DOI: 10.31359/2079-6242-2022-46-49
УДК 343.1(477):347.991

Н. В. Глинська, доктор юридичних наук, старший науковий співробітник завідувачка відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної Академії правових наук України
ORCID ID 0000-0001-5835-3798

Д. І. Клепка, кандидат юридичних наук, старший науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної Академії правових наук України
ORCID ID 0000-0001-8423-4581

ОСНОВНІ АСПЕКТИ СТРАТЕГІЇ УНОРМУВАННЯ ІНСТИТУТУ ЦИФРОВИХ ДОКАЗІВ В КРИМІНАЛЬНОМУ ПРОЦЕСУАЛЬНОМУ ЗАКОНОДАВСТВІ*

Постановка проблеми. Одним з аспектів впливу цифрового суспільства на кримінальне провадження є той факт, що цифрова інформація в тому чи іншому статусі займає значний сегмент інформаційного фонду цієї царини. Відповідно джерелами такої інформації в кримінальних провадженнях все частіше стають цифрові (будь-які типи електронних носіїв, електронні пристрої чи електронні інформаційні системи), у яких відображаються обставини кримінального правопорушення або проведені процесуальні дії. Втім, на справедливу думку сучасних дослідників, які предметно вдавались до аналізу питань діджиталізації кримінальної процедури, реалізувати увесь доказовий потенціал цифрової інформації в кримінальному процесі перешкоджають низка якість нормативно-правового регулювання, неузгодженість та непослідовність окремих нормативних правил, а також непристосованість чинної процесуальної форми до цифрових реалій сьогодення[1]. Відсутня і єдність думок серед науковців як щодо місця носіїв цифрової інформації у системі джерел доказів в кримінальному процесі (визнання носіїв цифрової інформації документами, речовими доказами, виділення цифрових носіїв доказової інформації в окреме процесуальне джерело доказів, поліваріантність закріплення цифрової інформації (цифрова інформація залежно від умов, способу й суб'єкта створення, процедури отримання та закріплення може бути будь-яким із джерел доказів[2]), так й щодо їх назви («електронні докази», «електронно-цифрові докази», «комп'ютерні докази», «цифрові докази», «електронні відображення та ін.) та розуміння їх сутності. Не ставлячи перед собою за мету докладний аналіз всього спектру дотичних наукових позицій, що вже знаходило неодноразове висвітлення у сучасній літературі[3], позначимо, що полярність наукових думок та чинна нормативна «непристосованість» до цифрової

* *Примітка.* Стаття виконаніа за фундаментальною темою «Теоретико-правові проблеми цифровізації кримінального провадження в Україні» (№ державної реєстрації в УкрІНТЕІ: 0121U114401)

[1] Скрипник А. В. *Використання цифрової інформації в кримінальному процесуальному доказуванні* : монографія (Право, 2022) 7

[2] Столітній А. В. 'Електронне кримінальне провадження на досