнавач тільки отримує об'єкти, що в подальшому підлягають огляду або експертним дослідженням. Саме за результатами огляду або експертизи слідчий, дізнавач може виявити й закріпити фактичні дані й відомості про їх джерела для отримання доказів або для перевірки цих доказів. Лише подальший огляд або експертні дослідження мають пошуково-пізнавальний характер, а також відповідають іншим сутнісним ознакам слідчої (розшукової) дії [198, с. 115].

Згідно із п. 18 Інформаційного листа Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 05.04.2013 р. беручи до уваги зміст положень ч. 1 ст. 86, частин 2 та 3 ст. 93 КПК, застосування стороною кримінального провадження такого способу збирання доказів як вилучення речей чи документів (ч. 7 ст. 163 КПК) під час отримання доступу до речей і документів може здійснюватися у випадках, якщо:

– особа, у володінні якої знаходяться речі або документи, не бажає добровільно передати їх стороні кримінального провадження або є підстави вважати, що вона не здійснить таку передачу добровільно після отримання відповідного запиту чи намагатиметься змінити або знищити відповідні речі або документи;

– речі та документи згідно зі ст. 162 КПК містять охоронювану законом таємницю і таке вилучення необхідне для досягнення мети застосування цього заходу забезпечення.

В інших випадках сторона кримінального провадження може витребувати та отримати речі або документи за умови їх добровільного надання володільцем без застосування процедури, передбаченої главою 15 КПК [167].

Проведення тимчасового доступу до електронних документів передбачає підготовчий, робочий та завершальний етапи.

На підготовчому етапі тимчасового доступу до електронних документів слідчий, дізнавач встановлює відомості про електронний документ (назва, дані про фізичний носій інформації, на якому він знаходиться, дані власника та його місцезнаходження), готує клопотання про тимчасовий доступ та подає його на розгляд суду. Після отримання рішення суду, необхідно визначити дату та час проведення тимчасового доступу, підготувати технічні носії інформації, які будуть необхідні для копіювання електронних документів з розрахунку необхідного об'єму пам'яті. Обов'язково слід залучати спеціаліста, так як є необхідність у копіюванні електронного документа, або ж судом задоволено клопотання про вилучення оригіналу.

Робочий етап тимчасового доступу до електронних документів полягає у виконанні слідчим, дізнавачем ухвали. Спочатку володільцю електронних документів пред'являється копія ухвали, яка в подальшому залишається у нього. Після цього, володілець електронних документів зобов'язаний надати тимчасовий доступ до зазначених в ухвалі електронних документів особі, зазначеній у відповідній ухвалі слідчого судді, суду.

Завершальний етап полягає у фіксації ходу тимчасового доступу до електронних документів та виготовленні копій чи вилученні оригіналів електронних документів. Так як копіювання електронних документів на інший матеріальний носій інформації та вилучення електронних документів потребує спеціальних знань, то воно повинно здійснюватися спеціалістом, з відображенням необхідної інформації у протоколі та складених до нього додатках.

Тимчасовий доступ може проводитись коли є необхідність отримання оригіналів електронних документів та їх копіювання.

Наприклад, слідчий звернувся до суду з клопотання про надання доступу до речей та документів, котрі перебувають у володінні Управління патрульної поліції в Луганській області Департаменту патрульної поліції, з можливістю їх копіювання, а саме до електронних інформаційних систем або їх частин, до програмно-апаратного комплексу (Hardware-software complex including): до усіх

відеозаписів з нагрудних відео реєстраторів № 129, № 137, № 110 та № 107, що знаходились на форменому одязі командира взводу та поліцейського, на яких зафіксовані події, що мали місце 12.07.2019 року [244].

Інформація з нагрудних відеореєстраторів, котра зберігається в електронній інформаційній системі має обмежений термін зберігання. Проблеми з копіюванням відеозапису та подальше його знищення, може призвести до втрати доказів, без яких іншими способами не можливо довести обставини, які передбачалось встановити. Тому, проведення тимчасового доступу до речей та документів може забезпечити отримання необхідних доказів.

Існує декілька поширених порушень вимог застосування тимчасового доступу до речей та документів з практики ЄСПЛ. Перший приклад – це отримання доступу до інформації без ухвали слідчого судді. Такі ситуації особливо поширені, коли в ході проведення обшуку житла чи офісу, на який було отримано рішення суду, вилучаються як тимчасово вилучене майно на підставі ст. 168 КПК, мобільні телефони. Надалі таке майно арештовується і цього, на думку правоохоронних органів, достатньо для використання наявної в мобільному телефоні інформації. Більш того, часто один лиш факт того, що доступ до інформації на телефоні не захищений паролем, розглядається слідчими, дізнавачами або детективами, як достатня підстава для її безперешкодного використання.

Проте ні ухвала про обшук, ні ухвала про арешт мобільного телефону не надає автоматичний дозвіл на доступ до наявної в ньому інформації, оскільки у жодному із зазначених рішень не досліджується питання щодо законності та необхідності таких дій. Так, слід зазначити, що згідно з практикою ЄСПЛ надто широке тлумачення змісту ухвал, винесених слідчим суддею, зокрема вчинення дій, що не були чітко передбачені такими ухвалами є окремою підставою для констатації ЄСПЛ порушення ст. 8 Конвенції про захист прав людини і основоположних свобод (рішення у справі «Hambardzumyan v. Armenia», заява № 43478/11, пп. 65–66 [207]). З тих же міркувань немає жодного значення, чи доступ до інформації на телефоні захищено паролем, чи ні. Перегляд, копіювання та

використання такої інформації є втручанням в право на повагу до приватного життя. Відтак, єдино можливим способом використання наявної на вилученому телефоні інформації є отримання з цією метою окремої ухвали суду, в якій буде чітко вказано, доступ до якої інформації надається. Відсутність такої ухвали автоматично тягне за собою порушення прав, гарантованих ст. 8 Конвенції про захист прав людини і основоположних свобод, а відтак і, згідно зі ст. 87 КПК, недопустимість як доказу вилученої з телефону інформації (документів) [41].

Ми не погоджуємся з думкою А.О. Просняка, який зазначає що для фіксації вмісту електронного листування месенджерів, встановлених у сучасних смартфонах недоцільно клопотати суд про тимчасовий доступ до речей, які знаходяться у його ж володінні, адже це суперечить суті даного заходу забезпечення [176, с. 215].

Як зазначає А.В. Шило, інформація, яка міститься на електронних пристроях, не може ототожнюватися із самим електронним пристроєм як її фізичним носієм. Відповідно, така інформація є окремим об’єктом права власності та об’єктом охорони таємниці приватного життя, а відтак її вилучення, копіювання має відбуватися на підставі судового рішення, проте не в режимі застосування негласних слідчих (розшукових) дій. У зв’язку з цим слід зазначити, що в науці кримінального процесу висловлювалася думка про те, що отримання та фіксування такої інформації має здійснюватися на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів (у даному випадку – документів, що існують в електронній формі) [268, с. 109].

Наприклад, під час розгляду клопотання про надання дозволу на проведення тимчасового доступу до документів Жовтневий районний суд м. Дніпропетровська встановив, що серед майна, вилученого в ході обшуку клубу «Потемкин» був мобільний телефон гр. П. Останній надав документи, які підтверджують придбання вказаного телефону. Встановлено, що в приміщенні клубу «Потемкин» під час виступів оголених артистів відвідувачі закладу здійснювали зйомку своїми особистими телефонами відео, котрі згідно проведеним експертизам містять елементи порнографічного характеру. На

теперішній час гр. П. відмовляється добровільно надавати на огляд свій мобільний телефон, та приховує його зміст, а в своїх показаннях говорить, що жодного разу не бачив артистів, які виступали з оголеними статевими органами на сцені клубу «Потемкин».

Орган досудового розслідування зазначив, що для подальшого проведення досудового розслідування цього кримінального провадження, та встановлення всіх обставин справи, необхідно оглянути мобільний телефон гр. П. та встановити, чи знімав він виступи артистів з оголеними статевими органами в клубі «Потемкин», чи отримував в листуванні з власником клубу відео та фото порнографічного характеру, оскільки вказані відомості мають доказове значення за матеріалами кримінального провадження.

Ухвалою Жовтневого районного суду м.Дніпропетровська від 26.06.2019 року, суд надав слідчому тимчасовий доступ до речей, які містять охоронювану законом таємницю (відомості про особисте листування та інші записи особистого характеру), які зберігаються в належному гр. П., мобільному телефоні, вилученому під час обшуку клубу «Потемкин», з можливістю ознайомлення з ними та зняти їх копії, а саме: листування з використанням електронної пошти змісту спілкування (листування) в програмному забезпеченні, що встановлене в мобільному телефоні та забезпечувало можливість передачі даних (Viber, Telegram, WhatsApp, Gmail, Google, Фото) і стосуються зв'язків та/або листування між власником клубу та іншими особами, які відвідували клуб «Потемкин» [230].

До основних слідчих (розшукових) дій, за допомогою яких сторона обвинувачення може збирати докази відносимо огляд та обшук.

Електронний документ можна отримати під час проведення огляду місця події, місцевості, приміщення, тощо. Кожен огляд має свої специфічні особливості, що визначають тактику його проведення. Однак, в той же час будь-який огляд місця події умовно можна розділити на три етапи: підготовчий, робочий, завершальний. Такий поділ не порушує цілісності цієї слідчої (розшукової) дії та забезпечує реалізацію загальних положень тактики огляду.

Зміст поділу на етапи полягає в тому, щоб систематизувати дії слідчого, дізнавача встановити їхню послідовність, забезпечити якість огляду [128, с. 163].

Огляд, як спосіб збирання електронних документів в загальному відповідає усім вимогам, які застосовуються до огляду місця події, приміщення, тощо. Проте, є певні особливості у кожному етапі такого огляду.

Підготовчий етап огляду, окрім стандартних, полягає у вирішенні таких питань:

- яке комп'ютерне обладнання / операційна система / програмне забезпечення / програми та носії інформації, обладнання для зв'язку та мережі (мережеве обладнання LAN / WLAN), ймовірно бути знайденим?
- хто відповідає за комп’ютерну систему та / або мережу (наприклад, чи існує локальна адміністратором або системою керує зовнішня компанія)?
- скільки обладнання може бути?
- скільки даних може бути потрібно скопіювати?
- чи доступна резервна копія системи на носії інформації? [8, с. 39]

До основних інструментів, які можуть знадобитись, закордонні науковці відносять: викрутки (плоскі та хрестові, а також специфічні для виробника (наприклад, Hewlett Packard, Apple)); гайкові ключі (шестигранний, зіркоподібного типу); плоскогубці (стандартні та голчасті); дроторізи (для зняття кабельних стяжок); маленький пінцет [8, с. 40]. Також можуть знадобитись під час огляду: кабелі, зовнішні жорсткі диски різного об’єму, флеш-карти.

Надалі, як слідчий, дізнавач підготує необхідну кількість технічних засобів, засобів для вилучення та пакування обладнання пристроїв, технічних носіїв інформації, вирішить питання про залучення спеціаліста/спеціалістів та понятих, проводиться інструктаж осіб-учасників слідчої (розшукової) дії. Якщо у місці, де проводиться огляд (офіс, компанія) є системний адміністратор, або технічний експерт, то слідчий, дізнавач може розглянути можливість залучення їх як спеціаліста (якщо така особа не розглядається як ймовірний підозрюваний, співучасник та не має іншого конфлікту інтересів).

Наступний, робочий етап полягає у проведенні таких дій:

— вжиття заходів щодо збереження ситуації такою, якою вона була до моменту прибуття з метою запобігання знищенню інформації: вивести всіх осіб із зони доступу до обладнання, запобігти втручанню у систему через лінії зв'язку (зокрема, через модеми), а також внесення змін у роботу системи. Якщо в приміщенні знаходяться декілька комп’ютерів, об’єднаних між собою в мережу, слідчий, дізнавач повинен попросити осіб, які за ними працюють, залишити місця роботи і відійти від цих комп’ютерів;

— проведення відеозапису місця події для фіксації поточного стану операційної системи комп’ютера та порядку розташування його обладнання;

— проведення фотозйомки серійних номерів та номерів моделей комп'ютерного обладнання;

— нумерація комп’ютерного обладнання відповідно до його розташування на місці події [4].

Важливо вимкнути WI-FI у приміщенні, щоб унеможливити зміну даних з інших пристроїв; залишити пристрої у тому стані, в якому вони перебували на момент виявлення (ввімкнені чи вимкнені), провести пошук речових доказів та інших документів, котрі можуть містити важливу інформацію (блокноти, щоденники, текстові роздруківки, записані паролі чи інші паперові примітки) тощо. Слід звернути увагу на те, що деякі технічні пристрої не завжди можна легко виявити, оскільки вони можуть мати вигляд брелків, іграшок, канцелярських товарів, годинників і т.п.

У протоколі огляду слід обов’язково зазначати марку, модель, серійний номер обладнання, типи підключень до пристрою (якщо такі наявні), місце розташування пристроїв, стан живлення (увімкнений/вимкнений), вигляд екрану монітора, тощо. Під час проведення огляду важливо забезпечити фотографування усіх важливих елементів та деталей місця. За необхідності, за допомоги спеціаліста можна накреслити схему з’єднань комп’ютерного обладнання, кабелів [8, с. 48-51].

В протоколі слідчої (розшукової) дії та додатку-схемі до нього ретельно фіксується місцезнаходження комп’ютера і його периферійних приладів,

описується порядок з'єднання між собою вказаних приладів, із зазначенням особливостей (колір, кількість з'єднувальних роз'ємів, їх специфікація) з'єднувальних проводів і кабелів; перед роз'єднанням корисно здійснити відеозапис чи фотографування місць з'єднань [139, с. 53].

На завершальному етапі важливим є пакування носіїв електронних документів. Вилучення та пакування повинно проводитись відповідно до вимог, що встановлюються для речових доказів, з урахуванням особливостей електронних документів. Під час пакування пристроїв, найбільш доцільно використовувати оригінальне пакування, якщо таке є. Якщо оригінального пакування немає, то використовувати антистатичне пакування, тобто таке пакування повинно унеможливлювати пошкодження, викликані електростатичним розрядом [8, с. 48-49]. Опечатуються тільки контейнери, коробки, або футляри. Пояснювальні записи можуть наноситись лише на ярлики, на яких має бути зафіксована інформація про перелік записаних файлів; паролі, необхідні для відкриття даних файлів; назву операційної системи, якій належать записані файли; інформацію про можливий чи наявний зміст файлу [139, с. 54].

В жодному разі не можна: використовувати клейкі етикетки на поверхню носія інформації; робити надписи на поверхні такого носія; дряпати, згинати чи іншим чином пошкоджувати носії інформації; використовувати матеріали, котрі можуть виробляти статичну електроенергію (наприклад, поліетиленові пакети) [8, с.48-49]. Усе обладнання повинно бути підписано за допомогою ярликів.

Відомості можуть мати доказове значення, якщо вони зберігаються в тому стані, в якому вони були вилучені без будь-яких модифікацій або змін. Тому, під час роботи з такими електронними пристроями як мобільні телефони, популярним є використання коробки Фарадея, яка блокує зовнішні сигнали (WI-FI, 4G) [3; 8, с. 40]. Окрім, коробки Фарадея експерти також використовують порожні металеві балончики для фарби (основним є герметичне упакування) та алюмінієву фольгу, якою пристрій обмотується декілька разів [3]. Мобільний телефон слід упаковувати у стані живлення (увімкненому чи вимкненому), в якому його було знайдено. Утримання мобільного телефону у ввімкненому стані

може значно скоротити час автономної роботи. У випадках низького заряду акумулятора пристрій можна перевести в режим польоту [8, с. 48-49].

До протоколу огляду електронного документа обов'язково повинен створюватись додаток до протоколу з записом проведеного огляду. Порушення вимог збереження оригінальних примірників технічних носіїв інформації зафіксованої процесуальної дії тягне за собою визнання їх недопустимими.

Наприклад, під час прийняття ухвали Бершадським районним судом Вінницької області, СД - диск, який містить відеозапис огляду місця події визнано недопустимим доказом та виключено можливість його дослідження в судовому засіданні в якості доказу. Вказану ухвалу суд обґрунтував через відсутність ідентифікуючих ознак відеокамери у протоколі огляду, ненадання такої відеокамери на вимогу суду та неможливість встановлення чим саме є відеозапис – оригіналом чи копією. Тому, суд не зміг встановити джерело походження такого доказу [223].

Також, електронні документи можуть бути отримані під час проведення **обшуку.**

Обшук проводиться відповідно до вимог КПК та з урахуванням особливостей, які нами наведені вище для проведення огляду.

Важливим під час обшуку є підготовка та отримання клопотання на проведення обшуку. Оскільки до проведення обшуку невідомо чи надасть особа доступ до особистого листування, яке міститься на технічних пристроях, то під час складання клопотання про проведення обшуку, у ньому треба обов'язково зазначати необхідність відшукання комп'ютерів, мобільних пристроїв, планшетів та надання доступу до відомостей які на них зберігаються та містять охоронювану законом таємницю.

Інформація у даному випадку є окремим об'єктом, який не слід ототожнювати з її фізичним носієм – електронним пристроєм [152, с. 77].

Наприклад, у справі, яка розглядалась Солом'янським районним судом м. Києва, адвокат оскаржував законність огляду мобільного телефону проведеного детективами НАБУ під час обшуку квартири. Зокрема, у своїй

скарзі зазначив, що детектив НАБУ не отримував дозвіл на тимчасовий доступ до речей і документів до моменту огляду телефону для проведення ефективного контролю з боку суду.

Однак, суд відмовив у задоволенні скарги та зазначив, що згідно ч. 7 ст.236 КПК, при обшуку слідчий, прокурор має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення обшуканого житла чи іншого володіння особи чи окремих речей, виготовляти відбитки та зліпки, оглядати і вилучати документи, тимчасово вилучати речі, котрі мають значення для кримінального провадження. Дозвіл на проведення обшуку отримано з метою відшукання та вилучення предметів, документів, пристроїв, котрі містять інформацію про постачання на користь OSUNA Holding LLP та GLD Trade Holding LLP деревини, в тому числі мобільних телефонів, мобільних терміналів систем (у випадку неможливості копіювання, якщо доступ до них обмежується їх власником, володільцем або утримувачем), що було зазначено в ухвалі. Окрім того, власник мобільного телефону добровільно надав його детективам для копіювання з нього інформації.

Оскільки детективу під час проведення обшуку було надано дозвіл на копіювання та вилучення інформації з мобільного телефону, а володільцем цього майна це не заперечувалося, слідчий суддя прийшов до висновку, що детектив діяв в межах наданого йому дозволу ухвалою від 18.04.2019 та в межах дискреційних повноважень, передбачених нормами КПК [245].

У іншій справі, Андрушівський районний суд Житомирської області встановив, що під час обшуку гр. Я. добровільно надав свій телефон марки «Самсунг» з сім карткою Київстар, окрім цього вилучено мобільний телефон марки «Самсунг» із сім картою Лайф та у кімнаті квартири виявлено комп'ютер, який добровільно гр. Я. увімкнув та здійснив вхід через браузер Опера на власну сторінку у соціальній мережі «Вконтакте». Під час обшуку було оглянуто листування з наступними користувачами: «гр. О.», «гр. А.», «гр. М.», «гр. Х.». Окрім цього, під час огляду сторінки встановлено, що вказаний

користувач є засновником групи «Вільна Житомирщина, адміністратором групи «Правильное ТВ», засновником групи «Ми не скачем ми москаль» та редактором групи «17 канал». Заяв та зауважень з приводу обшуку від понятих, учасників не надходило. Під час судового розгляду обвинувачений гр. Я. підтвердив, що добровільно увімкнув та здійснив вхід через браузер Опера на власну сторінку у соціальній мережі «Вконтакте» [60].

Отримання дозволу суду на вилучення предметів, документів, пристроїв, які містять кримінально-значиму інформацію, в тому числі мобільних телефонів, мобільних терміналів систем (у випадку неможливості копіювання, якщо доступ до них обмежується їх власником) пришвидшує і полегшує подальшу роботу сторони обвинувачення. В цьому випадку немає необхідності звертатись за санкцією суду на отримання доступу до такої інформації після вилучення технічних пристроїв, що зменшує кількість необхідних дій та скорочує час їх проведення.

Ми погоджуємось з думкою Є.С. Хижняка, що фізичні носії електронної інформації, на котрих може знаходитись криміналістично важлива інформація, слід вилучати під час огляду місця події, оглядах та обшуках житла чи робочих приміщень, під час огляду речей та комп'ютерної техніки учасників кримінального провадження. Проте, якщо електронні докази розміщені на серверах чи жорстких дисках підприємств, установ або організацій, слідчому рекомендується здійснити побайтову копію носія інформації, адже вилучення майна підприємства може призвести до негативних наслідків [255, с. 82].

Аналогічно, якщо власником електронного документа, який знаходиться на носії комп'ютерної інформації (комп'ютер, планшет, телефон), є фізична особа, котра постійно використовує його у повсякденному житті, то цей носій не обов'язково підлягає вилученню. В окремих випадках вилучення цифрових носіїв інформації може спричинити завдання незручностей або й шкоди його власникам (користувачам).

Згідно з ч. 3 ст. ст.100 КПК, за клопотанням володільця документа за необхідності слідчий, прокурор, суд можуть видати оригінал документа (у тому

числі електронного документа), долучивши замість них до кримінального провадження завірені копії.

У цьому випадку, після проведення огляду електронного документа, власника чи володільця електронного документа слід зобов'язати зберігати електронний документ у такому ж стані до завершення досудового розслідування та судового провадження, недопустити пошкодження, зміни чи знищення електронного документа за цей час. Також, за участі спеціаліста та володільця електронного документа виготовити його копію, яку долучити до матеріалів кримінального провадження.

До негласних слідчих (розшукових) дій, за допомогою здійснюється збирання електронних документів можна віднести: проведення аудіо-, відеоконтролю особи (ст. 260 КПК), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК), зняття інформації з електронних інформаційних систем (ст. 264 КПК), установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК), спостереження за особою, річчю або місцем (ст. 269 КПК), моніторингу банківських рахунків (ст. 269-1 КПК), аудіо-, відеоконтролю місця (ст. 270 КПК), контролю за вчиненням злочину (ст. 271 КПК) [130; 156, с. 15-16].

Зняття інформації з транспортних телекомунікаційних мереж полягає у спостереженні та фіксації змісту інформації уповноваженими оперативними підрозділами: за адресою в мережі передачі даних із комутацією пакетів (IP-адреса в мережі Інтернет); за апаратною адресою пристрою, приєднаного до мережного середовища (MAC-адреса); за адресою електронної пошти.

Зняття інформації з електронних інформаційних систем – полягає у виявленні і фіксації відомостей, що містяться в електронній інформаційній системі шляхом: безпосереднього (фізичного) доступу або віддаленого (програмного) проникнення [49, с. 122].

Зняття інформації з електронних інформаційних систем або їх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням

системи логічного захисту. Наприклад, огляд текстових повідомлень, які знаходились в мобільному телефоні та доступ до яких не був пов’язаний із наданням володільцем відповідного серверу (оператором мобільного зв’язку) доступу до електронних інформаційних систем [122].

Складність проведення таких негласних слідчих (розшукових) дій як зняття інформації з транспортних телекомунікаційних мереж та зняття інформації з електронних інформаційних систем може полягати у захищеності каналів передачі даних, використання правопорушниками спеціального, програмного чи апаратного забезпечення обчислювальної техніки [271, с. 88].

Після отримання матеріальної частини електронного документа чи доступу до нього, необхідно отримати відомості, які на ньому містяться. Для цього, в основному слідчий, дізнавач проводять таку слідчу (розшукову) дію як огляд. Проведення **огляду** електронного документа повинно здійснюватись в порядку ст. 237 КПК з оформлення відповідного протоколу.

Науковці зазначають, що не останню роль у дослідженні кіберпростору відіграє огляд документів, оскільки наявні форми передачі інформації передбачають можливість використання електронного документообігу. Матеріали фотозйомки, звукозапису, відеозапису, що містяться в кіберпросторі, мають бути досліджені як документи, та виявлена інформація у відповідній формі зафіксована і долучена до матеріалів кримінального провадження [98, с. 74].

Процес огляду електронних документів в цілому відповідає загальноприйнятому алгоритму дій, які вчиняються слідчим, дізнавачем під час огляду звичайних документів. Такий комплекс дій повинен складатися з наступного: 1 — пошук і виявлення документів; 2 — візуальний огляд зовнішнього стану без зміни умов сприйняття; 3 — фіксація за допомогою фотозйомки; 4 — фіксація в протоколі відповідної слідчої дії (фіксуються всі дії посадових осіб, стан документа і виявлені сліди); 5 — виявлення слідів рук (на фізичному носії електронного документа); 6 — виявлення слідів зміни первісного змісту; 7 — підготовка до упаковки; 8 — упаковка [48, с. 129].

Проте, тактика огляду «традиційних» документів відрізняється від тактики огляду електронних документів. Зокрема, під час проведення опитування працівників практичних підрозділів Національної поліції 89,8% опитаних вважає, що між цими оглядами існують суттєві відмінності, натомість 7,2% вважає що відмінності несуттєві і лише 3% вважає що відмінностей немає (додаток А).

Більшість науковців вважають, що до огляду електронних документів слід залучати спеціалістів (комп'ютерного техніка чи програміста). Доцільніше залучати в якості спеціалістів тих осіб, які подальшому будуть проводити відповідні судові експертизи [177, с. 134]. Під час опитування працівників практичних підрозділів Національної поліції України 64,7% усіх опитаних зазначили, що під час збирання та дослідження електронних документів необхідно залучати спеціаліста, 32,4% опитаних зазначили, що спеціаліста слід залучати в окремих випадках і лише 2,9% опитаних вважають що спеціаліста залучати не потрібно (додаток А).

Ми погоджуємося з такою думкою, оскільки для всебічного, повного й неупередженого дослідження електронного документа, необхідне обов'язкове залучення спеціаліста чи експерта. Особа, яка має певні знання у галузі комп'ютерних технологій може звернути увагу на певні особливості електронного документа, допомогти проаналізувати його, розкодувати та у деяких випадках вибрати найбільш доцільну програму яка допоможе представити інформацію у необхідній формі.

Так як електронний документ це певний комп'ютерний код, то такий код може бути прочитаний лише за допомогою спеціальних засобів, які забезпечують тлумачення цифрового коду та його перетворення в доступну для сприйняття форму. Така особливість електронного документа як доказу зумовлює особливість його слідчого огляду як окремої процесуальної дії.

О.В. Шведова зазначає, що результат експертного дослідження багато в чому залежить від своєчасного та якісного проведення слідчих дій (огляду, обшуку, виїмки і ін.), тому слідчий, дізнавач має здійснити низку обов'язкових підготовчих заходів (запросити учасників огляду, підготувати технічні засоби

тощо). А у справах, пов'язаних з комп'ютерними технологіями, участь у слідчих діях спеціалістів взагалі є обов'язковою [266, с. 10].

Є.С. Хижняк звертає увагу на те, що слідчий, дізнавач огляд електронних документів здійснюється з урахуванням певних особливостей об'єкта дослідження, що впливає як на сам процес дослідження, так і на спосіб процесуального закріплення отриманих результатів.

Він вважає, що під час огляду слід врахувати «вразливість» електронного доказу, яка полягає у його зміні, модифікації чи знищенні без будь-яких очевидних ознак. Вразливість електронного документа зумовлює необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи [255, с. 82].

Дослідження електронного документа не може проводитись без спеціальних засобів, а тому, як правило, така процесуальна дія здійснюється за допомогою спеціального обладнання на робочому місці слідчого. При цьому огляд та дослідження фізичного носія електронного документа не є дослідженням самого електронного документа. В такому випадку, фізичний носій може виступати лише в якості речового доказу [255, с. 82]. А.В. Коваленко зазначає, що будь-які дії з електронними документами мають здійснюватися уповноваженими особами за допомогою сертифікованого службового обладнання, з використанням ліцензійного програмного забезпечення. Використання несертифікованого обладнання або неліцензійного програмного забезпечення може призвести до викривлення інформації, отриманої з електронного документа через апаратні та/або програмні збої та помилки [122, с. 184].

До основних інструментів, які можуть знадобитись для огляду засобів комп'ютерної техніки відносять портативний комп'ютер з автономним джерелом живлення, привод CD-ROM (DVD-ROM); викрутки та інший інструмент, комплекти запасних батарей, диски з операційними системами та іншими програмними засобами, накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду,

блокувач жорсткого диску та/або набір дублікаторів, польовий комплект експерта криміналіста тощо.

Перелік інструментарію залежить від конкретної ситуації. Після підготовки відповідного інструментарію, який можна вважати підготовчим етапом огляду, проведення інших підготовчих заходів, працівники правоохоронного органу переходять безпосередньо до збирання даних [85, с. 104].

Огляд електронних документів, розміщених на фізичному носії інформації, здійснюється шляхом безпосереднього сприйняття слідчим, дізнавачем інформації, що міститься в електронному документі, за допомогою службового комп'ютера [122, с. 186]. В змісті самого протоколу огляду варто зазначити технічні характеристики та серійні номери обладнання, назви та версії програмного забезпечення, що використовуються в ході слідчого огляду [255, с. 82-83].

Під час проведення робочого етапу огляду слідчий, дізнавач вивчає та аналізує зміст документа, його метадані. Якщо документ має великий обсяг, слідчий, дізнавач може зафіксувати у протоколі лише найважливішу інформацію. В процесі огляду електронного документа доцільно проводити фотографування чи відеозапис послідовності проведених дій (відкриття файлу, отримання інформації по властивостях документа) та самого змісту документа, яке потім оформити у вигляді фототаблиці, відеозапису, носія комп'ютерної інформації тощо.

На завершальному етапі огляду слідчий, дізнавач ознайомлює учасників зі змістом протоколу, аналізує зауваження і доповнення до письмового протоколу з боку учасників процесуальної дії, проводить копіювання, дублювання інформації на технічний носій.

До протоколу огляду електронного документа слідчий, дізнавач складає додаток до протоколу, який також має важливе значення і є нерозривним з інформацією що міститься на ньому. Додатки до протоколу повинні бути належним чином виготовлені, упаковані з метою надійного збереження, а також

засвідчені підписами слідчого, прокурора, спеціаліста, інших осіб, які брали участь у виготовленні та/або вилученні таких додатків (ч.3 ст.105 КПК).

У матеріалах кримінального провадження зберігаються оригінальні примірники технічних носіїв інформації зафіксованої процесуальної дії, резервні копії яких зберігаються окремо (ч.3 ст.107 КПК).

Враховуючи особливості роботи із комп'ютерною технікою, а також відповідне апаратне та програмне забезпечення, використовуване для їх огляду, відповідний процес можна умовно групувати за такими категоріями:

1) електронні документи на фізичних носіях інформації;

2) електронні документи у вигляді публікацій у мережі Інтернет;

3) електронні документи, розміщені у хмарних сервісах зберігання інформації [122, с. 184].

До фізичних носіїв інформації, на яких можуть знаходитись електронні документи відносять стаціонарні персональні комп'ютери; ноутбуки та нетбуки; планшети; бортові комп'ютери автомобілів; «розумну» побутову техніку; «розумні» годинники; GPS-навігатори; носії цифрової інформації (диски, дискети, флеш-носії тощо); периферійне обладнання (принтери, сканери тощо); мобільні телефони; тощо.

На підготовчому етапі огляду електронних документів, розміщених на фізичному носії інформації, слідчому, прокурору рекомендується з'ясувати, якого типу фізичний носій інформації містить документи, що підлягають огляду та, відповідно, яке обладнання потрібне для роботи з таким носієм. Якщо носій захищено будь-яким типом захисту від зчитування чи копіювання, слід призначити судову експертизу комп'ютерної техніки і програмних продуктів та поставити перед експертом питання про можливість отримання доступу до вмісту такого носія, файлів, що розміщені на носії та їх атрибутів. За допомогою такої експертизи також можливо встановити технологію та хронологію створення конкретного електронного документа [28].

А.В. Коваленко звертає увагу на огляд електронних документів, розташованих у пам'яті мобільних пристроїв. Сучасні мобільні телефони й

смартфони оснащені функцією запису звуку (диктофон) та запису розмови, за допомогою яких створюються аудіозаписи, які можуть містити відомості, що мають значення для кримінального провадження. Крім того, за допомогою мобільного пристрою можуть створюватися фото- та відеозаписи, які також потребують огляду та попереднього дослідження [122, с. 185].

Під час огляду засобів комп'ютерної техніки із функцією телефону необхідно оглянути:

- телефонну та адресну книгу;
- записну книжку;
- короткі текстові повідомлення в телекомунікаційних мережах (смс);
- короткі мультимедійні повідомлення зі змістом повнокольорового зображення, фотографій, мелодій, відеокліпів (ммс);
- текстові та мультимедійні повідомлення різних додатків;
- аккаунти у соціальних мережах;
- журнал повідомлень, де зберігаються повідомлення системи, які користувач міг не зауважити;
- додатки з функцією запису розмови;
- нотатки зі списками зустрічей і справ;
- нагадування про події;
- спортивні додатки;
- фотогалерея де зберігаються фотографії зроблені користувачем, та які направлені до користувача, знімки екрана, анімації, відеозйомка; приховані та нещодавні видалені колекції;
- календар де накопичуються нагадування про події, зустрічі;
- диктофон, де зберігаються записи;
- історія перегляду інтернет-сторінок;
- електронна пошта;
- мобільний додаток служби таксі; мобільний додаток залізничних та авіаційних послуг [147, с. 56-57].

Є.С. Хижняк зазначає, що Інтернет, соціальні мережі, електронне листування останнім часом стає одним з найголовніших джерел інформації, яка має значення для розслідування злочинів [255, с. 83].

А.В. Коваленко приділяє увагу огляду електронних документів, розміщених в мережі Інтернет. Зокрема, він вважає за доцільне у протоколі огляду зазначити серійний номер службового комп'ютера, назву та версію операційної системи, якою керується даний комп'ютер, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі Інтернет. Веб-сторінка має бути масштабована у браузері на повний розмір (100%). У браузері мають бути відключені усі додатки та надбудови, що можуть змінити вигляд веб-сторінки, яка оглядається. Крім того, у протоколі має бути перелічено та коротко описано фото-, відео та аудіофайли, прикріплені до публікації, із зазначенням посилання на кожний із таких файлів у мережі Інтернет. Значна кількість мультимедійних файлів на сучасних веб-сторінках є рекламними оголошеннями, які не стосуються публікації, що вивчається. Такі елементи веб-сторінки не потрібно описувати у протоколі огляду електронного документа.

Веб-сторінку, що оглядається, необхідно роздрукувати за допомогою службового принтера та додати до протоколу огляду як невід'ємний додаток, із зазначенням серійного номера, назви та моделі принтера. Фото-, відео- та аудіофайли, що є частиною публікації, мають бути збережені та записані на диск, який стане другим додатком до протоколу огляду. Альтернативним засобом фіксації веб-сторінки є збереження її у форматі *.html засобами програми-браузера, з подальшим записом такого файла на диск [122, с. 187-188].

Головним атрибутом електронного документа, розміщеного в мережі Інтернет, є його електронна адреса (домен). Окрім домену, в протоколі огляду необхідно вказувати адресу веб-сторінки, який завжди є індивідуальним, а тому використовується як один з способів ідентифікації необхідної веб-сторінки, на якому розміщені електронні матеріали, що мають значення для розгляду справи. В протоколі огляду веб-сторінки в мережі Інтернет обов'язково вказуються стандартні реквізити документа: назва, автор та час створення електронних

документів, якщо такі відомі, призначення документа, стислий зміст та інші викладені в ньому обставини, які мають значення для розслідування злочину.

Одним із способів фіксування електронних документів, розміщених в мережі Інтернет є вилучення серверів, на яких зберігаються електронні докази. Будь-яка інформація, яка передається за допомогою інформаційно-телекомунікаційних систем зберігається у log-файлах. Відповідно log-файли можуть бути вилучені в інтернет-провайдерів та інших суб'єктів, які беруть участь у процесі інформаційно-телекомунікаційної передачі даних та у фактичному володінні яких знаходяться сервери [255, с. 83].

На нашу думку, одним з найзручніших способів фіксації електронного документа, розміщеного в мережі Інтернет є забезпечення безперервної відеофіксації огляду. Відеозапис зображення екрану комп'ютера можна здійснити через відповідну програму, або така функція може бути уже передбачена у сучасних версіях операційних систем чи самих пристроїв. Даний відеозапис зафіксує точну дату, час проведення огляду, місцезнаходження електронного документа, його властивості та зміст, що в подальшому дає можливість ознайомитись з електронним документом повторно, у випадку його зміни, пошкодження, модифікації чи знищення.

Унікальним джерелом інформації у провадженні, що фіксується відповідним чином, є дані соціальних мереж. Однак, у цьому напрямку технічна сторона фіксації потребує вдосконалення [195, с. 135].

На переконання Є.П. Бєгалова, особлива увага повинна бути звернена на таке, порівняно нове джерело інформації про злочин, як соціальні Інтернет-мережі, за допомогою яких користувачі здійснюють спілкування між собою, користуються інформацією, яка їх цікавить, надають інформацію про себе, що може проявлятись у відображенні їх особистих інтересів, поглядів тощо. Соціальні «сторінки» в мережі Інтернет дозволяють громадянам отримувати і розміщувати на них інформацію різного змісту. Відповідно до інформації, що зберігається на відповідній Інтернет-сторінці, можна з'ясувати уподобання

користувача, дати його початкову психологічну і моральну характеристику (за умови, що він особисто здійснює керівництво сторінкою).

У зв'язку з цим сторінка користувача соціальної мережі, ймовірних пособників та організаторів, може бути одним із джерел важливої інформації про уподобання особи, що можуть формувати мотив злочину, передбаченого ст. 332 КК України, бути елементом «слідової картини» мотиву його вчинення. Отже, за допомогою інформації, що міститься на «сторінці» користувача «соціальної мережі», представляється можливим отримати доказову інформацію про мотив як уже вчиненого злочину, так і про злочини, які плануються [42, с. 84].

Таким чином, вважаємо за доцільне надати рекомендації щодо проведення огляду сторінок у соціальних мережах.

Особливості огляду сторінки у соціальних мережах залежить від ступеня доступу до облікового запису. Так, огляд облікового запису може проводитись:

1) без відома особи – власника облікового запису із загальнодоступного ресурсу;

2) з добровільним наданням доступу володільцем до персональної інформації облікового запису, листування тощо;

3) отримання доступу до персональної інформації облікового запису, листування на підставі рішення суду.

Слідчий, дізнавач може проводити огляд загальнодоступної персональної сторінки особи у соціальній мережі без її відома. Зазвичай такий огляд проводиться для збирання відомостей, які з дозволу власника сторінки є оприлюдненими. До таких відомостей можуть бути віднесені фото власника облікового запису, дата народження, місце проживання, місце роботи, публікації, коментарі до цих публікацій власника та інших осіб. Особисте листування власника облікового запису у такий спосіб огляду отримати неможливо. Огляд загальнодоступного облікового запису можна здійснювати: 1) без входу в обліковий запис соціальної мережі (якщо мережа надає можливість оглянути сторінку); 2) з особистої сторінки працівника; 3) з новоствореного облікового запису.

На думку О.В. Малахової отримання з мережі Інтернет фактичних даних, доступ до яких необмежений, не може здійснюватися шляхом провадження такої дії, як зняття інформації з електронних інформаційних систем, оскільки порядок виявлення та фіксації таких відомостей не пов'язаний з подоланням захисту інформації від втручання інших осіб, а тому не відповідає суті негласної слідчої (розшукової) дії. Даний різновид інформації має виявлятися та фіксуватися шляхом проведення такої слідчої (розшукової) дії, як огляд [142, с. 66].

Ми погоджуємось з думкою Н.М. Ахтирської, що коли потрібна інформація міститься у відкритому віртуальному просторі, який не має визначених меж, то достатньою є лише електронна форма факту. Це стосується й випадків розміщення в Інтернеті на офіційних сайтах державних органів іноземних держав фотографій, на яких зображуються високопосадовці, які вручають або одержують цінні подарунки. Це є підставою для подальшої перевірки, куди скеровується цей предмет – до установи, яку під час офіційного візиту представляє посадовець (як встановлено законом), чи привласнює його (що має ознаки корупційного правопорушення) [38, с. 124].

Наприклад, під час досудового розслідування кримінального провадження за фактом вчинення кримінального правопорушення, передбаченого ч. 1 ст. 258-3 КК, проводився огляд загальнодоступних відомостей: проведено порівняння ознак зовнішності обличчя особи чоловічої статі, яке зображено у кадрі із зображеннями на фотознімку копії паспорта на гр. Д та фотознімку у протоколі огляду аккаунта в соціальній мережі «Вконтакте» та виявлено їх схожість; додатку до акту огляду публічно доступного аккаунту «гр. Ч» у соціальній мережі «ВКонтакте» оптичного носія інформації файлів. Згідно якого вбачається, що гр. Ч сам робив публікації на своїй сторінці, яку відвідували інші особи, деякі з них робили позначки «мені подобається».

Під час дачі показів у суді, спеціаліст, який був залучений до огляду сторінки «ВКонтакте» пояснив, що під час розміщення на сторінках у соціальній мережі «ВКонтакте» інформації над вказаним розміщенням автоматично зазначається ім'я користувача сторінки (аккаунту). Також під розміщеною

інформацією автоматично зазначається дата та час її розміщення, що відповідає реальному часу. Свідок зазначив, що під час досудового розслідування йому надавались роздруківки файлів із збереженою інформацією зі сторінки в соціальній мережі «Вконтакте» користувача «гр. К.», ознайомившись з якими він вказав, що всі розміщення, зафіксовані у вказаних роздруківках здійснено користувачем мережі «Вконтакте» під ім'ям «гр. К.». Активність на сторінці була досить велика, були дописи, пости, репости. Зокрема на сторінці було зображення прапора України, опущеного в унітаз.

Також, під час дослідження сторінки гр. Т. у соціальній мережі «Вконтакте» стало відомо, що останній вказав місце роботи «Новороссия ТВ, Народный телеканал, Донецьк, Технічний директор», а обвинувачений перебуває у нього в друзях [60].

Такий огляд, слідчий, дізнавач чи прокурор може проводити як з особистої сторінки так і з новоствореного облікового запису. У протоколі огляду обов'язково слід зазначити з якої сторінки здійснювався огляд, її основні дані, послідовність проведених дій. В жодному разі непотрібно вказувати логін і пароль облікового запису з якого здійснювався вхід. Вважаємо що проведення відеозйомки екрану є найкращим способом фіксації такого електронного документа.

Отже, якщо відомості, які можуть мати доказове значення, перебувають у відкритому доступі, то вони можуть бути оглянуті без надання дозволу особи чи рішення суду.

Огляд особистої сторінки у соціальній мережі з добровільним наданням її власника доступу до персональної інформації та листування може бути проведений з метою підтвердження чи спростування наявної інформації. Такий огляд проводиться у разі, якщо володілець облікового запису добровільно надає логін та пароль облікового запису або мобільний телефон чи інший технічний пристрій з авторизованим обліковим записом. Наприклад, під час огляду листування у соціальній мережі можна перевірити факт висловлення образ,

погроз, шантажу; схиляння до вчинення чи приховування злочинів; встановити мотив і мету злочину; факт отримання чи пересилання коштів тощо.

Якщо отримати кримінально значиму інформацію неможливо загальнодоступним способом, а особа не надає дозволу на отримання такої інформації добровільно, слідчий, дізнавач повинен звернутись з відповідним клопотанням до слідчого судді.

Перегляд, копіювання та використання такої інформації є втручанням у право на повагу до приватного життя. Тому єдино можливим способом використання наявної на вилученому телефоні інформації є отримання з цією метою окремої ухвали суду, в якій буде чітко вказано, доступ до якої інформації надається. Відсутність такої ухвали автоматично тягне за собою порушення прав, гарантованих статтею 8 Конвенції про захист прав людини і основоположних свобод, а отже, згідно зі ст. 87 КПК, недопустимість як доказу вилученої з телефону інформації (документів)

Під час огляду електронних документів, розміщених у хмарних сервісах зберігання інформації необхідно зазначати інформацію щодо комп'ютерного обладнання, програм. Так, у протоколі мають бути зазначені адреса в мережі Інтернет та назва сервісу, до якого отримується доступ. Логін та пароль доступу до аккаунту не мають зазначатися у протоколі, з метою забезпечення захисту особистих даних журналіста. Крім того, таке обмеження допоможе запобігти несанкціонованому доступу до зазначених даних з боку сторонніх осіб, які на різних етапах кримінального провадження ознайомлюються зі змістом протоколу та відповідно можуть отримати доступ до аккаунту журналіста та змінити чи знищити інформацію, що зберігається у хмарному сервісі. Більшість сервісів хмарного зберігання інформації дозволяють отримати інформацію про каталог розміщення у сховищі, час та авторство створення документа, що там зберігається, а також хронологію його редагування. Зазначену інформацію має бути відображено в протоколі огляду, так само, як і постійне посилання в мережі Інтернет на документ, що оглядається, якщо на момент доступу слідчого до хмарного сервісу таке посилання було створене володільцем аккаунту. Текстові

документи, а також зображення, що оглядаються, доцільно роздрукувати за допомогою службового принтера та додати до протоколу огляду як невід'ємний додаток, із зазначенням серійного номера, назви та моделі принтера. Фото-, відео- та аудіофайли, аналогічно з оглядом публікацій у мережі Інтернет, мають бути збережені та записані на диск, який стане другим додатком до протоколу огляду [122, с. 189].

У випадку зберігання електронного документа у хмарному середовищі вилучення електронної інформації разом з її фізичним носієм неможливе. Тому в даному випадку здійснюється фіксація семантичного сегмента кіберпростору шляхом його огляду в порядку ст. 237 КПК [195, с. 129].

Сторона захисту також може збирати електронні документи та подавати їх відповідно до ст. 93 КПК.

Передбачені ж для захисту процесуальним та іншим законодавством правові положення (до певної міри процесуальні гарантії), котрі покликані зрівноважити можливості сторін щодо доказування, зрозуміло, не можуть нейтралізувати ширших можливостей сторони обвинувачення для формування доказової бази в змагальному процесі [134, с. 307]. Однак, можуть забезпечити більш швидке, повне і неупереджене досудове розслідування.

Основні способи збирання електронних документів стороною захисту полягають у:

– витребуванні від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок

– отриманні від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок;

– ініціюванні проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій,

– здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів.

Підозрюваний, обвинувачений мають закріплене право витребовувати та отримувати докази, однак ні порядок звернень, ні процедура, ні строки розгляду не регламентована КПК чи будь-якими іншими нормативно-правовими актами. Вважаємо, що в даному випадку підозрюваний, обвинувачений може подавати клопотання до органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб у якому слід зазначити номер кримінального провадження, кваліфікацію кримінального правопорушення, особисті дані, статус у кримінальному провадженні, запитувані документи, бажаний спосіб отримання (особисто, поштовим зв'язком), тощо.

Надавши стороні захисту право витребовувати докази, законодавець не передбачив у КПК жодних правових гарантій його реалізації, у зв'язку із цим керуватися під час реалізації свого права, захисник має положеннями Закону України «Про адвокатуру та адвокатську діяльність», яким адвокату надано право, зокрема:

– звертатися з адвокатськими запитами, в тому числі щодо отримання копій документів, до органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб, підприємств, установ, організацій, громадських об'єднань, а також до фізичних осіб (за згодою таких фізичних осіб);

– збирати відомості про факти, що можуть бути використані як докази, в установленому законом порядку запитувати, отримувати й вилучати речі, документи, їх копії [134, с. 299].

Відповідно до Закону України «Про адвокатуру та адвокатську діяльність», відповідь на адвокатський запит повинна бути надана не пізніше п'яти робочих днів з дня отримання запиту та може бути продовжено до двадцяти робочих днів з обґрунтуванням причин такого продовження. Несвоєчасне надання відповіді на адвокатський запит, відмова у наданні відповіді тягне за собою адміністративну відповідальність.

С.А. Крушинський зазначає, що відсутні підстави говорити про те, що, ініціюючи проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, сторона захисту збирає докази. У цьому випадку суб'єктом збирання доказів буде виступати слідчий, дізнавач, прокурор, який задовольнив клопотання сторони захисту і провів певну слідчу (розшукову) чи іншу процесуальну дію.

Разом з тим, навіть реалізація стороною захисту на практиці такого права, як ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, може стати проблематичним. Досить часто такі клопотання не задовольняються, і не тому, що вони є безпідставні або не вмотивовані, а тому, що проведення цих дій займе певний час, а слідчий чи дізнавач або обмежений строком досудового розслідування, або проведення цих дій не є вигідним для слідства. У тому ж випадку, коли підозрюваний чи його захисник витребовують та отримують від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб певні речі, копії документів, відомості, висновки експертів, висновки ревізій, акти перевірок, їх дійсно можна визнати самостійними суб'єктами збирання доказів. Такий висновок обґрунтовується тим, що сторона захисту в цьому випадку самостійно здійснює активні пошукові процесуальні дії, визначені кримінальним процесуальним законом [134, с. 299].

Окремі види документів (матеріали фотозйомки, відеозапису, звукозапису, електронні документи, висновки ревізій, акти перевірок тощо) можуть бути витребувані шляхом направлення адвокатського запиту або отримані від фізичних осіб, які їх подають захиснику з власної ініціативи. Інші ж (зокрема протоколи слідчих (розшукових) дій, у тому числі й негласних) можуть створюватися виключно стороною обвинувачення під час провадження досудового розслідування і для сторони захисту фактично недоступні [134, с. 302].

Отже, збирання електронних документів може здійснюватись стороною обвинувачення шляхом: надання його добровільно учасником кримінального

провадження (отримання); витребування доказів; проведення тимчасового доступу до електронного документа; проведення слідчих (розшукових) дій (огляд; обшук); проведення негласних слідчих (розшукових) дій. В свою чергу, сторона захисту збирає електронні документи шляхом витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб; отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб; ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій; здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів.

3.2. Дослідження електронних документів у кримінальному провадженні

В більшості випадків під час дослідження електронних документів у кримінальному провадженні слідчий, дізнавач, прокурор повинен залучати спеціаліста чи експерта. Це пов’язано відсутністю навичок роботи з окремими видами електронних документів та можливістю легкої зміни чи знищення важливої інформації, відсутністю сучасного технічного обладнання та ліцензійного програмного забезпечення для роботи з електронними документами.

Зазвичай, участь спеціаліста закінчується після виготовлення копії електронного документа. Слідчий чи дізнавач здійснює огляд електронного документа самостійно. Проте, якщо існують сумніви у достовірності електронного документа, пошкоджений технічний носій інформації, наявні інші неполадки роботи пристрою, складно віднайти відомості, які становлять інтерес (вони приховані або зашифровані) чи існують інші випадки коли є потреба у спеціальних знаннях слід призначати проведення експертизи електронних документів.

З урахуванням існуючих джерел доказів, та відсутності окремого виду досліджень електронних документів, вони можуть досліджуватись як документ, або як речовий доказ.

Призначення та проведення експертизи електронних документів здійснюється на підставі закону України «Про судову експертизу» та Інструкцією про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції №53/5 від 08.10.1998 року.

У даний час відсутній такий вид експертного дослідження, як експертиза електронних документів. Фактично у віртуальному середовищі ми досліджуємо не сам документ, а файл як носій даного документа. В іншій формі документ не може існувати в електронному (віртуальному) середовищі. Файл – поки що єдина форма існування електронного документа що дозволяє його створювати, зберігати, проводити пошук та ідентифікувати. Саме спільність об’єктів, а в окремих випадках і предмету дослідження, пояснює такий характер дослідження [91, с. 141].

Унаслідок вчинення злочинів у кіберпросторі утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди, що потребує проведення в таких справах широкого спектру судових експертиз, а саме:

– експертизи комп’ютерної техніки і програмних продуктів;

– експертизи телекомунікаційних систем (обладнання) та засобів;

– технічної експертизи документів;

– експертизи відеозвукозапису;

– експертизи у сфері інтелектуальної власності;

– інших видів експертиз, без проведення яких неможливо отримати необхідні відомості, що свідчать про ознаки складу одного зі злочинів злочинної сукупності (наприклад, економічних експертиз, психологічної, мистецтвознавчої експертизи або відповідної комплексної експертизи; трасологічних експертиз, лінгвістичної експертизи мовлення (семантикотекстуальний аналіз писемного й усного мовлення), судово-балістичних, судово-хімічних експертиз тощо [194, с. 298-299].

Під час дослідження електронних документів як документів може проводитись семантико-текстуальна експертиза. В.А. Динту зазначає, що вказану експертизу доцільно призначати для дослідження інформації, наявної у

відповідних групах соціальних мереж («Вконтакте», «Facebook» та ін.), повідомлень, в яких містяться заклики, наприклад, до участі у масових заворушеннях, терористичних актах, тощо [98, с. 75]. Крім того, така експертиза може проводитись для виявлення ознак погроз і шантажу, примушування до вчинення кримінальних правопорушень, тощо.

Також може проводитись лінгвістична експертиза усного мовлення, яка необхідна для ідентифікації особи, голос якої наявний на відео- чи фонограмі, встановлення мовних особливостей та визначення типу висловлювань.

Об’єктами такого дослідження можуть бути голосові повідомлення, записані та відправлені електронною поштою чи за допомогою соціальних мереж, відеозаписи, аудіозаписи, тощо. Якщо необхідно встановити чи належить голос на записі певній особі необхідно надати окрім досліджуваного запис зразок запису голосу особи.

Однією з видів експертиз, якою може досліджуватись електронний документ є фототехнічна експертиза. Об’єктом такого дослідження є цифрові фотографії – оригінали та копії, покадрові зображення відеозапису. Основними завдання експертизи є встановлення ознак монтажу, встановлення розмірів на зображеннях та їх порівняння, покращення якості зображення, встановлення пристрою, за допомогою якого було створено зображення та інших ідентифікаційних ознак тощо.

Також при дослідженні фото або відеозображень, що містяться у кіберпросторі може бути призначена портретна експертиза для ідентифікації особи (трупа) за фотознімком (фотокарткою, негативом) та відеозаписом [98, с. 75].

Експерти відео- та звукозапису здійснюється при необхідності встановлення технічних особливостей запису, встановлення технічного пристрою, за допомогою якого здійснювався запис, ознаки монтажу чи безперервності відео чи аудіозапису.

Документи як джерела доказів при розслідуванні фінансових шахрайств вивчають у різний спосіб: щодо визначення способу виготовлення документа

(шляхом призначення техніко-криміналістичної чи комп'ютерно-технічної експертизи), з метою ідентифікації особи – виконавця документа (шляхом призначення відповідної криміналістичної експертизи) [261, с. 260].

На стадії призначення експертизи слідчий, дізнавач може одержувати зразки (вільні, експериментальні) особисто, але краще – за участю спеціалістів, який знає технологію їх одержання, і вимоги, що до них ставляться: відповідність досліджуваним документам за часом, змістом, умовами виконання, мовою, призначенням, матеріалом, стилем, особливостями режиму роботи принтера, параметрами друку (масштаб, розрізняльна здатність). Кількість зразків має бути не меншою, ніж 10-15 аркушів [266, с. 10].

В зв'язку з тим, що електронні документи копіюються на змінні носії, друкуються на різних видах принтерів, має досліджуватися весь апаратно-програмний комплекс (комп'ютер, його програмне забезпечення, принтер) створення документа. При цьому експерт має знати основні технічні характеристики комп'ютерних засобів, принцип дії, основні механізми, їх властивості, ознаки виконання документа на принтері певного типу, виду, моделі [266, с. 14].

Комп'ютерно-технічна експертиза може призначатись для виявлення інформації, що міститься на комп'ютерних носіях, які вилучені у організаторів незаконного переправлення осіб через державний кордон, співучасників злочину, незаконних мігрантів. Так в організаторів незаконного переправлення осіб через державний кордон може вилучатися комп'ютерна техніка, мобільні телефони тощо. У безпосередніх виконавців відповідно мобільні телефони, GPS-навігатори, відеореєстратори тощо [42, с. 189-190]. Аналогічно це можуть бути технічні пристрої, які вилучені під час проведення досудового розслідування усіх інших видів кримінальних правопорушень: проти життя і здоров'я, проти власності, проти незаконного обігу наркотичних засобів та прекурсорів, тощо.

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

роботі використовує програмно-апаратний комплекс «Cellebrite UFED TOUCH 2 Ultimate» [49, с. 125-126], який може використовуватись в межах оперативно-розшукових справ та кримінальних проваджень, зокрема під час огляду мобільних пристроїв та/або SIM-карт. За результатом такого огляду формується електронний звіт, який підписується алгоритмом хешування, записується на носій електронної інформації та додається до протоколу у вигляді додатку.

Якщо раніше слідчі або оперативні працівники задовольнялися даними з телефонної книги, SMS, MMS, викликами, графічними і відеофайлами, то зараз фахівців просять «витягти» більшу кількість даних, зокрема: дані з програм обміну повідомленнями, дані з електронної пошти, історію відвідування ресурсів мережі Інтернет, дані про геолокацію, видалені файли й іншу видалену інформацію тощо. Усі ці відомості можна витягти такими спеціальним програмним забезпеченнями як «Мобільний криміналіст», «Magnet AXIOM», «Magnet Forensics» і «Belkasoft Evidence Center» [49, с. 127-129].

При експертному дослідженні телефонних пристроїв доцільним є дослідження історії листувань, роботи в мережі Інтернет, підключення до базових точок WI-FI тощо. Водночас при великій кількості об’єктів під час призначення експертизи рекомендовано ділити їх на групи, що дозволить прискорити виконання експертного дослідження [44, с. 107].

Найчастіше об’єкти експертизи – є засобами вчинення злочинів (підробка документів, ухилення від сплати податків, виготовлення фальшивих грошей, приховування слідів злочину тощо). Однак не менш поширеними є злочини, при скоєнні яких об’єктом посягання стає інформація, що знаходиться в комп’ютері, на якому-небудь носії, чи саме програмне забезпечення. Крім того магнітні носії комп’ютерів нерідко є місцем зберігання чи навіть приховування інформації, що становить інтерес для досудового розслідування злочину [260].

За допомогою судової комп’ютерно-технічної експертизи електронних документів можливе вирішення наступних завдань: відтворення та роздрук усієї або частини інформації, що міститься на фізичних носіях, в тому числі і в нетекстовій формі; відновлення інформації, що раніше містилась на фізичних

носіях і в подальшому була стерта або змінена з різних причин; встановлення часу введення, зміни, знищення чи копіювання тієї чи іншої інформації; розшифрування закодованої інформації, підбір паролів та відкриття системи захисту інформації; встановлення авторства, місця, засобів підготовки та способу виготовлення документів (файлів, програм). Аналогічні завдання розв'язуються в ході інформаційно-комп'ютерної експертизи.

Як бачимо, предмет дослідження електронних документів значно відрізняється від предмету дослідження аналогових документів. Але це не дивно, оскільки специфічним є і сам об'єкт дослідження. На відміну від аналогового електронний документ має особливий статус оригіналу, і в такому статусі одночасно може існувати одразу в кількох місцях [91, с. 135-135].

Співробітниками Дніпропетровського НДЕКЦ МВС України розроблено Інформаційний лист щодо особливостей призначення та проведення судових експертиз за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів».

У Інформаційному листі зазначено, що об'єктами комп'ютерно-технічного дослідження є будь-які комп'ютерні носії інформації, флеш-накопичувачі, лазерні диски сервери, системні блоки персональних комп'ютерів, портативні комп'ютери, планшетні комп'ютери, термінали мобільного зв'язку (комунікатори, мобільні телефони, smart-годиники, смартфони), відеореєстратори, тощо.

До таких об'єктів, застосовуються певні вимоги. Перш за все, на дослідження необхідно надати сам носій інформації та, у більшості випадків, весь апаратно-технічний комплекс, у складі якого знаходився носій інформації. Усі предмети дослідження обов'язково повинні бути окремо упаковані, з унеможливленням доступу до них, їх увімкнення чи підключення до мережі живлення або Інтернет-мережі. Якщо необхідно встановити відповідність програмних продуктів певним параметрам, то на дослідження надається носій із копією досліджуваного програмного продукту чи програмного коду та технічна документація до них (технічне завдання, інструкція встановлення, налаштування,

користувача, тощо). Усі об’єкти дослідження надаються разом з блоками живлення, а також, при можливості, з інформацією про паролі доступу (кодами доступу до панелі адміністрування), даними графічних ключів, цифрових PIN-кодів, або із зазначенням у постанові ініціатора (ухвалі суду) даних про їх відсутність у розпорядженні досудового слідства.

Перелік питань, який може бути поставлений перед експертом не є вичерпним. Перед призначенням судової експертизи слід обов’язково проконсультуватись з експертом (спеціалістом) з проведення комп’ютерно-технічних досліджень [115].

О.А. Самойленко проаналізувала вимоги до питань, що ставлять на вирішення експертам під час призначення комп’ютерно-технічних експертиз, які запропоновані ДНДКЦ МВС України. Так, під час формулювання питання слід використовувати лише термінологію, встановлену нормативно-правовими актами (ДСТУ, закони України, тощо) та уникати використанні жаргонів (комп, флешка, тощо). Питання не повинно стосуватись етапів дослідження інформації, носити правовий чи довідковий зміст, виходити за межі компетенції експерта (експертів) та інші [194, с. 301-303].

Окрім державних експертних криміналістичних центрів, дослідження електронних документів також займаються приватні фірми. Наприклад, при підтверджені даних в мережі інтернет, ТОВ «Експертно-правова консалтингова компанія «Юрекс» пропонує послуги з встановлення власників вебсайту, фіксації відомостей, які містяться на вебсайті, дослідження технічних пристроїв на наявність електронного листування, встановлення власника електронної скриньки [219]. Однак, послугами приватних фірм більшою мірою користуються у цивільних справах. Натомість у кримінальних провадженнях призначають експертизи у НДЕКЦ МВС України.

Для оптимізації процесу проведення комп’ютерно-технічної експертизи Б. В. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін розробили алгоритм підготовчих заходів для слідчого, дізнавача (прокурора):

– провести огляд об’єктів із залученням фахівців з метою встановлення наявності даних, що можуть мати доказове значення в кримінальному провадженні, і для вирішення питання про доцільність подальшого призначення експертизи;

– попередньо узгодити перелік питань за конкретними об’єктами із фахівцями й оптимізувати кількість питань;

– визначити першочерговість і пріоритети дослідження наданих для експертизи об’єктів;

– за об’єктивної потреби дослідження значного обсягу різноманітної комп’ютерної техніки (понад 10 одиниць) призначати експертизи з розмежуванням за групами об’єктів дослідження [217, с. 91-92].

Фахівці Дніпропетровського НДЕКЦ МВС пропонують схожий алгоритм підготовчих заходів при призначенні комп’ютерно-технічних експертиз:

- проводити попередній огляд об’єктів дослідження із залученням фахівців для встановлення та виокремлення лише тих об’єктів, які необхідні для дослідження та складення питань експертизи;

- якщо такий попередній огляд провести неможливо, то перелік питань та об’єктів що надаються на дослідження повинні бути узгоджені з фахівцями іншим способом (наприклад у телефонному режимі);

- визначати першочерговість та пріоритети дослідження наданих об’єктів;

- якщо експертизу великої кількості технічних пристроїв (більше 5-ти одиниць) слід провести у короткий термін, то доцільно призначати експертизи окремими постановами з розмежуванням за групами об’єктів дослідження;

- питання в постанові слідчого, дізнавача не повинні носити довідковий, правовий характер і виходити за межі компетенції експерта. Питання повинні бути спрямовані на встановлення конкретних обставин розслідуваної події [115].

На нашу думку, вказаний алгоритм доцільно уточнити та доповнити наступними заходами:

По-перше, первинна консультація з фахівцями експертної установи повинна бути проведена до вилучення технічних пристроїв, якщо такі фахівці не будуть залучатись під час їх вилучення. Ця консультація може проводитись в телефонному режимі, без розголошення відомостей досудового розслідування (точного місця проведення обшуку, персональних даних фігурантів справи, тощо). Це пов'язано з тим, що слідчі і дізнавачі все частіше зустрічаються з необхідністю вилучення та призначення експертизи електронних документів у всіх видах кримінальних правопорушень, а тому немає можливості залучати спеціалістів чи експертів щоразу, коли виникне така необхідність. Основна мета такої консультації це узгодження та уточнення процедури вилучення, упакування, транспортування об'єктів дослідження. Зазвичай, перед проведення обшуку слідчому, дізнавачу уже частково відомо, що може бути вилучено, тому під час консультування слід узгодити спірні питання.

По-друге, якщо у провадженні наявні докази, які мають значення для проведення експертизи, то про них слід зазначити в мотивувальній частині постанови та долучити їх копії у вигляді додатків. Сюди можуть бути віднесені протокол огляду чи обшуку, яким технічні пристрої були вилучені, протоколи допиту власників технічних пристроїв, висновки експертів, тощо.

На даний час окрім ДСТУ ISO/IEC 27037:2017. «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» жодних рекомендацій роботи з електронними документами немає. Цей стандарт є лише перекладом міжнародних вимог та за своїм змістом не пристосований до вимог криміналістики, безліч термінів, які у ньому вживаються є невідомі для працівників Національної поліції.

Тому, розроблення методичних рекомендацій по роботі з електронними документами, у якому б містились словник термінів, інфографіка, типові слідчі ситуації, типові питання для експертизи є досить актуальним. Проте, хочемо звернути увагу що такі рекомендації повинні бути розроблені не закладами вищої освіти зі специфічними умовами навчання, а саме фахівцями науково-дослідних

установ, експертами, спеціалістами, які зустрічаються з електронними документами щодня та мають достатній досвід, яким можна поділитись.

Різновидами комп'ютерно-технічної експертизи є апаратно-комп'ютерна та комп'ютерно-мережева експертиз.

Найчастіше під час проведення цих експертиз виникають проблеми які пов'язані з відсутністю методик і методичних рекомендацій з питань діагностики наданого на експертизу обладнання, дослідження об'єктів у межах комп'ютерно-мережевої експертизи, мобільних телефонів, планшетних комп'ютерів під керуванням операційних систем «Android OS», «iOS», а також навчальних тренінгів; відсутність належного (бажано уніфікованого) оснащення лабораторій відповідними сучасними апаратними пристроями; відстуність достатнього обсягу знань у експертів.

Таким чином, умови сьогодення потребують внесення певних корективв у класифікацію комп'ютерно-технічної експертизи, а отже, більш виправданою сьогодні є така класифікація:

– експертиза комп'ютерної техніки стосовно її функціонування, технічного стану, придатності до вирішення певних завдань;

– експертиза носіїв інформації та програмних продуктів, у тому числі дослідження комп'ютерних програм, виявлення слідової інформації, відновлення видаленої інформації тощо;

– комп'ютерно-мережева експертиза, встановлення факту втручання у роботу комп'ютерних систем, пошук слідової інформації за вчиненими з використанням різних засобів зв'язку злочинами, дослідження мережевих операційних систем і програм для комп'ютерних мереж;

– експертиза мобільних телефонів і комунікаторів;

– експертиза відеореєстраторів.

Крім того, потребує вдосконалення і програма підготовки фахівців у закладах вищої освіти зі специфічними умовами навчання з проведення комп'ютерно-технічних експертиз з метою підвищення кваліфікації експертів, досконалого вивчення ними методологічних матеріалів, набуття

високопрофесійних практичних навичок. Її зміст доцільно пов’язати із запропонованою класифікацією комп’ютерно технічної експертизи, з поетапним вивченням всіх п’яти напрямів. Це дозволить експертам, які спеціалізуються на будь-якому з напрямів комп’ютерно-технічної експертизи, поетапно набути знань за кожним напрямом. Насамперед це стосується поглиблених знань стосовно форматів зберігання даних на накопичувачах, характеристик окремих операційних систем, баз і банків даних, мов програмування тощо. Зрозуміло, що специфічні особливості судової комп’ютерно-технічної експертизи слід враховувати не лише під час перепідготовки та підвищення кваліфікації судових експертів, а й під час добору кандидатів на посади експертів [254, с.98-99].

Не зовсім розробленим є питання визначення об’єктів дослідження, особливо безпосередніх, при експертизі електронних документів. Якщо при дослідженні аналогового документа нас цікавить матеріальна складова, матеріал документа, матеріали письма тощо, то при досліджені електронного документа вивченню піддаються як носії інформації, так і файли, в яких містяться окремі документи. При цьому може бути проведена експертиза комп’ютерної техніки, експертиза програмних продуктів або інформаційно-комп’ютерна експертиза (дослідження). Оскільки експерт в галузі судово-технічної експертизи документів не володіє, в достатній мірі, спеціальними знаннями в галузі експертизи комп’ютерної техніки та програмних продуктів, він не може проводити даного виду дослідження, і навпаки. Тому на практиці досить часто проводиться комплекс експертиз, проведення яких доручається експертам різних спеціальностей [91, с. 139].

Нерідко для отримання максимально достовірної інформації комп’ютерна експертиза може проводитися в комплексі з іншими видами експертиз, наприклад криптографічною, відеофоноскопічною і т.д., що дозволяє незалежним експертам надати слідству об'єктивні ґрунтовні висновки у справі [125].

На теперішній час в правоохоронних органах існує серйозна проблема проведення експертних досліджень електронних доказів у розумні строки. Недостатня кількість експертів, які мають право проводити комп’ютерно-

технічні експертизи, сприяє утворенню кількамісячних, а у деяких випадках кількарічних черг на проведення означеного виду експертиз. З урахуванням наведеного вбачається доречним розширення практики дослідження відповідних електронних доказів безпосередньо слідчим, дізнавачем із залученням спеціаліста (за необхідності) з подальшим оформленням проведеного дослідження протоколом огляду. Така практика вже існує в регіонах, проте вона все ще не є поширеною, зважаючи на недостатні знання слідчих (у переважній більшості) в сфері ІТ [85, с. 108].

Отже, електронні документи можуть досліджуватись шляхом проведення семантико-текстуальної експертизи, лінгвістичної, фототехнічної, портретної, комп'ютерно-технічної та інших видів експертиз. Наразі залишається неврегульованим питання дослідження електронних документів на усіх стадіях кримінального провадження, оскільки відсутні чіткі правила такого дослідження, інструментарій, технічні засоби та кадри.

3.3. Міжнародний досвід використання електронних документів у доказуванні

Уряди країн усього світу визнають необхідність боротьби з кіберзлочинністю в глобальному масштабі. Багато країн прийняли кримінальне законодавство та створили спеціалізовані підрозділи з питань боротьби з кіберзлочинністю, сприяють розвитку цифрової криміналістики. Для ефективного подолання кіберзлочинності державні органи влади повинні добре розуміти масштаби, типи та вплив злочинності в кіберпросторі.

Безмежний характер Інтернету і стрімка еволюція технологій та методів, що використовуються злочинцями за допомогою комп'ютерних технологій ускладнюють для органів кримінального судочинства повне розуміння проблеми. Тому, завданням урядів є забезпечення того, щоб суспільство та окремі особи могли отримувати вигоду з інформаційних технології й таке середовище було безпечним.

Спочатку електронні документи розглядалися як невід'ємний елемент під час боротьби із кіберзлочинністю. Однак, зараз майже в більшості кримінальних правопорушень є зв'язок з електронними документами, які можуть бути корисними для розслідування. Як результат, дослідженню тепер підлягає питання щодо використання електронних документів у всіх видах кримінальних правопорушень.

Аналіз закордонних публікацій та нормативно-правових актів свідчить про те, що науковцями та практиками найчастіше використовується термін «electronic evidence» (в перекл з англ. «електронний доказ»), або «digital evidence» (в перекл. з англ. «цифровий доказ»). Поняття «електронний документ» практично не використовується.

Юридичного визначення електронних доказів в європейських країнах не існує. Загальною тенденцією серед правових рамок є застосування загальних принципів та правил щодо традиційних доказів (щодо збору, обміну та доказового значення).

У Конвенції Ради Європи про кіберзлочинність, є лише визначення «комп'ютерні дані», під яким розуміють 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 [126].

У посібнику «Electronic evidence guide as basic guide for police officers, prosecutors and judges» наведено визначення «електронного доказу, під яким розуміють будь-яку інформацію, яка створюється, зберігається або передається у цифровій формі, та може бути використана для доведення або спростування факту, який оспорюється в судовому процесі [8, с.12].

Комітет безпеки ЄС дає наступне визначення електронних доказів - це дані, що зберігаються в електронному вигляді (наприклад, IP-адреси, електронні листи, фотографії або імена користувачів), які мають значення для кримінального процесу. Часто ці дані зберігаються у постачальників послуг, а правоохоронні та судові органи повинні звернутися до них, щоб отримати їх [21, с. 1].

У національному законодавстві Австрії, Болгарії, Чеської республіки, Італії, Швеції та інших державах відсутнє офіційне визначення електронних доказів [16, с. 1; 12, с. 1; 13, с. 1; 18, с. 1; 19, с. 1].

Законодавство Португалії також не дає визначає «електронного доказу». Однак, вони використовують наукове визначення даного терміну наступного змісту: електронний доказ це будь-який тип інформації, що має доказове значення та зберігається на будь-якому цифровому пристрої або передається у двійковій або цифровій формі [1, с. 39; 17, с. 1].

Під електронними доказами у Німеччині розуміють, інформацію, яка зберігається або передається у цифровій формі та має значення кримінального розслідування [15, с. 1].

У Франції, електронні докази – це будь-яка доказова інформація, яка створюється, зберігається або передається у цифровій формі за допомогою електронних пристроїв та має значення для досудового розслідування кримінальних правопорушень. Електронні докази стосуються різних типів даних в електронній формі – включаючи електронні листи, текстові повідомлення, фотографії та відео Інтернет-мереж, а також інші категорії даних: дані про абонентів або інформацію про трафік онлайн-аккаунту [14, с. 1]. Електронні докази мають таку ж саму юридичну силу, як і паперові, вони підписуються й не потребують зв’язку з конкретним технологічним засобом [189].

Жодна з досліджуваних країн не передбачає юридичних кодексів для роботи з електронними доказами. Аналіз законодавчого змісту існуючих номративно-правових актів держав показує, що електронні докази зазвичай еквівалентні традиційним доказам у всіх досліджуваних країнах. Найбільше електронний доказ співвідноситься з документами у паперовій формі.

Німеччина, Бельгія, Іспанія, Фінляндія, Франція, Ірландія, Італія. Люксембург, Португалія та Румунія ототожнюють електронні документи з паперовими допоміжними документами та надають їм значення як документа у суді [21, с. 286].

Відсутність єдиного визначення «електронного доказу» не заважає державам-членам ЄС та Ради Європи спільно працювати над збором, збереженням та використанням електронних доказів. Відсутність визначення поняття «докази» у Європейській конвенції про взаємодопомогу у кримінальних справах, не стає перешкодою для взаємодопомоги між європейськими країнами. Хоча, теоретично наявність єдиного визначення електронних доказів може допомогти полегшити процес обміну електронними доказами, що є необхідним для співпраці між державами-членами.

Не існує єдиної міжнародної чи європейської правової бази, яка б регулювала електронні докази. Зазвичай, держави покладаються на національне законодавство, коли йдеться про збір, збереження, використання та обмін електронними доказами. Національні кримінальні закони були написані задовго до того, як існувало таке поняття, як Інтернет та технології, які могли б створювати електронні докази. Деякі країни адаптували своє законодавство до таких інновацій, а інші покладаються на традиційні кримінальні закони і застосовують їх також до електронних доказів. Отже, існують великі відмінності у національному законодавстві та підході, що ускладнює обробку транснаціональних електронних доказів. Згідно з дослідженням ООН щодо кіберзлочинності, правила доказів значно різняться навіть серед країн зі схожими юридичними традиціями [27, с. 192; 33].

Є лише декілька документів ЄС, які можуть мати пряме чи опосередковане значення для збору, збереження, використання та обміну електронними доказами. Рада Європи є передовою міжнародною організацією в цьому відношенні, оскільки всі держави-члени ЄС також є державами-учасницями Ради Європи, а Рада Європи підготувала кілька міжнародних договорів, що стосуються електронних доказів.

До основних документів Ради Європи, які є надзвичайно актуальними для використання електронних доказів є: по-перше, Європейська конвенція про захист прав людини та основних свобод (ЄСПЛ), особливо коли мова йде про захист права на приватне життя; по-друге, Конвенція Ради Європи про

взаємодопомогу у кримінальних справах та його Протоколу 1978 року. Ця Конвенція набрала чинності 12 червня 1962 року і налічує 50 держав-учасниць, що включає всі держави-члени ЄС. У ньому немає конкретних положень щодо електронних доказів, але це найширший захід взаємодопомоги з метою збору доказів, заслуховування свідків, експертів та притягнення до відповідальності осіб, тощо у транскордонних кримінальних справах. Конвенція встановлює правила виконання судових доручень органами держави-учасниці, які спрямовані на отримання доказів або передачу доказів у кримінальному провадженні, розпочатому судовими органами іншої держави-учасниці, та визначає вимоги до таких проваджень. Однак, беручи до уваги 1959 рік, коли він був прийнятий, Конвенція про взаємодопомогу у кримінальних справах не враховує сучасні технології, з якими ми стикаємось сьогодні, що робить це занадто повільним процесом для сучасного швидкого світу. Найголовнішим, третім відповідним документом Ради Європи в контексті електронних доказів є Конвенція Ради Європи про кіберзлочинність. Ця Конвенція залишається головним і єдиним міжнародним договором, який визначає основні елементи, що призводять до того, що деякі кібернетичні дії класифікуються як злочини, і має процедурні положення, що дозволяють запобігати, розкривати та переслідувати цю діяльність. Хоча електронні докази не обов’язково можуть бути результатом кіберзлочинності, це основна довідкова система в цій галузі, яка пропонує безліч положень для розширення розслідувань, коли йдеться про електронні докази.

Міжнародна конвенція про кіберзлочинність укладена 23 листопада 2001 року в м. Будапешті. Дана конвенція ратифікована Україною у 2005 році [126]. В цій конвенції сформульовано найбільш загальні та разом із тим визначальні принципи щодо забезпечення заходів боротьби із кіберзлочинами на національному та міжнародному рівнях. Відповідно до ст. 23 цієї конвенції, сторони співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства з метою розслідування

або переслідування кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень [202, с. 96].

Ю.Ю. Орлов зазначає, що Конвенція про кіберзлочинність стала важливим правовим документом, на базі якого держави, що приєдналися до неї, розбудовують власні системи протидії кіберзлочинам [155, с. 3]

Для координації зусиль у боротьбі з кіберзлочинами Комісією ЄС була розроблена узгоджена політика співпраці між державами-членами ЄС та відповідними установами, що знайшло своє відображення у зверненні Єврокомісії до Європарламенту «Стратегії кібербезпеки Євросоюзу: відкритий, безпечний і надійний кіберпростір», де пропонувалось розширити співпрацю як на рівні правоохоронних органів окремих країн, так і глобальну міжнародну співпрацю [5].

Прийняття «Директиви про атаки проти інформаційних систем» надало змогу покращити міжнародне співробітництво між судовими органами та поліцією держав-членів ЄС і зобов’язати збирати статистичну інформацію про кібератаки та централізовано направляти її у компетентні органи.

У січні 2013 року був створений і розпочав роботу Європейський центр з боротьби з кіберзлочинністю, який здійснює свою діяльність під егідою Європолу [274, с. 113-114].

Поштовх держав до запровадження законодавства про електронні докази або внесення змін до існуючого законодавства про докази зумовлений визнанням того, що традиційні норми загального права щодо доказів, що використовуються для забезпечення кримінального законодавства, є недостатніми та потребують модернізації. Природа електронних доказів, включаючи їх новизну та той факт, що вони є легкозмінювані, створює виклики для країн при оновленні їх законодавства. Електронні докази часто також мають транснаціональний характер, коли сервери знаходяться в декількох країнах, що посилює труднощі у використанні доказів та належному їх прийнятті до суду.

З метою дослідження електронних доказів, аналізу стану їх використання на національному та міжнародному рівні, запровадженню єдиної практики збору, оброки, передачі, зберігання електронних доказів комітетами Ради Європи та ЄС створюються міжнародні проекти. В межах таких проектів проводяться конференції, семінари з провідних питань сфери електронних доказів, публікуються посібники, рекомендації, розробляється єдина криміналістична методика, тощо.

Протягом березня 2014 року – жовтня 2016 року такі держави як Італія, Нідерланди, Німеччина, Франція, Мальта, Болгарія, Бельгія були учасниками проекту «Evidence» (у перекл. з англ. «Докази»), який присвячений застосуванню новітніх технологій у збиранні, використанні та передачі електронних доказів. В межах проекту було розроблено «Каталог інструментів, що використовуються для роботи з електронними доказами». У цьому каталозі перелічено понад 1500 програм та пристроїв для виконання різноманітних завдань, серед яких: отримання даних з комп'ютера, аналіз файлів хмарного сховища або дослідження повідомлень, прихованих у зображеннях чи інших файлах [9]. Вказаний каталог є у вільному доступі у мережі Інтернет англійською мовою [11].

Наступним проектом, який працював над створенням юридичних документів для обміну цифровими доказами в рамках процедур взаємної правової допомоги були проекти «EVIDENCE2» (в перекл. з англ. «Доказ 2») та «e-CODEX» (в перекл. з англ. «Електронний кодекс»). Зокрема, проект «e-CODEX» створив перевірену цифрову інфраструктуру, яка підтримує обмін даними між юридичними органами для багатьох транскордонних юридичних процедур у цивільному та кримінальному праві. В свою чергу, проект «EVIDENCE2» розробив огляд правової бази щодо використання та обміну електронними доказами; працював над загальними визначеннями поняття доказів; визначив технічний стандарт для обміну електронними доказами [24, 25].

Європейський комітет з питань правового співробітництва Ради Європи підготував Методичні рекомендації щодо електронних доказів у цивільному та

адміністративному судочинстві, які були прийняті 30.01.2019 року. Вони спрямовані на надання практичних вказівок щодо обробки електронних доказів у цивільних та адміністративних провадженнях для суду, інших компетентних органів, які мають судові функції; професіоналів, включаючи юристів; та сторін в процесі. Дані методичні рекомендації містять визначення електронних доказів, метаданих, порядок отримання усних доказів за допомогою засобів дистанційного зв'язку, використання електронних доказів, збору, вилучення і передачі доказів, значення, достовірності, зберігання і забезпечення їх збереження, архівування, підвищення рівня обізнаності, моніторингу відповідних технічних стандартів, а також підготовки та навчання. Це перший у світі міжнародний документ у цій галузі. Зараз Європейський комітет з питань правового співробітництва працює над підвищенням обізнаності про ці рекомендації та їх впровадження в державах-членах [10].

За співпраці таких проектів як CyberCrime@IPA (Спільний регіональний проект ЄС та Ради Європи щодо співпраці проти кіберзлочинності), Global Action on Cybercrime (GLACY) (Спільний проект ЄС та Ради Європи), Cybercrime@EAP (в рамках програмного співробітництва ЄС та Ради Європи в країнах Східного партнерства), Cybercrime@Octopus (глобальний проект ЄС та Ради Європи), CyberEast (спільний проект ЄС та Ради Європи, реалізований у регіоні Східного партнерства Радою Європи) у березні 2020 року опубліковано посібник «Electronic evidence guide as basic guide for police officers, prosecutors and judges» (у перекл з англ. «Електронні докази: базовий посібник для поліцейських, прокурорів та суддів») [8]. Посібник розроблений для країн, які перебувають у процесі розробки та встановлення власних правил та протоколів щодо роботи з електронними доказами [8, с. 8].

Перше видання даного посібника було опубліковане 18 березня 2013 року. З тих пір воно стало популярним джерелом права для виконавчих та судових органів різних країн. У деяких країнах посібник перекладено на свої вітчизняні мови [8, с. 8].

У посібнику розглянуто основні характеристики та властивості електронних доказів, принципи роботи з ними, джерела доказів, підготовка та порядок дій під час обшуку та вилучення електронних доказів, їх упакування, транспортування та зберігання; розглянуто типові ситуації при вилученні електронних доказів, у т.ч. з хмарного сховища та мережі Інтернет, розглянуто види досліджень таких доказів, подання доказів у суді. Посібник з ілюстраціями та схемами дозволяє легко зрозуміти інформацію та розрахований для користувачів різного рівня знань (від базового до більш фахового).

Автори звертають увагу на те, що посібник є шаблонним документом, який може бути адаптований країнами відповідно до їх національного законодавства. Основні принципи, які в ньому описані відповідають загальновизнаній належній практиці роботи з електронними доказами [8, с. 9].

У жовтні 2020 року під супроводом спільного проекту ЄС та Ради Європи під назвою «Global Action on Cybercrime Extended» (GLACY+) підготовлено посібник «Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence» (в перекл. з англ. «Посібник із статистики кримінального правосуддя щодо кіберзлочинності та електронних доказів») у якому ключовими є алгоритм збору та аналізу статистики, для забезпечення розуміння мінливого середовища та розробки стратегічних показників для вимірювання ефективності політики держав, оперативних реакцій щодо зменшення впливу кіберзлочинності [23, с. 3].

Окрім існуючих міжнародно-правових документів, існують також міжнародні керівні принципи та рекомендації, наприклад ті, що надаються ЄС та Радою Європи та які доповнюють правові інструменти і надають практичні вказівки щодо роботи з електронними доказами. З огляду на важливість електронних доказів, особливо у кримінальних провадженнях (при переслідуванні злочинів), дедалі більше уваги приділяється встановленню загальних стандартів для отримання, збору, зберігання та обміну електронними доказами.

Так, у 2012 році Асоціацією керівників поліції Англії, Уельсу та Північної Ірландії (Association of Chief Police Officers of England, Wales and Northern

Ireland (ACPO)) розроблено «Good Practice Guide for Digital Evidence. The Association of Chief Police Officers» (у перекл. з англ. «Посібник рекомендованих стандартів з цифрових доказів»).

Даний посібник призначений для використання його керівництвом правоохоронних органів Великобританії та інших осіб, які можуть мати справу з цифровими доказами. Автори зазначили, що поширення цифрових пристроїв та досягнення цифрових комунікацій призводять до того, що цифрові докази зараз є присутні або потенційно присутні майже у кожному злочині [22, с. 6].

У посібнику зазначено, що цифрові докази можуть перебувати у різних місцях, наприклад:

– на локальному пристрої кінцевого користувача – зазвичай це комп'ютер користувача, мобільний / смартфон, супутникова навігаційна система, флеш-накопичувач USB або цифрова камера;

– на віддаленому загальнодоступному ресурсі – наприклад, вебсайтах, що використовуються для соціальних мереж, дискусійні форуми та групи новин;

– на приватному віддаленому ресурсі – журналах діяльності постачальників послуг Інтернету, записи мобільних телефонів про оплату платежів, облікові записи веб-користувачів та все частіше – віддалене файлове зберігання (хмарне сховище);

– під час передачі – наприклад, текстові повідомлення мобільного телефону, голосові дзвінки, електронні листи чи Інтернет-чат.

Часто доказ може знаходитись у декількох місцях одразу. Однак отримати докази з одного місця може бути набагато простіше ніж з іншого. Наприклад, якщо потрібні докази контакту між двома номерами мобільних телефонів, то найкращий метод полягав би у отриманні даних про дзвінки від постачальників послуг зв'язку, а не призначати експертизу мобільних телефонів. Такі дані дзвінків, ймовірно, будуть більш повні, ніж журнали дзвінків з мобільного телефону, дата і час дзвінків будуть достовірними доказами, що не завжди можна сказати про журнали дзвінків з мобільного телефону [22, с. 7-8].

Автори рекомендують під час вилучення цифрових носіїв інформації та пристроїв кінцевих користувачів відноситись до них як до об’єктів експертизи. Звернено увагу на особливості вилучення цифрових носіїв інформації, залучення осіб, які мають відповідні знання (спеціалістів), проведення експертизи, аналізу і перевірки отриманих відомостей, вимоги до складення звіту експерта, участь експерта у судових засіданнях з приводу проведених експертиз, навчання поліцейських у проведенні цифрового розслідування, залучення приватних криміналістів, перелічено та описано нормативно-правові акти, якими врегульована діяльність правоохоронних органів Великобританії, розглянуто особливості збору нестійких даних, збору доказів, якщо злочини вчинені з використання вебсайтів, форумів, блогів, особливості збору цифрових доказів з комп’ютерів, ноутбуків, лептопів, мобільних пристроїв, поводження з доказами та їх транспортування та ін. Відповідно до вказаного посібника, на електронні докази поширюються ті самі правила і закони, які застосовуються до документів.

На даний час Асоціації не існує, оскільки вона була реорганізована у 2015 році у Раду керівників Національної поліції (The National Police Chiefs’ Council (NPCC). Однак, посібник досі використовується у криміналістиці.

Укладення міжнародних нормативно-правових актів, необхідність комплексного дослідження електронних документів у кримінальному провадженні, виявлення та вилучення цифрових слідів сприяло створенню нових організацій, які б займались розробкою відповідних програмних продуктів, методів досліджень.

Зокрема, у 2001 році у Великобританії засновано компанію «Digital Detective» (у перекл. з англ. «цифровий детектив»), яка розробляє криміналістичне програмне забезпечення для вилучення та аналізу цифрових даних з різних цифрових пристроїв.

У 2002 році «Digital Detective» випустила свій флагманський продукт «NetAnalysis» – програмний додаток, розроблений спеціально для вилучення та аналізу даних Інтернет-слідів. Програмне забезпечення довіряє і

використовується провідними правоохоронними органами, комерційними компаніями та державними структурами у всьому світі.

Їх мета – розробка нових інноваційних технологій, що пропонують суттєві вдосконалення до існуючих програм та методів досліджень. Вони зосереджують свої зусилля на сферах, де наука відкриває нові можливості, які, швидше за все, призведуть до значного судово-медичного прогресу. Вони хочуть бути першовідкривачами в галузі цифрової криміналістики та прагнуть розробляти провідні продукти, які сприятимуть тому, щоб світ ставав безпечнішим завдяки цифровій криміналістичній експертизі.

Клієнтами «Digital Detective» є урядові та неурядові організації різних держав, зокрема: Британська транспортна поліція, Слідчий комітет Російської Федерації, Міністерство оборони Сполучених штатів Америки, Національна жандармерія Франції, Королівська канадська кінна поліція, японський виробник електроніки та IT-компанія «FUJITSY», американська технологічна компанія «Hewlett-Packard», корпорація «Microsoft», міжнародна мережа кафе швидкого обслуговування американської фірми «Starbucks Corporation», британська міжнародна телекомунікаційна компанія «Vodafone Group plc.» [7].

Одним з посібників, які використовує «Digital Detective» у своїй діяльності є «Good Practice Guide for Digital Evidence»[30, с. 213].

Цифрова криміналістика розвивається швидшими кроками у порівнянні з кримінальним процесуальним закріпленням міжнародних норм. Зокрема, у 2012 році прийнято «Forensics Standards (ISO/IEC 27037 ISO/IEC 27037:2012) information technology. Guidelines for identification, collection, acquisition and preservation of digital evidence» (у перекл. з англ. «Стандарти криміналістики (ISO / IEC 27037 ISO / IEC 27037: 2012) Інформаційні технології. Рекомендації щодо ідентифікації, збору, збору та збереження цифрових доказів» [20]. У міжнародному стандарті надано вказівки щодо таких пристроїв та/або функцій:

– цифрові носії інформації, що використовуються у звичайних комп’ютерах, таких як жорсткі диски, дискети, оптичні та магнітооптичні диски, пристрої передачі даних із подібними функціями;

– мобільні телефони, персональні цифрові помічники, персональні електронні пристрої, карти пам'яті;

– мобільні навігаційні системи;

– цифрові фотокамери та відеокамери (включаючи відеоспостереження);

– стандартний комп’ютер з мережевими підключеннями;

– мережі, засновані на TCP / IP та інших цифрових протоколах;

– пристрої з подібними функціями, як зазначено вище.

Наведений вище список пристроїв є орієнтовним та не вичерпним.

Цей міжнародний стандарт надає керівництву особам щодо поширених ситуацій, що виникають у процесі обробки цифрових доказів, та допомагає організаціям у сприянні обміну потенційними цифровими доказами між юрисдикціями.

Стрімке використання електронних доказів під час міжнародного співробітництва, розробка практиками рекомендацій роботи з електронними доказами не залишила осторонь науковців, які також досліджували електронні докази. У 2017 році науковцями Стівеном Мейсоном та Даніелем Сенгом у співавторстві з іншими науковцями у Лондоні було опубліковано четверте видання книги «Electronic Evidence» (у перекл. з англ «електронний доказ»). У даному посібнику розкрито основні характеристики електронних доказів та пристроїв на яких вони можуть міститись, способи збирання і зберігання електронних доказів, проведення експертних досліджень. Під час дослідження використано нормативно-правову базу та судові прецеденти Англії та Уельсу [26].

Науковці Гронінгенського університету (Нідерлади) зазначають, що існують різні визначення електронних доказів, і в деяких випадках цей термін використовується як взаємозамінний із терміном «цифрові докази». Однак, вони використовують термін «електронні докази», який визначається як будь-яка інформація, яка може мати доказове значення, яка створюється, зберігається або передається будь-яким електронним пристроєм. Вчені застосовують широкий

підхід до електронних доказів, включаючи: фізичні або традиційні (не електронні) докази, такі як зброя вбивства або плями крові, які можуть бути оцифровані, наприклад, шляхом цифрового фотографування зброї вбивства; докази, створені в аналоговому форматі (відеокасета чи вініл), які можуть бути оцифровані та введені в процес оцифрування з набуттям цифрового статусу; і докази, одразу створені цифровим пристроєм (комп'ютером або подібним до нього пристроєм). Усі ці типи доказів розглядаються як «електронні докази», незалежно від їх походження [27, с. 190].

Електронні докази можуть містити таємницю листування, телефонних переговорів, телеграфної та іншої кореспонденції що є особистісним, немайновим правом, що традиційно належить до основних природних прав людини. Згідно ст. 8 Конвенції про захист прав людини і основоположних свобод, кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб. Електронні документи також використовуються у рішеннях ЄСПЛ. Зокрема, у справах справах «P. and S. v. Poland» (від 30.10.2012 року), «Eon v. France» (від 14.03.2013 року), «Shuman v. Poland» (від 03.06.2014 року) [106].

Порушення процедури збирання електронних доказів, які містять таємницю приватного і сімейного життя часто є предметом спору, які вирішуються ЄСПЛ. Наприклад, У справі «М. Н. та інші проти Сан-Марино» (M.N. and Others v. San Marino), заява № 28005/12, пункт 71, від 07 липня 2015 року) суд відмітив, що вилучення даних у сенсі копіювання банківських даних (отриманих з банківських виписок, чеків, фідуціарних розпоряджень та повідомлень електронної пошти), які суд вважає, підпадають під поняття

«приватне життя» та «листування» та подальше зберігання з боку органів таких даних становлять втручання для цілей статті 8 Конвенції [§ 51]».

У справі «Copland проти Сполученого Королівства», заява № 62617/00, рішення від 3 квітня 2007 р., ЄСПЛ зазначив, що відправлені з роботи електронні листи також повинні захищатися на підставі ст.8 Конвенції про захист прав людини і основоположних свобод, як і інформація, отримана з відстеження приватного використання мережі Інтернет. Заявниця у цій справі не була попереджена про те, що її дзвінки можуть бути піддані відстеженню, тому вона обґрунтовано сподівалася на приватність дзвінків, зроблених з її робочого телефону (див. § 45 рішення Суду у справі Halford). Таке ж очікування мала заявниця і щодо електронної пошти та використання мережі Інтернет [206]. ЄСПЛ визнав порушення ст. 8 Конвенції про захист прав людини і основоположних свобод, щодо моніторингу інформації про телефонні дзвінки, використання електронної пошти чи інтернету працівницею за відсутності відповідного закону для такого втручання, хоча не виключив ситуації, що такий моніторинг може в деяких випадках бути визнано «необхідним в демократичному суспільстві» і з законною метою, проте, з огляду на відсутність законності втручання, ЄСПЛ не розглядав питання необхідності в цій справі [253, с. 156].

Аналіз вищевказаних публікацій, рекомендацій та посібників свідчить про те, що на міжнародному рівні невизначено єдиного поняття «електронного доказу», однак встановлено базові основи роботи з таким видом доказу. Залучення держав до міжнародних проектів щодо поширення єдиної практики роботи з електронним доказами у цивільних, адміністративних, кримінальних справах та у боротьбі з кіберзлочинністю позитивно впливає на гармонізацію законодавства держав-членів та поступову розробку власних досліджень.

Висновки до третього розділу

1. Збирання електронного документа, у зв’язку з його електронною формою здійснюється у два етапи: спочатку необхідно отримати матеріальний носій

інформації, або доступ до нього, після цього проводиться огляд інформації, яка на ньому міститься.

2. Сторона обвинувачення отримує електронні документи під час їх добровільної видачі учасниками кримінального провадження, шляхом витребування, проведення тимчасового доступу до речей та документів (як заходу забезпечення), слідчих та негласних слідчих (розшукових) дій.

3. Добровільна видача електронного документа стороні обвинувачення здійснюється на підставі написання відповідної заяви чи клопотання, у додатках до якої повинен бути доданий матеріальний носій інформації. Наголошено на тому, що витребування електронного документа повинно здійснюватися у вигляді вимоги про витребування речей та документів.

4. Під час проведення огляду місця події, місцевості, приміщення можна отримати електронний документ. Правила проведення такого огляду в загальному відповідають правилам огляду під час збирання інших джерел доказів, однак, з урахуванням особливостей електронного документа має свої відмінності.

6. Обшук проводиться за загальними правилами проведення обшуку, з урахуванням вимог щодо огляду як слідчої (розшукової) дії під час збирання електронних документів. Під час звернення до суду на отримання санкції на обшук варто одразу клопотати суд на надання дозволу на копіювання та вилучення інформації, яка міститься у комп’ютерах, мобільних терміналах, тощо.

7. Сторона захисту здійснює збирання шляхом витребування та отримання електронних документів, ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та здійснення інших дій, які не заборонені законом. Зазвичай, ці права реалізовуються шляхом написання клопотань на адресу підприємств, установ, організацій, слідчому та через надсилання адвокатських запитів захисником.

8. Електронний документ може бути досліджений під час проведення експертизи експертом чи комісією експертів. До основних експертиз, які можуть бути призначені для дослідження електронного документа належать техніко-

криміналістична, комп’ютерно-технічна, семантико-текстуальна, лінгвістична, фототехнічна та ін.

9. Аналіз міжнародного досвіду використання електронного документа підтверджує, що запровадження єдиної практики збирання і дослідження електронних документів може відбуватись навіть без встановлення законодавчого визначення терміну. Дослідження електронного документа відбувається як практиками, так і науковцями у кримінальній процесуальній та криміналістичній сферах.

ВИСНОВКИ

Проведене дослідження кримінальних процесуальних та криміналістичних основ використання електронних документів у доказуванні дозволило сформулювати ряд висновків, що носять як науково-теоретичний, так і прикладний характер, зокрема:

1. Аналіз стану наукового розроблення свідчить, що комплексних досліджень електронного документа у доказуванні, з урахуванням чинного законодавства не проводилось. Неоднакове розуміння сутності електронних документів, відсутність єдиних уявлень щодо особливостей їх формування на практиці спричиняють труднощі під час збирання, перевірки та оцінки доказів, які містяться у таких джерелах у кримінальному провадженні.

2. Встановлено, що зазвичай електронний документ розглядався як різновид документа або речового доказу, як джерел доказів, в залежності від того, що може використовуватись як доказ факту чи обставин, які підлягають доказуванню у кримінального провадження: відомості чи матеріальний об’єкт. Однак, двоєдина сутність електронного документа – інформаційна та технічна складова, потреба у наявності спеціальних технічних засобів та програм для розкодування та візуалізації інформації, її копіювання та дослідження, вільне переміщення між носіями інформації, «чутливість» інформації та легка зміна даних є суттєвими відмінностями з «традиційними» доказами, а тому спричиняє необхідність виокремлення «електронних документів» як окремого джерела доказів. Запропоновано авторське визначення «електронних документів» під яким розуміємо відомості в електронній формі, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження

3. Запропоновано класифікувати електронні документи з таких підстав: за стадіями виготовлення; за комбінацією метаданих; в залежності від доступу до метаданих електронного документа; за ступенем захисту; за джерелом походження; за їх місцем розташування; за формою.

4. Належність електронного документа є його властивістю, яка полягає у можливості встановлювати чи спростовувати обставини та факти, які підлягають доказуванню. Електронні документи можуть встановлювати подію кримінального правопорушення, винуватість особи, форму вини та мотив правопорушника, вартість завданої шкоди, або мати допоміжне значення для складання версій, їх перевірки, встановлення можливих місць вчинення злочину та можливих учасників, тощо.

Для визнання електронних документів допустимими слід здійснити перевірку сукупності таких умов, як: належний суб'єкт, належний спосіб, належне джерело, належна форма фіксації. Сторона обвинувачення здійснює збирання електронних документів лише у законодавчо закріплений спосіб, натомість законодавець допускає можливість порушення способу чи форми закріплення електронних документів стороною захисту, потерпілим чи його представником, які не завжди впливають на їх допустимість. Для визнання допустимими електронних документів, доступ до технічного носія яких неможливо отримати (віддалений сервер) слід внести відповідні зміни до КПК.

Достовірність електронних документів полягає у відображенні у них фактів об'єктивної дійсності, які мають значення для кримінального провадження. Встановлення достовірності електронних документів є завжди суб'єктивною оцінкою особи, яка її здійснює, що проводиться шляхом їх співставлення з іншими доказами у кримінальному провадженні, котрі стосуються одного і того ж факту, який доказується.

Встановлення достатності сукупності доказів, у тому числі електронних документів, здійснюється особою, на основі раніше зібраних належних, допустимих і достовірних доказів з метою прийняття відповідного рішення.

5. Збирання електронних документів, умовно можна поділити на два етапи: отримання доступу чи вилучення фізичного носія інформації та дослідження і аналіз його змісту. Це пов'язано з тим, що способи отримання фізичного носія інформації регламентовані у КПК щодо «традиційних доказів», натомість візуалізація та відображення електронного документа у формі, яка

може бути сприйнята людиною потребує використання технічних пристроїв, спеціального програмного забезпечення та залученням спеціаліста. Відтак, ми можемо отримати електронний документ у формі оригіналу чи копії.

До способів збирання електронних документів стороною обвинувачення відносимо: отримання його від особи, яка надає добровільно; витребування та отримання речей, документів тощо; проведення слідчих (розшукових) дій (огляд, обшук); проведення негласних слідчих (розшукових) дій. На окрему увагу заслуговує тимчасовий доступ до речей та документів, як захід для забезпечення дієвості кримінального провадження з метою встановлення (пошуку) фактичних даних, які надалі через проведення слідчих (розшукових) дій (наприклад, огляд) будуть оформлені як доказ.

Вважаємо, що добровільна видача повинна здійснюватись разом із поданням клопотання про долучення доказів, а форма, зміст, строк розгляду вимоги про витребування документів та речових доказів слід закріпити у КПК.

Проведення тимчасового доступу до електронних документів є заходом забезпечення кримінального провадження, який проводиться у випадках, коли відомі точні відомості про електронний документ, або такі відомості містять охоронювану законом таємницю.

Під час огляду місця події чи обшуку слід використовувати технічний інструментарій та залучати спеціаліста для правильного вилучення електронних доказів, недопущення будь-яких змін чи знищення інформації, яка міститься на фізичних носіях. Важливо упаковувати та транспортувати технічні пристрої у тому стані живлення, у якому вони знаходились на момент огляду та використовувати при цьому заводське пакування чи коробки Фарадея.

Для отримання доступу до приватної інформації, яка міститься на технічному пристрої, необхідно зазначати про таку необхідність під час підготовки клопотання про проведення обшуку.

Проведення огляду електронних документів та дослідження їх змісту здійснюється в залежності від їх носіїв: фізичні носії, які можна вилучити; публікації в мережі Інтернет (облікових записів) та на віддалених Інтернет-

серверах. Зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем є основними негласними слідчими (розшуковими) діями, за допомогою яких здійснюється збирання електронних документів.

Встановлено, що сторона захисту може збирати електронні документи шляхом їх витребування та отримання; ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій; здійснення інших дій, які не заборонені законом. Витребування електронних документів підозрюваним, обвинуваченим, потерпілим та їх представниками не регламентований у КПК, тому, зазвичай під витребуванням науковці розглядають збирання доказів захисником шляхом надсилання адвокатського запиту.

Дослідження електронних документів здійснюється відповідно до експертиз, які розроблені для дослідження документів та речових доказів. Зазвичай, електронні документи досліджуються під час проведення таких експертиз: семантико-текстуальна, лінгвістична, фототехнічна, портретна, комп'ютерно-технічна та інших експертиз (у т.ч. комплексних). На якість проведення експертизи впливають спосіб вилучення, пакування та зберігання об'єктів (технічних носіїв інформації), які надані на дослідження. Відсутність єдиних правил дослідження, необхідних технічних засобів та інструментарію спричиняє труднощі під час призначення та проведення експертиз.

6. Вивчення міжнародного досвіду можливостей використання «електронних документів» у кримінальному провадженні як доказів, дає можливість нам констатувати, що національне законодавство та практика його застосування потребує приведення їх у відповідність до сучасних вимог розвитку науки та техніки. Такі заходи нададуть ширші можливості правоохоронним органам під час розслідування кримінальних правопорушень, зокрема, кіберзлочинів, щодо збирання електронних документів, участі в ефективному співробітництві між поліцією та підрозділами з питань кіберзлочинності в Європі та інших регіонах.

7. Пропонуємо доповнити ч. 2 ст.84 КПК «Докази» та викласти її у такій редакції: Процесуальними джерелами доказів є показання, речові докази, документи, електронні документи, висновки експертів.

Доповнити КПК ст. 99-1 під назвою «Електронні документи» у такій редакції:

1. Електронним документом є відомості в електронній формі які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

2. До електронних документів можуть належати: текстові документи, фотографії та інші зображення, аудіо- та відео- записи, електронні повідомлення (смс-повідомлення, електронна пошта, голосові повідомлення), кеш-файли, cookie-файли, вебсайти, дані геолокації та інші відомості у електронній формі.

3. Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал електронного документа на фізичному носії інформації. Оригіналом електронного документа є його відображення, яке зберігається на первинному фізичному носії інформації. Якщо один і той самий електронний документ зберігається на кількох носіях інформації, то оригіналом є електронний документ, дата створення або дата копіювання якого є більш ранньою.

4 Копія електронного документа, виготовлена слідчим, дізнавачем, прокурором за участі спеціаліста визнається судом як оригінал електронного документа.

5. Електронний документ визнається допустимим доказом, якщо отримати зміст його відображення можливо без доступу до фізичного носія інформації, або такі відомості перебувають у вільному доступі (вебсайти). Для підтвердження змісту електронного документа можуть бути визнані допустимими й інші відомості, якщо: 1) оригінал електронного документа втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає; 2) оригінал електронного документа не може бути отриманий за допомогою доступних правових процедур; 3) оригінал електронного документа

знаходиться у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.

6. Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції, узагальнення електронного документа, які незручно повністю досліджувати в суді разом з електронним документом у повному обсязі.

Доповнити абзац 2 ч. 3 ст. 93 КПК, та викласти його у такій редакції:

Ініціювання стороною захисту, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, проведення слідчих (розшукових) дій та *подання доказів* здійснюється шляхом подання слідчому, прокурору відповідних клопотань, які розглядаються в порядку, передбаченому статтею 220 КПК. Постанова слідчого, прокурора про відмову в задоволенні клопотання про проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій може бути оскаржена слідчому судді.

Доповнити ст.110-1 КПК «Вимога про витребування документів та речових доказів» та викласти її у такій редакції:

1. Слідчий, дізнавач, прокурор звертається з вимогою про витребування документів та речових доказів до органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб з метою збирання доказів.

2. Вимога про витребування документів та речових доказів виготовляється на офіційному бланку та підписується службовою особою, яка прийняла відповідне процесуальне рішення.

3. Вимога про витребування документів та речових доказів повинна бути складена відповідно до ч.2 ст.160 КПК.

4. До вимоги про витребування документів та речових доказів додається витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, в рамках якого подається клопотання.

5. У вимозі повинно бути зазначено строк на її виконання, який не може бути меншим 10 днів.

6. У випадку відмови в наданні документів та речових доказів, несвоєчасного або неповного надання документів та речових доказів, надання документів та речових доказів, які не відповідають дійсності на вимогу про витребування документів та речових доказів, слідчий, дізнавач, прокурор має право звернутись до суду з клопотанням про тимчасовий доступ до речей і документів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Benjamim Silva Rodrigues, Direito Penal. Informático-Digital. Coimbra: Coimbra Editora, 2009. 722 p.

2. Casey E. Digital evidence and computer crime: forensic science, computers and the internet (3rd edition). 2011. 770 p.

3. Chris Currier. Safeguard your digital evidence with Faraday bags. URL: https://www.msab.com/2020/10/23/safeguard-your-digital-evidence-with-faraday-bags/ (дата звернення: 26.10.2020)

4. Computer Crime: A Crime fighter's Handbook. D.Icove, K.Seger, W.Von Sorsh. O'Reylli &Associates, Ins. 1995. 437p.

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint communication to the European parliament, the Council, the European economic and social committee and the Committee of the regions. 2013. Brussels. URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en (дата звернення: 15.11.2020).

6. Datareportal. Digital 2021: Global overview report. URL: https://datareportal.com/reports/digital-2021-global-overview-report (дата звернення 11.01.2021).

7. Digital detective. URL: https://www.digital-detective.net/ (дата звернення 09.12.2020).

8. Electronic evidence guide as basic guide for police officers, prosecutors and judges. Version 2.1. Cybercrime division. Directorate General of Human Rights and Rule of Law. Strasbourg. 2020. 200 p.

9. Electronic evidence, expertly explored. An official website of the European Union. URL: https://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/headlines/news/article_17_03_16 (дата звернення: 15.11.2020).

10. European Committee on Legal Co-operation. Digital evidence. URL: https://www.coe.int/en/web/cdcj/-/electronic-evidence (дата звернення: 15.11.2020).

11. European Informatics Data Exchange Framework for Courts and Evidence. EVIDENCE Project. URL: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d4-1-413 (дата звернення: 15.11.2020).

12. Fiches Belges on electronic evidence. Austria. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/AT-electronic-evidence-fb (дата звернення: 29.08.2020).

13. Fiches Belges on electronic evidence. Bulgaria. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/BG%20Fiches%20Belges%20on%20electronic%20evidence (дата звернення: 29.08.2020).

14. Fiches Belges on electronic evidence. France. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/France_Fiches%20Belges-on-electronic-evidence (дата звернення: 29.08.2020).

15. Fiches Belges on electronic evidence. Germany. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FB-EEGermany (дата звернення: 29.08.2020).

16. Fiches Belges on electronic evidence. Italy. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FB_Italy (дата звернення: 29.08.2020).

17. Fiches Belges on electronic evidence. Portugal. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/New%20Fiches%20Belges%20on%20electronic%20evidence%20-%20Portugal (дата звернення: 29.08.2020).

18. Fiches Belges on electronic evidence. Sweden. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FB_SV (дата звернення: 30.08.2020).

19. Fiches Belges on electronic evidence. Czech republic. European Judicial network. URL: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FB_CZ (дата звернення: 29.08.2020).

20. Forensics Standards (ISO/IEC 27037 ISO/IEC 27037:2012. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012. 38 p.

21. Fredesvinda Insa. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*. 2007. 1:4. P. 285-289.

22. Good Practice Guide for Digital Evidence. The Association of Chief Police Officers. 2012. URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5 (дата звернення: 30.11.2020)

23. Guide for criminal justice statistics on cybercrime and electronic evidence. Global Action on Cybercrime Extended (GLACY+). Joint project of the European Union and the Council of Europe. 2020. 23p.

24. Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. URL: https://www.interpol.int/es/Quienes-somos/Marco-juridico/Information-communications-and-technology-ICT-law-projects/EVIDENCE2e-CODEX (дата звернення: 16.11.2020).

25. Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. URL: https://evidence2e-codex.eu/ (дата звернення: 17.11.2020).

26. Mason Stephen, Daniel Seng, editors. Electronic Evidence. University of London Press, 2017. URL: www.jstor.org/stable/j.ctv512x65 (дата звернення: 15.11.2020).

27. Mifsud Bonnici J. P., Tudorica M., Cannataci J. A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. *Law, Governance and Technology Series.* 2018. Vol. 39. URL: https://doi.org/10.1007/978-3-319-74872-6_11 (дата звернення: 28.11.2020).

28. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standardsand Technology. National Institute of Standards and Technology. 2011. 7 p.

29. Ratnova A. Legal admissibility of electronic documents as evidence in

Ukraine. *Право. Комунікація. Суспільство. Law. Communication. Society. Das recht. Die kommunikation. Das geselschaft. Le droit. La communication. La société*: матеріали науково-практичної конференції здобувачів вищої освіти (українською та іноземними мовами) / за заг. ред. канд. філол. наук, доц. І. Ю. Сковронської. Львів: ЛьвДУВС. 2019. С. 117-119.

30. Ratnova A. The state of scientific development of an electronic document as evidence in criminal proceedings. *Visegrad Journal on Human Rights*. 2020. № 5. P. 210-214.

31. Research & Branding Group. Соцмережі як джерело інформації. URL: http://rb.com.ua/uk/blog-uk/omnibus-uk/socmerezhi-jak-dzherelo-informacii/ (дата звернення 11.01.2021).

32. Security Union. Facilitating access to electronic evidence. European Commission Explanation. April 2018. 3 p.

33. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime. New York. 2013. 158 p.

34. Алєксєєва-Процюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*: Збірник наукових праць. К.: Науково-дослідний інститут публічного права. 2018. Випуск 2. С. 247-253.

35. Аналіз судової практики місцевих судів м. Харкова і Харківської області, Апеляційного суду Харківської області та Харківського апеляційного суду щодо використання електронних доказів (доказів вчинення злочину, які можна отримати в електронній формі) по справам, які перебували на розгляді у 2018 та 2019 роках/ вик. Грошева О.Ю., Луніна О.В. URL: https://hra.court.gov.ua/sud4818/inshe/inf_court/uzag20k1 (дата звернення 05.09.2020).

36. Аналіз судової практики щодо використання електронних доказів у кримінальних провадженнях Чаплинського районного суду Херсонської області. Вик. І. О. Пилипенко. URL: https://cp.ks.court.gov.ua/sud2122/analiz/analizeldok/ (дата звернення: 09.11.2020).

37. Ахтирська Н. К вопросу об электронных доказательствах в уголовном процессе Украины. *Jurnalul juridic national: teorie şi practică (Республика Молдова)*. 2015. № 4(14). С. 122–127.

38. Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2016. Вип. 36(2). С. 123–125.

39. Белкин А.Р. Теория доказывания. Научно-методическое пособие. М.: Издательство НОРМА. 1999. 429 с.

40. Белкин Р.С. Собирание, исследование и оценка доказательств (Сущность и методы). Москва: Наука.1966. 295 с.

41. Бем М. Отримання доступу до речей і документів у світлі практики ЄСПЛ. URL: https://vkp.ua/publication/otrimannya-dostupu-do-rechey-i-dokumentiv-u-svitli-praktiki-iespl (дата звернення: 12.10.2020).

42. Бєгалов Є.П. Розслідування незаконного переправлення осіб через державний кордон України: дис…. канд. юр. наук. 12.00.09/ Національна академія внутрішніх справ, Київ, 2020. 278 с.

43. Бідняк Г.С. Використання спеціальних знань при розслідуванні шахрайств: дис. … канд. юр. наук: 12.00.09/ Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 218 с.

44. Бідняк Г.С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

45. Біленчук П.Д. Криміналістична тактика і методика розслідування окремих видів злочинів: навч. посіб. для студ. вищ. навч. закл. / П. Д. Біленчук, А. П. Гель, Г. С. Семаков. К.: МАУП, 2007. 512 с.

46. Білоус В.В. Криміналістичне значення метаданих цифрової фотографії. *Юридична наука в XXI столітті: перспективи та пріоритетні напрями досліджень:* тези доповідей міжнародної наукової практичної

конференції (м. Запоріжжя, 13-14 трав. 2016 р.)/ за заг. ред. Т.О. Коломоєць. Запоріжжя: ЗНУ, 2016. С.134–137.

47. Білоусов А.С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. … канд. юрид. наук/ 12.00.09. Київ. 2008. 18 с.

48. Бірюков В.В. Криміналістичне документознавство. Київ: Паливода А.В, 2007. 331 с.

49. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.

50. Боннер А.Т. Аудио- и видеозаписи как доказательство в гражданском и арбитражном процессе. *Законодательство.* М. 2008. №3. С.75–83.

51. Боннер О.Т. Науково-технічний прогрес і розвиток російського процесуального законодавства та судової практики. *Право України.* 2011. № 10. С. 45–62.

52. Вапнярчук В.В. Теорія і практика кримінального процесуального доказування : монографія. Х. : Юрайт, 2017. 408 с.

53. Вапнярчук В.В. Витребування та отримання, проведення інших процесуальних дій як способи збирання доказів у кримінальному провадженні. *Науковий вісник Херсонського державного університету. Серія юридичні науки.* 2015. Випуск 3 .Том 3. С. 85–89.

54. Вапнярчук В.В. Загальна характеристика властивостей доказів та їх розмежування між собою. *Держава і право*: *Збірник наукових праць. Серія Юридичні науки.* 2015. Випуск 67. С.361–375

55. Вбивцю з Twitter засудили до смертної кари. BBC news Україна. 15.12.2020. URL: https://www.bbc.com/ukrainian/news (дата звернення 15.12.2020).

56. Веб-сторінка. Портал знань. http://www.znannya.org (дата звернення: 16.11.2020).

57. Великий енциклопедичний юридичний словник/ за ред. акад. НАН України Ю.С. Шемшученка. 2-ге вид., переробл.і доповн. Київ: Юридична думка, 2012. 1020 с.

58. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. /М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

59. 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.

60. Вирок Андрушівського районного суду Житомирської області від 28.09.2017 року у справі № 296/3990/16-к. URL: http://reyestr.court.gov.ua/Review/69213571 (дата звернення: 09.10.2020).

61. Вирок Балаклійського районного суду Харківської області від 14.11.2018 року у справі №610/3451/17. URL: http://reyestr.court.gov.ua/Review/77837570# (дата звернення: 10.12.2020).

62. Вирок Вищого антикорупційного суду від 25.09.2020 року у справі 752/4292/16-к. URL: https://reyestr.court.gov.ua/Review/91800240 (дата звернення 13.11.2020).

63. Вирок Вільнянського районного суду Запорізької області від 30.11.2018 року у справі № 314/8121/16-к. URL: https://reyestr.court.gov.ua/Review/78221802 (дата звернення: 17.11.2020).

64. Вирок Гайсинського районного суду Вінницької області від 23.12.2019 року у справі № 129/1215/19. URL: http://reyestr.court.gov.ua/Review/86531564# (дата звернення: 03.12.2020).

65. Вирок Дзержинського районного суду міста Харкова від 29.05.2018 року у справі №638/3994/18. URL: http://reyestr.court.gov.ua/Review/74337878# (дата звернення: 07.12.2020).

66. Вирок Жовтневого районного суду м. Маріуполя Донецької області від 07.08.2020 року у справі №263/5377/20. URL: http://reyestr.court.gov.ua/Review/90830685# (дата звернення: 03.12.2020).

67. Вирок Зарічного районного суду м. Суми від 28.04.2016 року у справі 591/2665/15-к. URL: http://reyestr.court.gov.ua/Review/57452822 (дата звернення: 18.05.2019).

68. Вирок Індустріального районного суду м. Дніпропетровська від 01.07.2020 року у справі №200/17433/18. URL: http://reyestr.court.gov.ua/Review/90151611 (дата звернення: 19.09.2020).

69. Вирок Індустріального районного суду м. Дніпропетровська від 21.04.2017 року у справі № 202/1342/16-к. URL: http://reyestr.court.gov.ua/Review/66107826 (дата звернення: 14.05.2019).

70. Вирок Калуського міськрайонного суду Івано-Франківської області від 22.11.2017 року у справі №345/2756/17. URL: http://reyestr.court.gov.ua/Review/70420489 (дата звернення: 08.12.2019).

71. Вирок Ковпаківського районного суду м. Суми від 18.02.2019 року у справі № 592/6246/17. URL: http://reyestr.court.gov.ua/Review/79968639 (дата звернення: 05.12.2020).

72. Вирок Корольовського районного суду м. Житомира від 30.09.2015 року у справі № 296/10500/15-к. URL: http://reyestr.court.gov.ua/Review/51672384 (дата звернення: 21.05.2019).

73. Вирок Ленінського районного суду м. Кіровограда від 29.07.2020 року у справі № 405/3155/20. URL: http://reyestr.court.gov.ua/Review/90653291# (дата звернення: 03.12.2020).

74. Вирок Ленінського районного суду м. Харкова від 01.12.2015 року у справі № 642/6283/15-к. URL: http://reyestr.court.gov.ua/Review/53911255 (дата звернення: 05.06.2020).

75. Вирок Ленінського районного суду м. Харкова від 06.06.2018 року у справі №642/1999/18. URL: http://reyestr.court.gov.ua/Review/74502081 (дата звернення: 03.12.2020).

76. Вирок Ленінського районного суду м. Харкова від 21.12.2018 року у справі № 642/7101/18. URL: http://reyestr.court.gov.ua/Review/78778130# (дата звернення: 03.12.2020).

77. Вирок Любомльського районного суду Волинської області від 20.05.2015 року у справі № 163/535/15-к. URL: http://reyestr.court.gov.ua/Review/44245342 (дата звернення: 10.05.2018).

78. Вирок Новозаводського районного суду м. Чернігова від 15.05.2020 року у справі №751/2735/20. URL: http://reyestr.court.gov.ua/Review/89243759# (дата звернення: 03.12.2020).

79. Вирок Орджонікідзевського районного суду м. Запоріжжя від 21.04.2017 року у справі № 335/1279/17. URL: http://reyestr.court.gov.ua/Review/66096375 (дата звернення: 18.05.2019).

80. Вирок Першотравневого районного суду м. Чернівці від 09.07.2020 року у справі №725/1211/20. URL: http://reyestr.court.gov.ua/Review/90301368# (дата звернення: 09.11.2020).

81. Вирок Святошинського районного суду м. Києва від 25.01.2017 року у справі № 759/9988/16-к. URL: http://reyestr.court.gov.ua/Review/64299618 (дата звернення: 12.08.2019).

82. Вирок Суворовського районного суду м. Одеси від 25.10.2019 року у справі № 523/11014/19. URL: http://reyestr.court.gov.ua/Review/85198192# (дата звернення: 06.12.2020).

83. Вирок Тячівського районного суду Закарпатської області від 04.08.2016 року у справі 307/3022/14-к. URL: http://reyestr.court.gov.ua/Review/59430012 (дата звернення: 14.05.2019).

84. Вирок Херсонського міського суду Херсонської області від 27.11.2017 року у справі № 766/11084/17. URL: http://reyestr.court.gov.ua/Review/71314449 (дата звернення: 03.12.2020).

85. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс/ А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов. К, 2017. 148 с.

86. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право.* 2019. №1 (28). С.108–117.

87. Гиляка О.С. Юридичний документ: поняття, особливості, види: дисертація на здобуття наукового ступеня к.ю.н. за спеціальністю 12.00.01/ Національний юридичний університет ім. Я. Мудрого. Харків, 2017. 227 с.

88. Глібко В.М. Роль документів у розслідуванні злочинів. *Теорія і практика правознавства.* 2016. № 1. С.1–11.

89. Гонгало С.Й. Електронні документи як об'єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат*. 2013. №1(148). С.33–36.

90. Гонгало С.Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку: автореф. дис. … канд. юр. наук: 12.00.09 / Київський національний університет ім. Т. Шевченка. Київ, 2013. 21 с.

91. Гонгало С.Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку: дис. … канд. юр. наук : 12.00.09/ Київський національний університет ім. Т.Шевченка. Київ, 2013. 190 с.

92. Гонгало. С.Й. Классификация электронных документов как объектов судебной технико-криминалистической экспертизы документов. *Вестник Томского государственного университета*. 2013. № 367. С. 95–97.

93. Горбачик О.А. Стандарт метаданих для файлів в інтернет як альтернатива організації комп'ютерних архівів соціальних даних. *Актуальні проблеми соціології, психології, педагогіки*: збірник наукових праць. 2012. №17. С. 97–106.

94. Григорьев О.Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: дисс. …канд. юрид. наук: 12.00.09. Омск. 2003. 221 с.

95. Гришина Е.П. Достосверность доказательств и способы ее обеспечения в уголовном процессе : автореф. дисс. … канд. юрид.наук : 12.00.09/ МГЮА. М. 1996. 12 с.

96. Дєєв М.В. Визначення достатності доказів як складова частина

процесу оцінки доказів. *Держава та регіони. Серія: Право.* 2015. №4 (50). С. 65-74.

97. Дєєв М.В. Достатність доказів у кримінальному процесі України : дис. канд. наук: 12.00.09/ Київський національний університет ім. Т.Шевченка. Київ, 2008. 218 с.

98. Динту В.А. Місце кіберпростору у системі обстановки злочину. *Науковий вісник Херсонського державного університету.* 2016. Випуск 2. Том 3. С.72–75.

99. Докази і доказування. Кримінальний процес: підручник / за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Х.: Право, 2013. 824 с.

100. Докази та доказування у кримінальному провадженні: навч. посібник / Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін. Львів: ЛьвДУВС, 2018. 272 с.

101. Доказування у кримінальному провадженні: курс лекцій за заг. ред. О.О. Юхно. Харків: ХНУВС, 2018. 155 с.

102. Доказування у кримінальному провадженні: навч.-практ. посібн./ кол. авт. К.: Національна академія прокуратури України. 2017. 346 с.

103. ДСТУ 7157:2010. Видання електронні. Основні види та вихідні відомості. [Чинний від 2010-03-11]. Вид. Офіц. Київ, 2010. 14 с. (Інформація та документація).

104. ДСТУ ISO/IEC 27037:2017. «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. [На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT, чинний від 01.01.2019]. Вид. офіц. Київ : УкрНДНЦ, 2018. VI. 31 с.

105. Егоров Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты. Москва: Юрлитинформ. 2007. 304 с.

106. Електронні докази: регулювання, яке буде складно застосувати на практиці. URL: http://kdkako.com.ua/elektronni-dokazi-regulyuvannya-yake-bude-skladno-zastosuvati/ (дата звернення: 23.11.2020).

107. Енциклопедія державного управління : у 8 т. / Нац. акад. держ. упр. при Президентові України. Київ: НАДУ, 2011. Т. 2: Методологія державного управління. 692 с.

108. Енциклопедія державного управління : у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Київ: НАДУ, 2011. Т. 6: Державна служба. 524 с.

109. Загальнодоступний інформаційно-довідковий ресурс. Чи треба завіряти печаткою банку роздруківку електронної квитанції. URL: http://vobu.ua/ukr/analytics/consultations/item/chy-treba-zaviriaty-pechatkoiu-banku-rozdrukivku-elektronnoi-kvytantsii (дата звернення: 30.10.2020).

110. Зайцев П. Электронный документ как источник доказательств. *Законность*. 2002. № 4. С. 40–44.

111. Запотоцький А.П. Документи як процесуальні джерела доказів у кримінальному судочинстві: автореф. дис. … канд. юрид. наук: 12.00.09. Київ. 2009. 26 с.

112. Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. Москва: Юрлитинформ. 2011. 176 с.

113. Знімок екрана: матеріал з Вікіпедії. URL: https://uk.wikipedia.org/wiki (дата звернення: 11.12.2020).

114. Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 08.10.1998 року №53/5. URL: http://zakon4.rada.gov.ua/laws/show/z0705-98 (дата звернення: 18.05.2019).

115. Інформаційний лист щодо особливостей призначення та проведення судових експертиз за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів». Дніпро: Дніпропетровський НДЕКЦ МВС України. 2018. 5 с. URL: http://ndekcmvd.dp.ua (дата звернення 24.09.2020).

116. Історія GPS: від задуму до масового використання. Компанія «КОМП'ЮТЕРІНФО ТА СУЧАСНІ ТЕХНОЛОГІЇ». URL: https://freetrack.com.ua/istoriya-gps-vid-zadumu-do-masovoho-vykorystannya/ (дата звернення: 11.12.2020).

117. Каламайко А.Ю. Електронні засоби доказування в цивільному процесі: автореф. дис. ... канд. юрид. наук: 12.00.03/ Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2016. 20 с.

118. Каламайко А.Ю. Електронні засоби доказування в цивільному процесі: дис. … канд. юрид. наук: 12.00.03/ Національний юридичний університет ім. Я. Мудрого. Харків, 2016. 242 с.

119. Калужна О. Тактика збирання речей і документів як доказів у кримінальному провадженні. *Вісник Національної академії прокуратури України.* 2015. №2 (40). С. 83–90.

120. Карнеева Л.М. Доказательства в советском уголовном процессе: Усеб. пособие. Волгоград: ВСШ МВД СССР. 1988. 68 с.

121. Коваленко А.В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2018. Вип. 4. С. 237–245.

122. Коваленко А.В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України*. Х.: Право. 2017. № 1 (88). С. 182–191.

123. Коваленко Є.Г. Теорія доказів у кримінальному процесі України: Підручник. К.: Юрінком Інтер, 2006. 632 с.

124. Ковальчук С.О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи: дис. … д-ра юрид. наук: 12.00.09/ Національний університет «Одеська юридична академія». Одеса, 2018. 626 с.

125. Комп'ютерно-технічна експертиза. Незалежний інститут судових експертиз. URL: https://nise.com.ua/it-ekspertyza (дата звернення 07.10.2020).

126. Конвенція Ради Європи про кібезрлочинність від 23.11.2001 року.

URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.11.2020).

127. Котляревський О.І., Киценко Д.М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації:* збірник наукових праць. Запоріжжя. 1998. №2. С. 70–79.

128. Криміналістика: навч. посібник / Р. І. Благута, Р. І. Сибірна, В. М. Бараняк та ін.; за заг. ред. Є. В. Пряхіна. К.: Атіка, 2012. 496 с.

129. Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туман та ін.; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Х.: Пр., 2013. 824 с.

130. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI (зі змінами та доповненнями). URL: http://zakon3.rada.gov.ua/laws/show/4651-17 (дата звернення: 30.11.2020).

131. Кримінальний процесуальний кодекс України: Науково-практичний коментар / відп. ред.: С.В. Ківалов, С.М. Міщенко, В.Ю. Захарченко. Х.: Одіссей. 2013. 1104 с.

132. Крицька І.О. Речові докази у кримінальному провадженні: дис. … канд. юрид. наук 12.00.09/ Національний юридичний університет ім. Я. Мудрого. Харків, 2017. 249 с.

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

134. Крушинський С.А. Проблемні аспекти збирання та подання доказів стороною захисту у кримінальному провадженні. *Університетські наукові записки.* 2017. №63. С. 296-310.

135. Кузубова Т.О. Правові засади інституту тимчасового доступу до речей та документів у кримінальному провадженні: дис. канд. юр. наук: 12.00.09/ Харківський національний університет внутрішніх справ, Дніпропетровський державний університет внутрішніх справ. Харків, 2019. С. 250.

136. Кукарникова Т.Э. Электронный документ в уголовном процессе и криминалистике: дисс. … к.ю.н.:12.00.09/ Воронежский государственный университет. Воронеж, 2003. 204 с.

137. Лисенко В.В. Проблеми отримання і використання у доказовому процесі інформації, що міститься у електронному вигляді на магнітних, оптичних чи інших носіях (за матеріалами діяльності податкової міліції). *Вісник прокуратури*. 2007. №4. С. 61–69.

138. Лисиченко В.К. Криминалистическое исследование документов (правовые и методологические проблемы) : дис. ... д-ра юрид. наук : 12.00.09/ Киев. гос. ун-т им. Т. Г. Шевченко. Киев, 1973. 64 с.

139. Лісовий В.В. Огляд місця події при розслідуванні «комп'ютерних» злочинів. *Право України.* 2001. № 1. С. 52-54.

140. Лог. Вікіпедія. https://uk.wikipedia.org/ (дата звернення 13.12.2020).

141. Лозинська Ю.І. Теоретичні основи визначення поняття достовірності доказів у кримінальному провадженні. *Jurnalul juridic naţional: teorie şi practică.* 2017. № 4 (26). С. 162–166.

142. Малахова О.В. До питання огляду сторонами кримінального провадження змісту інтернет-сторінок. *Вісник кримінального судочинства*. 2017. Вип №2. С. 64–69.

143. Малюга Р.В. Доказування в кримінальному процесі: проблеми визначення структурних елементів. *Наукові записки Львівського університету бізнесу та права.* 2013. Вип. 11. С. 280–283.

144. Марков В.В., Савченко Р.Р. Принципи належності електронних доказів, отриманих з мобільних пристроїв. *Право і Безпека*. 2014. №1 (52). С. 89-95.

145. Метелев О.П. Цифрові докази як окремий вид доказів у кримінальному процесі. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення.* Харків: Право, 2018. Вип. 10. С.100–104.

146. Метелев О.П. Гносеологічна і правова природи цифрових доказів у кримінальному процесі. *Правова позиція.* 2018. №1 (20). С. 75–86.

147. Методика розслідування торгівлі людьми: альбом схем/ О.В. Захарова, О.І. Гарасимів, О.М. Дуфенюк, А.І. Кунтій, С.І. Марко, Є.В. Пряхін. Львів: ЛьвДУВС, 2019. 112 с.

148. Мультимедійна платформа іномовлення України «Укрінформ». За допомогою чат-бота у месенджері Telegram «СтопНаркотик» заблоковано вже 301 адресу, через яку можна було замовити наркотики. URL: https://www.ukrinform.ua/rubric-society/2857277-catbot-u-telegram-dopomig-zablokuvati-vze-ponad-300-narkoadres.html (дата звернення: 03.12.2020).

149. Мурадов В.В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. №3-2. С. 316–318.

150. Назарук Т. Метаданные: Невидимая информация о фотографии. *StopFake*. 2015. URL: https://www.stopfake.org/metadannye-nevidimaya-informatsiya-o-fotografii/ (дата звернення: 01.07.2018).

151. Нацполіція провела масштабну спецоперацію для ліквідації понад 100 інтернет-магазинів продажу наркотиків. Офіційний сайт Національної поліції. URL: http://npu.gov.ua/news (дата звернення 19.12.2020).

152. Оконенко Р.И. Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дис. … канд. юрид. наук : 12.00.09 / Моск. гос. юрид. ун-т им. О. Е. Кутафина (МГЮА). Москва, 2016. 158 с.

153. Окрема думка судді Кофанова А.В. у кримінальному провадженні від 30.11.2018 року у справі № 314/8121/16-к. URL: http://reyestr.court.gov.ua/Review/78221894 (дата звернення: 04.09.2020).

154. 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.

155. Орлов Ю.Ю. Реалізація вимог міжнародної Конвенції ро кіберзлочинність у законодавстві України. *Науковий вісник національної академії внутрішніх справ.* 2011. Випуск №6. С.3–9.

156. Орлов Ю.Ю., Чернявський С.С. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3 (104). С. 13–24.

157. Офіційний сайт Кіберполіції України. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті. URL: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/ (дата звернення 11.01.2021).

158. Павлова Ю.С. Електронний документ як джерело доказів у цивільному процесі: дис. ... канд. юрид. наук: 12.00.03/ НУ «Одеська юридична академія». Одеса, 2019. 239 с.

159. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право.* 2020. №6. С. 243-247.

160. Постанова Верховного суду від 07.09.2019 року у справі № 607/14707/17. URL: http://reyestr.court.gov.ua/Review/83589933 (дата звернення: 16.11.2020).

161. Постанова Верховного Суду від 09.04.2020 року у справі №727/6578/17. URL: https://reyestr.court.gov.ua/Review/88749345 (дата звернення: 09.10.2020).

162. Постанова Верховного суду від 10.09.2020 року у справі №751/6069/19. URL: https://reyestr.court.gov.ua/Review/91722819 (дата звернення 05.01.2021).

163. Постанова Верховного суду від 29.09.2020 року у справі № 601/1143/16. URL: http://iplex.com.ua/doc.php?regnum=92335214&red=1000035b1d3642df2806f2c7f44ef10c966d51&d=5 (дата звернення 11.01.2021).

164. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів: Закон України від 03.10.2017 р. №2147-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2147-19 (дата звернення: 05.09.2019).

165. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів: проект закону від 01.09.2020 року №4004. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення: 30.09.2020).

166. Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам: проект закону від 01.09.2020 року №4003. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770 (дата звернення: 30.09.2020).

167. Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження: Лист Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 05.04.2013 № 223-559/0/4-13. URL: https://zakon.rada.gov.ua/laws/show/v0558740-13#Text (дата звернення: 13.10.2020).

168. Про деякі питання практики вирішення спорів, пов’язаних із захистом прав інтелектуальної власності: Постанова Пленуму Вищого Господарського суду України від 17.10.2012 року №12. URL: http://zakon.rada.gov.ua/laws/show/v0012600-12 (дата звернення: 19.05.2019).

169. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: http://zakon3.rada.gov.ua/laws/show/851-15/parao7#o7 (дата звернення: 30.11.2020).

170. Про електронну комерцію: Закон України від 03.09.2015 р. № 675-VIII. URL: http://zakon2.rada.gov.ua/laws/show/675-19 (дата звернення: 30.06.2018).

171. Про затвердження Положення про електронні освітні ресурси: Наказ Міністерства освіти і науки; молоді та спорту України від 01.10.2012 р. №1060. URL: http://zakon2.rada.gov.ua/laws/show/z1695-12 (дата звернення: 01.12.2019).

172. Про звернення громадян: Закон України від 02.10.1996 року №393/96-

ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#n106 (дата звернення 12.08.2020).

173. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text (дата звернення: 09.11.2020).

174. Про телекомунікації: Закон України від 18.11.2003 р. №1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text (дата звернення: 10.05.2020).

175. Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі: постанова КМУ від 10.11.2017 року № 833. URL: http://zakon3.rada.gov.ua/laws/show/833-2017-%D0%BF (дата звернення: 09.10.2019)

176. Просняк А.О. Електронні докази в кримінальному процесі: юридичні аспекти та практичні проблеми. Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення : матеріали постійно діючого наук.- практ. семінару (м. Харків, 23 трав. 2019 р.) / редкол.: С. О. Гриненко (голов. ред.) та ін. Харків: Право, 2019. Вип. 10. С. 212–215.

177. Пчеліна О. Окремі аспекти використання спеціальних знань у галузі інформаційних і комп'ютерних технологій під час розслідування злочинів у сфері службової діяльності. *Публічне право.* 2014. №4 (16). С. 131–138.

178. Ратнова А.В. Класифікація електронних документів, як джерел доказів, у кримінальному провадженні. *Журнал східноєвропейського права.* 2021. №84. С. 42–47.

179. Ратнова А.В. Використання роздруківки та скріншоту інтернет-сторінки під час доказування у кримінальному провадженні. *Кримінальне процесуальне та криміналістичне забезпечення досудового розслідування*: матеріали науково-практичного семінару (25 жовт. 2019 р.)/ упор. Р. М. Шехавцов. Львів: ЛьвДУВС. 2019. С. 92–95.

180. Ратнова А.В. Використання даних геолокації під час доказування у кримінальному провадженні. *Механізм правового регулювання правоохоронної та правозахисної діяльності в умовах формування громадянського суспільства (осінні читання)*: збірник тез Всеукраїнської наукової конференції здобувачів вищої освіти (23 лист. 2018 р.) / упор. Л. В. Павлик. Львів: ЛьвДУВС, 2018. С.351–354.

181. Ратнова А.В. Використання метаданих під час проведення експертизи електронного документа у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування*: тези доповідей учасників науково-практичного семінару (30 лист. 2018 р.) / упор. А.Я. Хитра. Львів: ЛьвДУВС. С. 81–83.

182. Ратнова А.В. Допустимість електронних документів у кримінальному провадженні на етапі збирання доказів (Admissibility of electronic documents in criminal proceedings at the stage of evidence collection).*Sciences of Europe.* 2019. Вип. 4 (№ 44). С. 37–42.

183. Ратнова А.В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2018. Вип. 3. С. 231–241.

184. Ратнова А.В. Електронні документи як докази під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків. *Процесуальне та криміналістичне забезпечення досудового розслідування:* тези доповідей учасників науково-практичного семінару (30 жовт.2020 р.) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2020. С. 81–83.

185. Ратнова А.В. Проведення огляду облікового запису користувача в соціальній мережі під час досудового розслідування кримінального провадження. *Науково-практичний журнал «Прикарпатський юридичний вісник»*. Випуск №3(32), 2020. С.97-102.

186. Ратнова А.В. Електронний документ як джерело доказу у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення*

досудового розслідування: збірник тез науково-практичного семінару (01 грудня 2017 року). Львів: ЛьвДУВС. 2017. С. 90–94.

187. Резник Г.М. Внутреннее убеждение при оценке доказательств. М.: Юрид. лит. 1977. 120 с.

188. Рішення Ленінського районного суду м. Севастополя від 25.12.2012 року у справі № 2-2881/11. URL: http://reyestr.court.gov.ua/Review/29621337 (дата звернення: 14.05.2019).

189. Рогальська В., Михайлова О. Отримання речей і документів стороною обвинувачення в кримінальному провадженні за законодавством України / *Jurnalul juridic national: teorie si practica.* 2018. № 4. Т.2. С. 128–131.

190. Руда Т. Критерій достатності при оцінці доказів у цивільному судочинстві України і США: порівняльний аналіз. *Вісник Київського національного університету ім. Т.Шевченка. Серія юридичні науки.* 2011. Випуск №88. С.106–110.

191. Салтевський М.В. Криміналістика у сучасному викладі: підручник. К.: Кондор. 2005. 588с.

192. Салтевський М.В. Криміналістика. Підручник: У 2-х ч. Ч.1. Х.: КонСУМ. Основа. 1999. 416 с.

193. Самойленко О.А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник. Одеса, 2020. 112 с.

194. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса :ТЕС. 2020. 372 с.

195. Селезньов В.В. Основи ринкової економіки України: посібн. К.: А.С.К. 2006. 688 с.

196. Сергєєва Д. Б. Належність доказів за новим КПК України. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2013. № 3 (спец. вип.). С. 234–239.

197. Сергєєва Д.Б. Проблеми визначення достовірності доказу як його властивості за новим кримінальним процесуальним кодексом України. *Юрист*

України. 2013. №4 (25). С. 106–111.

198. Сєргєєва Д.Б., Шаповал О.В. Організація і тактика тимчасового доступу до документів під час розслідування економічних злочинів. *Вісник кримінального судочинства.* №3. 2016. С. 113–119.

199. Ситуація з наркозлочинністю є критичною в усіх регіонах України. Укрінформ. URL: https://www.ukrinform.ua (дата звернення 27.12.2020).

200. Сімашко В. Сучасні тенденції розвитку білінгу. *Наука молода* : зб. наук. праць молодих вчених ТНЕУ. 2011. № 15-16. С. 314–319.

201. Сіренко О.В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2019. Вип. 14. С. 208–214.

202. Скулиш Є.Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право*. 2014. №1 (10). С. 93–100.

203. Словник. Портал української мови та культури. URL: https://slovnyk.ua/index.php?swrd=%D0%BA%D0%B5%D1%88 (дата звернення 13.10.2019)

204. Собур С. В. Теоретичні підходи до визначення поняття «електронний документ». *Правова інформатика.* 2008. № 4(20). С.32–36.

205. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін. НАН України, Нац. б-ка України ім. В. І. Вернадського. К., 2014. 295 с.

206. Справа «Копланд проти Сполученого Королівства» Copland v. the United Kingdom): Рішення Європейського суду з прав людини від 03.04.2007 року, заява № 62617/00, Страсбург. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-117767&filename=001-117767.pdf&TID=ihgdqbxnfi (дата звернення: 23.11.2020).

207. Справа «Хамбардзумян проти Вірменії»: Рішення Європейського суду з прав людини від 05.12.2019 року, заява №43478/11. URL: http://hudoc.echr.coe.int/eng?i=001-198708 (дата звернення: 23.12.2020).

208. Справа «Шабельник проти України»: Рішення Європейського суду з

прав людини від 19.02.2009, заява №16404/03, Страсбург. URL: http://zakon3.rada.gov.ua/laws/show/974_457 (дата звернення: 02.11.2019).

209. Справа «Яременко проти України»: Рішення Європейського суду з прав людини від 12.06.2008, заява № 32092/02, Страсбург. URL: https://zakon.rada.gov.ua/laws/show/974_405 (дата звернення: 10.11.2020).

210. Справа за конституційним поданням Служби безпеки України щодо офіційного тлумачення положення ч.3 ст. 62 Конституції України: Рішення Конституційного суду України від 20.10.2011 № 1-31/2011. URL: https://zakon.rada.gov.ua/laws/show/v012p710-11 (дата звернення: 15.08.2019).

211. Стахівський С. М. Кримінально-процесуальні засоби доказування : автореф. дис. на здобут. наук. ступеня канд. юрид. наук : спец. 12.00.09. Київ, 2005. 32 с.

212. Степанов О.С. Належність та допустимість доказів у кримінальному процесі України: автореф. дис. … канд. юрид. наук: 12.00.09. Київ. 2007. 19 с.

213. Столітній А.В., Каланча І. Г. Формування інституту «електронних доказів» у кримінальному процесі України. *Проблеми законності.* 2019. Вип. 146. С. 179–191.

214. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні : дис. … д-ра. юрид. наук : 12.00.09 / Національна академія прокуратури України, Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 648 с.

215. Стоянов М.М. Властивості доказів у кримінальному процесі України: автореф. дис. ... канд. юрид. наук : 12.00.09/ Нац. університет «Одеська юридична академія». Одеса, 2010. 20 с.

216. Стоянов М.М. Система правил допустимості доказів у кримінальному провадженні України. *Актуальні проблеми держави і права*. 2013. Вип. 70. С. 245–250.

217. Теплицький Б.В., Шарай Л.Г., Ковальов К.М., Кузьмін С.А. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку : наук.-практ. посіб. Київ :

Паливода А. В., 2019. 168 с.

218. Типи адрес у мережах TCP/IP. IP адресація в мережах TCP/IP: форми запису IP–адреси: Лекція 12. URL: http://km.ptngu.com/lections/12.html (дата звернення: 10.12.2020).

219. ТОВ «Експертно-правова консалтингова компанія «Юрекс». Орієнтовні питання комп'ютерно-технічної експертизи. URL: https://yureks.com.ua/sudovi-ekspertyzy/kompiuterno-tekhnichna-ekspertyza (дата звернення 07.10.2020).

220. Тушев А.А., Назаров Н.А. Информация как основа всех видов доказательств в уголовном процессе. *Общество и право.* 2012. №3 (40). URL: https://cyberleninka.ru/article/n/informatsiya-kak-osnova-vseh-vidov-dokazatelstv-v-ugolovnom-protsesse (дата звернення 13.04.2019).

221. Узагальнення аналізу судової практики щодо використання електронних доказів під час здійснення кримінального судочинства суддями Комсомольського міського суду Полтавської області за 2018 та 2019 роки. URL: https://kom.pl.court.gov.ua/sud1612/pokazniki-diyalnosti/pidsymku_robotu/uzagalnennya_111 (дата звернення: 06.09.2020).

222. Ухвала Апеляційного суду м. Києва від 29.06.2017 року. URL: http://reyestr.court.gov.ua/Review/67858013 (дата звернення: 18.05.2019).

223. Ухвала Бершадського районний суду Вінницької області від 28.02.2017 у справі № 126/2040/16-к. URL: http://reyestr.court.gov.ua/Review/65047645 (дата звернення: 03.04.2019).

224. Ухвала Вінницького міського суду Вінницької області від 14.06.2019 року у справі №127/16197/19. URL: http://reyestr.court.gov.ua/Review/82514262 (дата звернення: 13.10.2020).

225. Ухвала Галицького районного суду м. Львова від 11.05.2018 року у справі № 461/1143/18. URL: http://reyestr.court.gov.ua/Review/73935448 (дата звернення: 17.09.2019).

226. Ухвала Галицького районного суду м. Львова від 13.07.2018 року у справі № 461/4858/18. URL: https://reyestr.court.gov.ua/Review/75285640 (дата

звернення 13.11.2020).

227. Ухвала Галицького районного суду м. Львова від 29.04.2016 року у справі № 461/5592/15-к. URL: http://reyestr.court.gov.ua/Review/57475054 (дата звернення: 04.06.2018).

228. Ухвала Голопристанського районного суду Херсонської області від 07.04.2020 року у справі № 654/292/20. URL: https://reyestr.court.gov.ua/Review/88973144 (дата звернення 11.01.2021).

229. Ухвала Дніпровського районного суду м. Дніпродзержинська Дніпропетровської області від 11.01.2021 року у справі №209/3843/20. URL: https://reyestr.court.gov.ua/Review/94062298 (дата звернення: 12.01.2021).

230. Ухвала Жовтневого районного суду м. Дніпропетровська від 26.06.2019 року у справі № 201/7375/19. URL: https://zakononline.com.ua/court-decisions/show/82783231 (дата звернення:10.11.2020).

231. Ухвала Жовтневого районного суду м. Запоріжжя від 16.02.2017 року у справі № 331/5137/16-к. URL: http://reyestr.court.gov.ua/Review/64754080 (дата звернення: 16.02.2020).

232. Ухвала Заводського районного суду м. Миколаєва від 02.05.2019 року у справі № 487/8662/18. URL: http://reyestr.court.gov.ua/Review/81498815 (дата звернення: 15.10.2020).

233. Ухвала Київського районного суду м. Полтава від 22.04.2020 року у справі № 552/5337/19. URL: http://reyestr.court.gov.ua/Review/88864501 (дата звернення: 16.11.2020).

234. Ухвала Кіровського районного суду м. Кіровограда від 04.03.2016 року у справі. URL: № 404/1446/16-к. http://reyestr.court.gov.ua/Review/56298647 (дата звернення: 20.09.2020).

235. Ухвала Колегії суддів судової палати з розгляду кримінальних справ Львівського апеляційного суду від 06.02.2019 року у справі № 461/485/17. URL: http://reyestr.court.gov.ua/Review/79744493 (дата звернення: 04.09.2019).

236. Ухвала Луцького міськрайонного суду Волинської області від 04.02.2019 року у справі № 161/1438/19. URL:

http://reyestr.court.gov.ua/Review/79603809 (дата звернення: 17.11.2020).

237. Ухвала Новоукраїнського районного суду Кіровоградської області від 27.05.2020 року у справі 287/3/19. URL: http://reyestr.court.gov.ua/Review/89476008 (дата звернення: 16.11.2020).

238. Ухвала Печерського районного суду м. Києва від 04.08.2017 року у справі 757/45163/17-к. URL: http://reyestr.court.gov.ua/Review/68461188 (дата звернення: 12.03.2018).

239. Ухвала Печерського районного суду м. Києва від 10.07.2019 року у справі № 757/32181/19-к. URL: http://reyestr.court.gov.ua/Review/82940763 (дата звернення: 09.11.2020).

240. Ухвала Печерського районного суду м. Києва від 12.07.2018 року у справі № 757/32158/18-к. URL: http://reyestr.court.gov.ua/Review/75396252 (дата звернення: 05.08.2019).

241. Ухвала Печерського районного суду м. Києва від 12.07.2018 року у справі № 757/32174/18-к. URL: http://reyestr.court.gov.ua/Review/75396270 (дата звернення: 08.09.2019).

242. Ухвала Печерського районного суду м.Києва від 17.03.2016 року у справі № 757/12089/16-к. URL: http://reyestr.court.gov.ua/Review/56950544 (дата звернення: 18.05.2019).

243. Ухвала Приморського районного суду м. Одеси від 10.02.2020 року у справі № 522/12728/19. URL: http://reyestr.court.gov.ua/Review/87580083 (дата звернення: 17.11.2020).

244. Ухвала Сєвєрдонецького міського суду Луганської області від 30.07.2019 року у справі № 428/8462/19. URL: http://reyestr.court.gov.ua/Review/83357851 (дата звернення:15.12.2020).

245. Ухвала Солом'янського районного суду м. Києва від 19.07.2019 року у справі №760/16979/19. URL: http://reyestr.court.gov.ua/Review/84005340 (дата звернення: 09.10.2020).

246. Ухвала Старокостянтинівського районного суду Хмельницької області від 21.03.2018 року у справі № 683/362/17. URL: http://reyestr.court.gov.ua/Review/72967641 (дата звернення: 19.07.2019).

247. Ухвала Центрального районного суду м. Миколаєва від 01.08.2018 року у справі № 490/6183/18. URL: http://reyestr.court.gov.ua/Review/75950191 (дата звернення: 09.11.2020).

248. Ухвала Червоноармійського районного суду Житомирської області від 17.03.2020 у справі №292/329/20. URL: https://reyestr.court.gov.ua/Review/88243069 (дата звернення 13.11.2020).

249. Ухвала Шевченківського районного суду м. Києва від 18.06.2019 року у справі № 761/19131/19. URL: http://reyestr.court.gov.ua/Review/82512811 (дата звернення: 16.11.2020).

250. Файли cookies. URL: https://www.nissan.ua/legal/cookies.html (дата звернення 13.12.2020)

251. Фаринник В. Особливості формування доказів та доказування в кримінальному судочинстві України. Х.: Фактор. 2013. 96 с.

252. Федотов Н.Н. Форензика – Компьютерная криминалистика. М.: Юридический мир, 2007. 432 с.

253. Фулей Т.І. Застосування практики Європейського суду з прав людини при здійсненні правосуддя: Науково-методичний посібник для суддів. 2-ге вид. випр., допов. Київ, 2015. 208 с.

254. Харківський П.П. Комп’ютерно-технічна експертиза. *Проблемні питання.* Криміналістичний вісник. 2014. №2 (22). С.97–100.

255. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право*. 2017 р. №4 (58). С. 80–85.

256. Хом’яченко С.І., Часова Т.О. Використання електронних доказів у кримінальному процесі. *Право. Людина. Довкілля: науково-практичний журнал.* 2020. 11 (2). С. 175–181.

257. Цехан Д.М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 256–260.

258. Цехан Д.М. Використання високих інформаційних технологій в ОРД ОВС: монографія. Одеса, 2011. 216 с.

259. Чаплинський К.О. Тактика проведення окремих слідчий дій: монографія. Дніпропетровськ, 2006. 416 с.

260. Черкаський НДЕКЦ. Комп'ютерно-технічна експертиза. URL: https://ndekc.ck.ua/novini/740-kompyuterno-tehnichna-ekspertiza.html (дата звернення 07.10.2020).

261. Чернявський С.С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ : Хай-Тек Прес. 2010. 624 с.

262. Чигрина Г.Л. Джерела доказів у кримінальних справах про ухилення від сплати податків, зборів, інших обов'язкових платежів: автореф. дис. … канд. юр.наук: 12.00.09 / Національний університет внутрішніх справ. 2004. 21 с.

263. Чупрікова І.Л. Допустимість доказів у світлі нового Кримінального процесуального кодексу: дис. … канд. юрид. наук : 12.00.09/ НУ «Одеська юридична академія». Одеса, 2016. 191 с.

264. Чупрікова І.Л. Належне джерело отримання доказів як гарантія допустимості. *Юридичний науковий електронний журнал.* 2015. Вип.№4. С. 266–269.

265. Шабаровський Б.В. Перевірка доказів у кримінальному процесі України: дис. … канд. юрид. наук: 12.00.09/ Національний університет «Острозька академія», Львівський національний університет ім. І. Франка. Львів, 2019. 237 с.

266. Шведова О.В. Комплексне криміналістичне дослідження документів, виконаних за допомогою комп'ютерних технологій: автореф. дис. … канд. юрид. наук: 12.00.09. Київ. 2006. 19 с.

267. Шехавцов Р.М., Кудінов С.С. Речові докази та інші матеріальні об'єкти, що отримуються в результаті проведення негласних слідчих

(розшукових) дій: проблеми визначення та використання в кримінальному провадженні. *Південноукраїнський правничий часопис.* 2015. Випуск №2. С. 186–190.

268. Шило А.В. Використання в кримінальному провадженні відомостей, отриманих у результаті проведення негласних слідчих (розшукових) дій : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2019. 241 с.

269. Шульгін С.О. Достатність доказів як підстава прийняття процесуальних рішень слідчим та прокурором. *Право та державне управління.* 2019. Випуск №2 (35). Т.2. С. 109–116.

270. Юридична енциклопедія: в 6 т. / Ю.С. Шемшученко (голова редкол.) та ін. Київ: Українська енциклопедія, 1998 . Т.2: Д-Й. 744 с.

271. Юхно О.О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС.* 2016. №2 (16). С. 86–95.

272. Як очистити кеш і видалити файли cookie. Google Довідка. URL: https://support.google.com/ (дата звернення: 11.12.2020).

273. Ясковець С. Що таке браузер і які функції він виконує. URL: https://rdob-blog.ucoz.ua/files/NTC (дата звернення 15.09.2018).

274. Яцик Т.П. Розслідування інформаційного тероризму та кіберзлочинності (міжнародно-правовий аспект). *Міжнародний юридичний вісний: актуальні проблеми сучасності (теорія та практика).* 2017. Випуск 1(5). С. 111–115.

ДОДАТКИ

Додаток А

Узагальнені результати опитування (207 респондентів) працівників підрозділів органів Національної поліції

№ п/п	Запитання	Кількість осіб	%
1.	**Ваша посада:**		
	1.1. Слідчий або дізнавач	92	44,4%
	1.2. Старший слідчий	19	9,2%
	1.3. Заступник керівника органу досудового розслідування	5	2,4%
	1.4. Керівник органу досудового розслідування або керівник органу дізнання	3	1,5%
	1.5. Оперуповноважений	71	34,3%
	1.6. Старший оперуповноважений	17	8,2%
2.	**Ваш стаж практичної роботи на посаді:**		
	2.1. До 1 року	13	6,3%
	2.2. Від 1 до 3 років	35	17%
	2.3. Від 3 до 5 років	71	34,3%
	2.4. Від 5 до 10 років	57	27,5%
	2.5. Більше 10 років	31	14,9%
3.	**Чи доводилось Вам раніше, під час проведення досудового розслідування, або виконання доручень слідчого/дізнавача збирати електронні документи?**		
	3.1. Так	178	86%
	3.2. Ні	18	8,7%
	3.3. Мені невідомо що це	11	5,3%
	3.3. Документи або речові докази	106	51,2%
4.	**З яким різновидом електронних документів, під час проведення досудового розслідування, Ви зустрічались? (декілька варіантів відповідей)**		
	4.1. Відеозаписи	173	25,8%
	4.2. Аудіозаписи	128	19,1%
	4.3. Цифрові фотографії та зображення	189	28,2%
	4.4. Електронні повідомлення (смс- та ммс-повідомлення, електронна пошта, соціальні месенджери тощо)	76	11,3%
	4.5. Вебсайти	84	12,5%
	4.6. Дані геолокації (GPS)	17	2,5%
	4.7. Свій варіант	4	0,6%
5.	**Які способи збирання електронних документів, на Вашу думку, здійснюються зазвичай? (декілька варіантів відповідей)**		
	5.1. Витребування та отримання	83	10,9%
	5.2. Огляд (місця події, приміщення)	172	22,8%
	5.3. Обшук	185	24,4%
	5.4. Зняття інформації з транспортних телекомунікаційних мереж	79	10,4%
	5.5. Зняття інформації з електронних інформаційних систем	81	10,7%
	5.6. Тимчасовий доступ до речей та документів (як захід забезпечення) з подальшим проведення огляду	158	20,8%

6.	**Під час вилучення електронних документів, слід:**		
	6.1. Вилучати усю техніку	123	59%
	6.2. Копіювати усю інформацію на фізичні носії	85	40,5%
	6.3. Свій варіант	2	0,5%
7.	**Чи існують відмінності у тактиці огляду «традиційних» доказів та електронних документів?**		
	7.1. Так, існують суттєві відмінності	186	89,8%
	7.2. Відмінності несуттєві	15	7,2
	7.3. Ні, відмінностей немає.	6	3%
8.	**Чи необхідно залучати спеціаліста або експерта під час збирання та дослідження електронних документів?**		
	8.1. Так, у більшості випадків необхідно	134	64,7%
	8.2. В окремих випадках	64	32,4%
	8.3. Ні, не потрібно	9	2,9%
9.	**Чи призначали ви проведення електронних документів?**		
	9.1. Так	125	60%
	9.2. Ні	82	40%
10.	**Які судові експертизи, на Вашу думку, найдоцільніше призначати під час дослідження електронних документів? (декілька варіантів відповідей)**		
	10.1. Семантико-текстуальна	49	7,6%
	10.2. Лінгвістична	34	5,3%
	10.3. Фототехнічна	64	9,8%
	10.4. Портретна	57	8,7%
	10.5. Комп’ютерно-технічна	165	25,4%
	10.6. Апаратно-комп’ютерна (як різновид комп’ютерно-технічної)	101	15,5%
	10.7. Комп’ютерно-мережева (як різновид комп’ютерно-технічної)	167	25,7%
	10.8. Свій варіант	13	2%
11.	**На Вашу думку, у яких кримінальних правопорушеннях найчастіше джерелами доказів є електронні документи?**		
	11.1. Проти основ національної безпеки України		
	11.2. Проти життя та здоров’я особи	69	10%
	11.3. Проти волі честі та гідності особи	0	0
	11.4. Проти статевої свободи та статевої недоторканості особи	46	6,7%
	11.5. Проти виборчих, трудових та інших особистих прав і свобод людини і громадянина	0	0
	11.6. Проти власності	75	10,9%
	11.7. У сфері господарської діяльності	73	10,6%
	11.8. Проти довкілля	0	0
	11.9. Проти громадської безпеки	60	8,7%
	11.10. Проти безпеки виробництва	0	0
	11.11. Проти безпеки руху та експлуатації транспорту	74	10,8%
	11.12. Проти громадського порядку та моральності	0	0
	11.13. У сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші кримінальні правопорушення проти здоров’я населення	83	12,1%

	11.14. У сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації	0	0
	11.15. Проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та кримінальні правопорушення проти журналістів	0	0
	11.16. У сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку	98	14,3%
	11.17. У сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг	0	0
	11.18. Проти правосуддя	0	0
	11.19. Проти встановленого порядку несення військової служби (військові кримінальні правопорушення)	0	0
	11.20. Проти миру, безпеки людства та міжнародного правопорядку	0	0
	11.21. Усі вищеперераховані	109	15,9%
12.	**Чи відчували Ви труднощі під час збирання та дослідження електронних документів? Якщо так, то з якими саме? (декілька варіантів відповідей)**		
	12.1. Труднощів не виникало.	6	0,1%
	12.2. Відсутність законодавчого закріплення поняття та критеріїв їх оцінки	54	6%
	12.3. Складність процесу встановлення оригіналу, копії, дублікату інформації в електронній формі	98	10,4%
	12.4. Відсутність базових знань у сфері інформаційних технологій	62	7%
	12.5. Відсутність сформованої методики збирання та використання	79	8,5%
	12.6. Відсутність технічних засобів для копіювання, вилучення, транспортування, зберігання таких доказів	154	16,3%
	12.7. Відсутність ліцензійного програмного забезпечення для копіювання, вилучення, транспортування, зберігання таких доказів (у тому числі ліцензійних операційних систем)	167	17,7%
	12.8. Відсутність достатньої кількості спеціалістів для залучення до проведення слідчих (розшукових) дій	143	15,1%
	12.9. Складність призначення експертизи (складення переліку питань, направлення доказів, тривалість експертизи)	178	18,8%
	12.10. Свій варіант	4	0,1%

Додаток Б

Статистика Національної поліції України

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ БОРОТЬБИ З НАРКОЗЛОЧИННІСТЮ
просп. Повітрофлотський, 24/2,
м. Київ, 03049, тел. 363-18-69,
dbn@antidrug.gov.ua,
код згідно з ЄДРПОУ 43673764

січня 2021 року № _____

На № _____ від _____

Аліні Ратновій

Івано-Франківська область, 77303

Про надання інформаційних матеріалів

За дорученням керівництва Національної поліції України Департаментом боротьби з наркозлочинністю в межах компетенції розглянуто Ваш запит на отримання публічної інформації про надання звіту про стан боротьби з наркозлочинністю протягом 2017-2020 рр. та з інших питань.

За результатами опрацювання надсилаємо Вам запитувану інформацію в розрізі статей Кримінального кодексу України.

Водночас інформуємо, що належним розпорядником інформації про зареєстровані кримінальні правопорушення та результати їх досудового розслідування у державі є Офіс Генерального прокурора як держатель Єдиного реєстру досудових розслідувань (наказ Офісу Генерального прокурора від 30 червня 2020 року № 298). На підставі даних ЄРДР органами прокуратури здійснюється формування єдиної (за результатами роботи усіх органів досудового розслідування у цілому по державі) звітності про кримінальні правопорушення та осіб, які їх учинили.

Додатки: 1. Стан боротьби з наркозлочинністю за період 2017-2020 рр. на 1 арк.;
2. Звіт про результати оперативно-службової діяльності підрозділів Департаменту кіберполіції Національної поліції України у сфері протидії кіберзлочинності протягом 2017-2020 років на 3 арк.

Начальник
підполковник поліції **Сергій ФЕДЧЕНКО**

Ігор Чупряк
363-1852-0774

Додаток 1

Стан боротьби з наркозлочинністю за період 2017-2020 рр.

Результати роботи	Роки				Динаміка
	2017	2018	2019	2020	
Зареєстровано кримінальних правопорушень у сфері незаконного обігу наркотиків	27772	25904	27982	27315	-2%
Кількість кримінальних правопорушень, по яких особі повідомлено про підозру	22731	20218	20652	21217	3%
Задокументовано фактів використання коштів, отриманих від незаконного обігу наркотичних засобів (ст. 306 КК України)	38	112	69	144	109%
Викрито організованих злочинних груп та злочинних організацій (ст. 28 КК України)	27	63	68	95	40%
Зареєстровано тяжких та особливо тяжких злочинів	5621	6235	7353	9578	30%
Зареєстровано фактів схиляння злочинцями громадян до вживання наркотичних засобів і психотропних речовин (ст. 315 КК України)	41	32	43	37	-14%
Задокументовано фактів схиляння неповнолітніх до вживання наркотиків (ч. 2 ст. 315 КК України)	8	3	4	4	
Зареєстровано злочинів щодо збуту наркозасобів з використанням мережі Інтернет	143	196	421	1175	179%
Задокументовано кримінальних правопорушень за фактом збуту наркотичних засобів і психотропних речовин (ст. 307 КК України)	4445	5098	6152	8096	32%

Департамент боротьби з наркозлочинністю Національної поліції України

Додаток 2

ЗВІТ
про результати оперативно-службової діяльності підрозділів Департаменту кіберполіції Національної поліції України у сфері протидії кіберзлочинності протягом 2017-2020 років

1. Виявлення кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій.

Усього, протягом звітних періодів 2017-2020 років *(з урахуванням раніше вчинених кримінальних правопорушень)* працівниками ДКП супроводжувалося **18709** кримінальних проваджень (2017 – ***5328***, 2018 – ***4864***, 2019 – ***3734***, 2020 – ***4783***).

Порівняльна таблиця виявлених кримінальних правопорушень у сфері використання високих інформаційних технологій протягом 2017-2020 років

Підрозділ	Виявлено КП за 2017 рік	Виявлено КП за 2018 рік	Виявлено КП за 2019 рік	Виявлено КП за 2020 рік
ДКП	4068	3233	1839	2873

Сфери виявлення кримінальних правопорушень

ст. КК України	2017	2018	2019	2020
І. У сфері обігу протиправного контенту і телекомунікацій:				
ст. 176	26	43	53	45
ст. 229	8	20	6	18
ч. 3, 4, 5 ст. 301	320	369	104	172
Усього:	**354**	**432**	**163**	**235**
ІІ. У банківській сфері:				
ст. 185	329	334	159	136
ст. 200	210	230	180	432
ст. 231	54	217	0	1
ст 362	478	440	362	510
Усього:	**1071**	**1221**	**701**	**1079**
ІІІ. У сфері онлайн шахрайств:				
ч. 3, 4 ст. 190	1922	900	354	822
Усього:	**1922**	**900**	**354**	**822**
IV. У сфері комп'ютерних систем:				
ст. 361	670	576	458	598
ст. 361-1	8	65	140	88
ст. 361-2	39	28	21	50
ст. 363	2	2	0	0
ст. 363-1	2	9	2	1
Усього:	**721**	**680**	**621**	**737**

2. Результати розслідування кримінальних правопорушень у сфері високих інформаційних технологій за матеріалами ДКП.

ст. КК України	Кількість КП у яких особам повідомлено про підозру у вчиненні кримінального правопорушення				Кількість осіб, яким повідомлено про підозру у вчиненні кримінального правопорушення			
	2017	2018	2019	2020	2017	2018	2019	2020
I. У сфері обігу протиправного контенту і телекомунікацій:								
ст. 176	23	37	61	34	20	17	20	7
ст. 229	2	13	11	2	4	8	10	5
ч. 3, 4, 5 ст. 301	318	373	108	167	58	51	21	33
Усього:	**343**	**423**	**180**	**203**	**82**	**76**	**51**	**45**
II. У банківській сфері:								
ст. 185	353	347	175	163	217	95	119	128
ст. 200	222	209	235	475	35	28	39	30
ст. 231	55	215	1	0	4	6	1	0
ст 362	509	479	355	542	46	58	49	79
Усього:	**1139**	**1250**	**766**	**1180**	**302**	**187**	**208**	**237**
III. Онлайн шахрайства:								
ч. 3, 4 ст. 190	1979	1019	444	809	323	209	120	175
Усього:	**1979**	**1019**	**444**	**809**	**323**	**209**	**120**	**175**
IV. У сфері комп'ютерних систем:								
ст. 361	617	505	429	592	112	110	102	109
ст. 361-1	7	55	148	91	4	33	37	36
ст. 361-2	38	19	23	51	6	7	16	21
ст. 363	1	0	1	0	2	0	1	0
ст. 363-1	0	8	1	0	0	1	1	0
Усього:	**663**	**587**	**602**	**734**	**124**	**151**	**157**	**166**
Усього за ДКП	**4124**	**3279**	**1992**	**2926**	**831**	**623**	**536**	**623**
Усього за період	**12321**				**2613**			

За результатами звітних періодів 2017 – 2020 років за матеріалами ДКП закінчено досудове розслідування у ***12374*** кримінальних провадженнях (2017 – ***3946***, 2018 – ***3363***, 2019 – ***2131***, 2020 – ***2934***), з них до суду з обвинувальними актами направлено – **11444** (2017 – ***3724***, 2018 – ***3129***, 2019 – ***1929***, 2020 – ***2662***). Протягом вказаного періоду **2029** особам пред'явлено обвинувальні акти (2017 – ***633***, 2018 – ***496***, 2019 – ***401***, 2020 – ***499***).

Загальна установлена сума матеріальних збитків у кримінальних провадженнях, розпочатих за ознаками кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій становить ***163 млн. 734 тис. грн.,*** **сума відшкодованих збитків**, з урахуванням накладеного арешту та вилученого майна, становить ***77 млн. 583 тис. грн.***

3. Протидія організованим групам та злочинним організаціям.

Протягом звітних періодів 2017 – 2020 років за матеріалами ДКП до суду з обвинувальними актами направлено **37** кримінальних проваджень (2017 – *7*,

2018 – *11*, 2019 – *5*, 2020 – *14*) відносно протиправної діяльності організованих злочинних груп у складі **134** осіб (організаторів – **37**, активних учасників – **97**).

Зазначеними злочинними групами на території України вчинено **600** злочинів, з яких – **564** тяжких та особливо тяжких.

Департамент кіберполіції Національної поліції України

Додаток В

Пропозиції та зауваження до Проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» (реєстр. № 4003 від 01.09.2020)

ВЕРХОВНА РАДА УКРАЇНИ

Комітет з питань правоохоронної діяльності

01008, м.Київ-8, вул. М. Грушевського, 5, тел.: 255-35-06

Національна академія правових наук України

Національний інститут стратегічних досліджень

Інститут законодавства Верховної Ради України

Національний юридичний університет імені Ярослава Мудрого

Національна академія внутрішніх справ

Харківський національний університет внутрішніх справ

Дніпропетровський державний університет внутрішніх справ

Львівський державний університет внутрішніх справ

Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України

У Комітеті Верховної Ради України з питань правоохоронної діяльності знаходиться на опрацюванні проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» (**реєстр. № 4003 від 01.09.2020**), поданий народним депутатом України Д. Монастирським та іншими народними депутатами України.

Враховуючи значущість сфери правового регулювання, відповідно до пункту 9 частини першої статті 15 Закону України «Про комітети Верховної Ради України» та статті 93 Регламенту Верховної Ради України з метою підготовки зазначеного проєкту для попереднього розгляду Комітетом просимо, за наявності, **до 05 жовтня 2020 року** надати Ваші пропозиції та зауваження до нього на адресу Комітету через СЕВ ОВВ (систему електронної взаємодії органів виконавчої влади), а у разі відсутності технічної можливості - засобами поштового зв'язку на адресу Комітету та електронну пошту: cherniienko@rada.gov.ua.

Ознайомитися з вказаним вище законопроєктом можна на сайті Верховної Ради України за адресою:

http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

Голова Комітету **Д. Монастирський**

МВС УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

вул. Городоцька, 26, м. Львів, 79007
тел.: (032) 295-47-74 факс: (032) 233-11-19, 233-24-34
vdzr@lvduvs.edu.ua

05.10.2020 № 23/1855
На № 04-27/3-2020/155025 від 11.09.2020

Голові Комітету з питань
правоохоронної діяльності
Верховної Ради України
Денису МОНАСТИРСЬКОМУ

Про надання пропозицій

Шановний Денисе Анатолійовичу!

Направляємо пропозиції до проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» (реєстр. № 4003 від 01.09.2020).

Додатки: пропозиції на 6 арк. у 1 прим.

З повагою
ректор **Роман БЛАГУТА**

Пропозиції та зауваження до Проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» (реєстр. № 4003 від 01.09.2020)

Положення проєкту	Пропозиції	Обґрунтування
Стаття 110. Процесуальні рішення … 6. Постанова слідчого, прокурора виготовляється на офіційному бланку та підписується службовою особою, яка прийняла відповідне процесуальне рішення. **У разі необхідності постанова слідчого, прокурора про термінове збереження інформації виготовляється на офіційному бланку в електронній формі та засвідчується кваліфікованим електронним підписом службової особи, яка прийняла відповідне процесуальне рішення, відповідно до вимог Закону України «Про електронні документи та електронний документообіг».**	**Постанова слідчого, прокурора може бути виготовлена на офіційному бланку в електронній формі з засвідченням кваліфікованим електронним підписом службової особи, яка прийняла відповідне процесуальне рішення, відповідно до вимог Закону України «Про електронні документи та електронний документообіг».**	Накладення електронного підпису може здійснюватись не тільки на постанову слідчого, прокурора про термінове збереження інформації, але і на інші постанови.
Стаття 164[1]. Постанова прокурора, слідчого про тимчасовий доступ до терміново збереженої інформації 1. У постанові прокурора, слідчого про тимчасовий доступ до терміново збереженої інформації має бути зазначено: 1) реєстраційний номер кримінального провадження; 2) правову кваліфікацію кримінального правопорушення із зазначенням статті (частини статті) Кримінального кодексу України;	1-1) короткий виклад обставин кримінального правопорушення, у зв'язку з яким подається клопотання.	Вважаємо, що клопотання про тимчасовий доступ до терміново збереженої інформації повинен відповідати ст. 160 КПК України. Наприклад, п.1, 5 ч.2 ст.160 КПК України не зазначені у даній статті, тому їх слід врахувати у новій запропонованій редакції.

3) прізвище, ім'я та по батькові або найменування власника, володільця або утримувача електронних інформаційних систем або їх частин, або мобільних терміналів систем зв'язку, інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем або невід'ємних частин цих систем, які мають надати тимчасовий доступ до терміново збереженої інформації; 4) назва, опис, інші відомості, які дають можливість визначити терміново збережену інформацію; 5) розпорядження надати (забезпечити) тимчасовий доступ до терміново збереженої інформації, зазначеної в постанові прокурора, слідчого та надати їм можливість зняти копії цієї інформації; 6) положення закону, які передбачають наслідки невиконання постанови прокурора, слідчого.	4-1) значення терміново збереженої інформації для встановлення обставин у кримінальному провадженні.	

Пропозиції та зауваження до Проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» (реєстр. № 4004 від 01.09.2020)

ВЕРХОВНА РАДА УКРАЇНИ

Комітет з питань правоохоронної діяльності

01008, м.Київ-8, вул. М. Грушевського, 5, тел.: 255-35-06

Назарук Ю. 14.09.20
Красницький
Пр. надати пропозиції
та зауваження
Т. Созанський
11.09.2020

Національна академія правових наук України

Національний інститут стратегічних досліджень

Інститут законодавства Верховної Ради України

Національний юридичний університет імені Ярослава Мудрого

н. Яременко 21.09.20.

Національна академія внутрішніх справ

Пр. надати пропозиції
до 30.09.2020
16.09.2020

Харківський національний університет внутрішніх справ

Дніпропетровський державний університет внутрішніх справ

н. О. Данчук
Для організації виконання
21.09.20.

Львівський державний університет внутрішніх справ

н. Хитра
Прошу підготувати пропозиції
22.09.2020

Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України

У Комітеті Верховної Ради України з питань правоохоронної діяльності знаходиться на опрацюванні проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» (**реєстр. № 4004 від 01.09.2020**), поданий народним депутатом України Д. Монастирським та іншими народними депутатами України.

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Вх.№ 1714 від "11" 09 2020 р.
кількість аркушів
Осн.док. 2 додат. –

Враховуючи значущість сфери правового регулювання, відповідно до пункту 9 частини першої статті 15 Закону України «Про комітети Верховної Ради України» та статті 93 Регламенту Верховної Ради України з метою підготовки зазначеного проєкту для попереднього розгляду Комітетом просимо, за наявності, **до 05 жовтня 2020 року** надати Ваші пропозиції та зауваження до нього на адресу Комітету через СЕВ ОВВ (систему електронної взаємодії органів виконавчої влади), а у разі відсутності технічної можливості - засобами поштового зв'язку на адресу Комітету та електронну пошту: cherniienko@rada.gov.ua.

Ознайомитися з вказаним вище законопроєктом можна на сайті Верховної Ради України за адресою:

http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

Голова Комітету **Д. Монастирський**

МВС УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

вул. Городоцька, 26, м. Львів, 79007
тел.: (032) 295-47-74 факс: (032) 233-11-19, 233-24-34
vdzr@lvduvs.edu.ua

05. 10. 2020 № 23/1854
На № 04-27/3-2020/155028 від 11. 09. 2020

Про надання пропозицій

Голові Комітету з питань
правоохоронної діяльності
Верховної Ради України
Денису МОНАСТИРСЬКОМУ

Шановний Денисе Анатолійовичу!

Направляємо пропозиції до проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» (реєстр. № 4004 від 01.09.2020).

Додатки: пропозиції на 12 арк. у 1 прим.

З повагою
ректор **Роман БЛАГУТА**

Пропозиції та зауваження до Проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» (реєстр. № 4004 від 01.09.2020)

Положення проєкту	Пропозиції	Обґрунтування
Стаття 93. Збирання доказів … 2. Сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання, **у тому числі шляхом копіювання, збереження**, від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом. 3. Сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, здійснює збирання доказів шляхом витребування та отримання**, у тому числі шляхом копіювання, збереження**, від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів	не потребує змін	Копіювання та збереження може здійснюватись під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій, витребування та отримання доказів та не потребує додаткового уточнення у даній частині статті. Про копіювання доказу зазначається у заключній частині протоколу, що передбачено ч. 3 ст. 104 КПК України

перевірок; ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів. …		
Стаття 100[1]. Електронні докази 1. 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. 2. 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.		(до ч. 2) Не надано визначення понять «віртуальні активи», «метадані», «веб-сайт» і «веб-сторінка» та їх різниця, що може спричинити неоднакове трактування.
Стаття 104. Протокол … 3. Протокол складається з:		Неможливо встановити спосіб підтвердження цілісності та справжності.

… 3) заключної частини, яка повинна містити відомості про: **отриману інформацію в електронній (цифровій) формі та спосіб підтвердження її цілісності та справжності;** вилучені речі і документи та спосіб їх ідентифікації;		
у статті 164: пункт 1 викласти в такій редакції: «1) прізвище, ім'я та по батькові особи або найменування органу досудового розслідування, прокуратури, якій (якому) надається право тимчасового доступу до інформації в електронній (цифровій) формі, речей і документів»; пункт 6 викласти в такій редакції: «6) розпорядження надати (забезпечити) тимчасовий доступ до інформації в електронній (цифровій) формі, речей і документів зазначеній в ухвалі особі або офіційному представнику органу досудового розслідування, прокуратури та надати їй (йому) можливість вилучити речі і документи, якщо відповідне рішення було прийнято слідчим суддею, судом»;	**Стаття 3.** Визначення основних термінів Кодексу … 27) офіційний представник органу досудового розслідування чи прокуратури -	Тимчасовий доступ до відомостей в електронній формі, речей і документів може здійснювати лише уповноважений на те суб'єкт. Зокрема, належним суб'єктом, який уповноважений на проведення досудового розслідування є слідчий, визначений керівником органу досудового розслідування для здійснення конкретного кримінального провадження (п.1 ч.2 ст.39, ч. 1 ст. 214 КПК України). Винесення ухвали про тимчасовий доступ цілому органу досудового розслідування чи прокуратури може спричинити в подальшому недопустимість отриманих в результаті його проведення доказів. Таким чином, лише ті слідчі, прокурори, які зазначені у витягу з ЄРДР, постанові про призначення слідчого/групи слідчих, постанові про призначення прокурора/групи прокурорів та оперативні працівники, які призначені постановою про створення слідчо-оперативної групи є належними суб'єктами та повинні зазначатись у відповідні ухвалі слідчого судді/суду. Неможливо встановити яким чином підтверджується повноваження офіційного представника (довіреність чи інший документ), яка може бути у нього посада. У зв'язку з невизначеністю даного суб'єкта можна дійти

		висновку що офіційним представником органу досудового розслідування може бути навіть інспектор. В той же час, вичерпний перелік сторін кримінального провадження зазначений у п.19 ч. 1 ст. 3 КПК України. Офіційний представник органу досудового розслідування чи прокуратури не є стороною кримінального провадження та не має жодних повноважень на проведення будь-яких процесуальних дій у кримінальному провадженні.
		У проєкті не надано роз'яснень щодо порядку використання, зберігання електронних доказів, які були знаряддям (програма, вірус) вчинення кримінального правопорушення, зберегли сліди (наприклад, база даних під час несанкціонованого втручання в роботу). Тобто тих доказів, які за своїм змістом є речовими доказами. Таким чином, складно встановити який порядок збирання, зберігання речового доказу в електронній формі, оскільки це специфічний доказ якому притаманні особливості речових та електронних доказів.

Додаток Г

Словник термінів, які використані у дисертації

№	Термін	Визначення	Джерело
1.	Cookie-файли	Невеликі за обсягом текстові файли, які зберігаються на комп'ютері, планшеті чи мобільному телефоні користувача з метою аналізу користування вебсайтом та покращення роботи з системами.	272
2.	GPS	(Global Positioning System) збірне поняття яке застосовується до всіх приладів та систем супутникової навігації.	116
3.	IP-адреси	(з англ. «Internet Protocol address» - унікальний код пристрою у мережі Інтернет, який використовується на мережевому рівні та призначається адміністратором.	218
4.	Log-файл	спеціальний файл, у якому накопичується зібрана службова та статистична інформація про події в системі (програмі). Операційні системи (особливо це стосується серверних ОС) та серверне програмне забезпечення зазвичай мають розвинуту систему ведення логів. За допомогою них можна змусити систему (програму) реєструвати у лог-файлах фактично будь-які події. Відповідно різні типи подій, різну інформацію можна зберігати у своїх спеціалізованих логах.	140
5.	Адреса мережі Інтернет	визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв.	174
6.	Білінгові системи	телекомунікаційні підприємства, у яких автоматизовано основний технологічний процес, а саме: укладання договорів з клієнтами, надання послуг, проведення розрахунків зі споживачами, облік реалізації послуг та платежів за послуги.	200, с. 314-315
7.	Браузер	програма, яка використовується в мережі Інтернет для пошуку, обробки, перегляду вебсайтів, виведення сторінок на екран для пошуку потрібної інформації.	273
8.	Веб-сторінка	Інформаційний ресурс доступний в мережі World Wide Web (Всесвітня павутина), який можна переглянути у веб-браузері . Зазвичай, ця інформація записана в форматі HTML або XHTML , і може містити гіпертекст з навігаційними гіперпосиланнями на інші веб-сторінки.	241
9.	Інтернет	всесвітня інформаційна система загального доступу, яка логічно зв’язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами.	174
10.	Інформаційна технологія (ІТ)	цілеспрямована організована сукупність інформаційних процесів з використанням засобів	173

		обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.	
11.	Кеш	місце для тимчасового зберігання даних і команд, які часто використовуються.	203
12.	Кеш-файли	файли, які розміщуються в кеші браузера.	272
13.	Метадані	це структуровані дані, що виступають характеристиками певних сутностей та призначені для їх ідентифікації, пошуку, оцінювання, відповідного управління тощо.	93, с. 99
14.	Скріншот	Знімок екрана (англ. screenshot, скриншот, зняток) — зображення, отримане комп'ютером, що зображує дійсно те, що бачить користувач на екрані монітора. Це зображення створене із запису видимих елементів екрана комп'ютера або іншого візуального пристрою виведення інформації. Як правило, це цифрове зображення створюється операційною системою або спеціальним програмним забезпеченням, хоча може також бути зроблене за допомогою фотокамери або іншого приладу для перехоплення сигналу відео з виходу комп’ютера.	113
15.	Трафік	сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію.	174

Додаток Д

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Ратнова А.В. Проведення огляду облікового запису користувача в соціальній мережі під час досудового розслідування кримінального провадження. *Науково-практичний журнал «Прикарпатський юридичний вісник»*. 2020. Випуск №3 (32). С. 97-102 *(стаття в науковому виданні, включеному до переліку наукових фахових видань України з присвоєнням категорії «Б»)*.

2. Ratnova A. The state of scientific development of an electronic document as evidence in criminal proceedings. *Visegrad Journal on Human Rights*. 2020. № 5. P. 210-214 *(стаття в періодичному науковому виданні іншої держави, яка входить до Організації економічного співробітництва та розвитку та Європейського Союзу)*.

3. Ратнова А.В. Класифікація електронних документів, як джерел доказів, у кримінальному провадженні. *Журнал східноєвропейського права.* 2021. №84. С. 42-47 *(стаття в науковому виданні, включеному до переліку наукових фахових видань України з присвоєнням категорії «Б»)*.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4. Ратнова А.В. Електронний документ як джерело доказу у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування:* збірник тез науково-практичного семінару (01 груд. 2017 р.) / упор. А.Я. Хитра, Р.М. Шехавцов, Є.В. Пряхін, С.І. Марко. Львів: ЛьвДУВС. 2017. С. 90-94.

5. Ратнова А.В. Використання даних геолокації під час доказування у кримінальному провадженні. *Механізм правового регулювання правоохоронної та правозахисної діяльності в умовах формування громадянського суспільства (осінні читання)*: збірник тез Всеукраїнської наукової конференції здобувачів вищої освіти (23 лист. 2018 р.) / упор. Л.В. Павлик. Львів: ЛьвДУВС, 2018. С. 351-354.

6. Ратнова А.В. Використання метаданих під час проведення експертизи електронного документа у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування*: тези доповідей учасників науково-практичного семінару (30 лист. 2018 р.) / упор. А.Я.Хитра. Львів: ЛьвДУВС. 2018. С. 81-83.

7. Ratnova A. Legal admissibility of electronic documents as evidence in Ukraine. *Право. Комунікація. Суспільство. Law. Communication. Society. Das recht. Die kommunikation. Das geselschaft. Le droit. La communication. La société*: матеріали науково-практичної конференції здобувачів вищої освіти (українською та іноземними мовами) (12 квіт. 2019 р.) / за заг. ред. канд. філол. наук, доц. І.Ю. Сковронської. Львів: ЛьвДУВС. 2019. С. 117-119.

8. Ратнова А.В. Використання роздруківки та скріншоту інтернет-сторінки під час доказування у кримінальному провадженні. *Кримінальне процесуальне та криміналістичне забезпечення досудового розслідування*: матеріали науково-практичного семінару (25 жовт. 2019 р.) / упор. Р.М. Шехавцов. Львів: ЛьвДУВС. 2019. С. 92-95.

9. Ратнова А.В. Електронні документи як докази під час розслідування злочинів, пов’язаних з незаконним обігом наркотиків. *Процесуальне та криміналістичне забезпечення досудового розслідування:* тези доповідей учасників науково-практичного семінару (30 жовт. 2020 р.) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2020. С. 81-83.

Наукові праці, які додатково відображають наукові результати дисертації:

10. Ратнова А.В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2018. Вип. 3. С. 231-241.

11. Ратнова А.В. Допустимість електронних документів у кримінальному провадженні на етапі збирання доказів. *Sciences of Europe.* 2019. VOL 4. № 44. С. 37-42.

Додаток Е

Акти впровадження

ЗАТВЕРДЖУЮ
Перший проректор
Львівського державного університету
внутрішніх справ
кандидат юридичних наук, доцент
полковник поліції

Тарас СОЗАНСЬКИЙ
2021

АКТ

25.01. 2021 Львів № 10

Про впровадження результатів дисертації Ратнової Аліни Володимирівни на тему: «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні» в освітній процес ЛьвДУВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

- заступника начальника відділу організації наукової роботи кандидата юридичних наук Галини САВЧИН;
- заступника начальника навчально-методичного відділу кандидата юридичних наук, доцента Олега РИБАКА;
- в.о. декана факультету № 1 ІПФПНП кандидата юридичних наук, доцента підполковника поліції Руслана ШЕХАВЦОВА;
- завідувача кафедри кримінального процесу та криміналістики факультету №1 кандидата юридичних наук, доцента, підполковника поліції Андрія ХИТРИ.

Комісія відповідно до наказу по університету від 24 вересня 2012 року №431 розглянула й узагальнила результати дисертації, поданої на здобуття ступеня доктора філософії у галузі права за спеціальністю 12.00.09 – кримінальний процес та криміналістика, судова експертиза, оперативно-розшукова діяльність, та наукові праці ад'юнкта кафедри кримінального процесу та криміналістики факультету №1 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ Ратнової Аліни Володимирівни за темою дисертації «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні».

Проаналізовано основні результати дослідження Ратнової А.В., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Ратнова А.В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2018. Вип. 3. С. 231-241.

2. Ратнова А.В. Допустимість електронних документів у кримінальному провадженні на етапі збирання доказів. *Sciences of Europe.* VOL 4, № 44, (2019). С. 37-42.

3. Ратнова А.В. Проведення огляду облікового запису користувача в соціальній мережі під час досудового розслідування кримінального провадження. *Науково-практичний журнал «Прикарпатський юридичний вісник»*. Випуск №3(32), 2020. С. 97-102.

4. Ratnova A. The state of scientific development of an electronic document as evidence in criminal proceedings. *Visegrad Journal on Human Rights.* 2020. № 5. P. 210-214.

5. Ратнова А.В. Класифікація електронних документів, як джерел доказів, у кримінальному провадженні. *Журнал східноєвропейського права.* №84. 2021. С. 42-47.

6. Ратнова А.В. Електронний документ як джерело доказу у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування: збірник тез науково-практичного семінару (01 грудня 2017 року)* / упор. А.Я. Хитра, Р.М. Шехавцов, Є.В. Пряхін, С.І. Марко. Львів: ЛьвДУВС. С. 90-94.

7. Ратнова А.В. Використання даних геолокації під час доказування у кримінальному провадженні. *Механізм правового регулювання правоохоронної та правозахисної діяльності в умовах формування громадянського суспільства (осінні читання): збірник тез Всеукраїнської наукової конференції здобувачів вищої освіти* (23 листопада 2018 року) / упор. Л. В. Павлик. Львів: ЛьвДУВС, 2018. С. 351-354.

8. Ратнова А.В. Використання метаданих під час проведення експертизи електронного документа у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 листопада 2018 року)* / упор. А.Я. Хитра. Львів: ЛьвДУВС. С. 81-83.

9. Ratnova A. Legal admissibility of electronic documents as evidence in Ukraine. *Право. Комунікація. Суспільство. Law. Communication. Society. Das recht. Die kommunikation. Das geselschaft. Le droit. La communication. La société: матеріали науково-практичної конференції здобувачів вищої освіти (українською та іноземними мовами)* / за заг. ред. канд. філол. наук, доц. І. Ю. Сковронської. Львів: ЛьвДУВС, (12.04.2019). С. 117-119.

10. Ратнова А.В. Використання роздруківки та скріншоту інтернет-сторінки під час доказування у кримінальному провадженні. *Кримінальне процесуальне та криміналістичне забезпечення досудового розслідування: матеріали науково-практичного семінару (25 жовтня 2019 р.)* / упор. Р. М. Шехавцов. Львів: ЛьвДУВС, 2019. С. 92-95.

11. Ратнова А.В. Електронні документи як докази під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків. *Процесуальне та*

криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 жовтня 2020 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2020. С. 81-83.

На основі проведеного аналізу комісія зробила висновок, що наукові праці Ратнової А.В. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Львівського державного університету внутрішніх справ, зокрема при викладанні навчальних дисциплін «Кримінальний процес», «Криміналістика», «Теоретичні проблеми кримінального судочинства», «Досудове розслідування», «Дізнання», а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти освітнього ступеня «бакалавр» та «магістр».

Члени комісії:

Галина САВЧИН

Олег РИБАК

Руслан ШЕХАВЦОВ

Андрій ХИТРА

ЗАТВЕРДЖУЮ
Заступник начальника слідчого управління Головного Управління Національної поліції України у Львівській області
підполковник поліції

Андрій ТКАЧИК

25.01.2021

АКТ

25.01.2021 м. Львів № 1133

Про впровадження результатів дисертації Ратнової Аліни Володимирівни на тему: «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні»

Комісія у складі:

- Старший слідчий ОМВ СУ ГУНП у Львівській області капітан поліції Вайда Сергій Олегович;
- Слідчий ОМВ СУ ГУНП у Львівській області майор поліції Цап Олеся Володимирівна.

розглянула й узагальнила наукові праці ад'юнкта кафедри кримінального процесу та криміналістики факультету №1 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ старшого лейтенанта поліції Ратнової Аліни Володимирівни за темою дисертації «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні».

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Ратнова А.В. Електронний документ та його місце у системі доказів у кримінальному провадженні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2018. Вип. 3. С. 231-241.
2. Ратнова А.В. Допустимість електронних документів у кримінальному провадженні на етапі збирання доказів. *Sciences of Europe.* VOL 4, № 44, (2019). С. 37-42.
3. Ратнова А.В. Проведення огляду облікового запису користувача в соціальній мережі під час досудового розслідування кримінального провадження. *Науково-практичний журнал «Прикарпатський юридичний вісник».* Випуск №3(32), 2020. С. 97-102.
4. Ratnova A. The state of scientific development of an electronic document as evidence in criminal proceedings. *Visegrad Journal on Human Rights.* 2020. № 5.

Р. 210-214.

5. Ратнова А.В. Класифікація електронних документів, як джерел доказів, у кримінальному провадженні. *Журнал східноєвропейського права.* №84. 2021. С. 42-47.

6. Ратнова А.В. Електронний документ як джерело доказу у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування: збірник тез науково-практичного семінару (01 грудня 2017 року)* / упор. А.Я. Хитра, Р.М. Шехавцов, Є.В. Пряхін, С.І. Марко. Львів: ЛьвДУВС. С. 90-94.

7. Ратнова А.В. Використання даних геолокації під час доказування у кримінальному провадженні. *Механізм правового регулювання правоохоронної та правозахисної діяльності в умовах формування громадянського суспільства (осінні читання): збірник тез Всеукраїнської наукової конференції здобувачів вищої освіти* (23 листопада 2018 року) / упор. Л. В. Павлик. Львів: ЛьвДУВС, 2018. С. 351-354.

8. Ратнова А.В. Використання метаданих під час проведення експертизи електронного документа у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 листопада 2018 року)* / упор. А.Я. Хитра. Львів: ЛьвДУВС. С. 81-83.

9. Ratnova A. Legal admissibility of electronic documents as evidence in Ukraine. *Право. Комунікація. Суспільство. Law. Communication. Society. Das recht. Die kommunikation. Das geselschaft. Le droit. La communication. La société: матеріали науково-практичної конференції здобувачів вищої освіти (українською та іноземними мовами)* / за заг. ред. канд. філол. наук, доц. І. Ю. Сковронської. Львів: ЛьвДУВС, (12.04.2019). С. 117-119.

10. Ратнова А.В. Використання роздруківки та скріншоту інтернет-сторінки під час доказування у кримінальному провадженні. *Кримінальне процесуальне та криміналістичне забезпечення досудового розслідування: матеріали науково-практичного семінару (25 жовтня 2019 р.)* / упор. Р. М. Шехавцов. Львів: ЛьвДУВС, 2019. С. 92-95.

11. Ратнова А.В. Електронні документи як докази під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків. *Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 жовтня 2020 року)* / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2020. С. 81-83.

На основі проведеного аналізу комісія дійшла висновку, що наукові праці Ратнової А.В. містять науково обґрунтовані теоретичні положення та практичні рекомендації та можуть використовуватись у практичній діяльності підрозділів досудового розслідування СУ ГУНП України у Львівській області, а також під час проведення занять зі службової підготовки.

Члени комісії: **Сергій ВАЙДА**

Олеся ЦАП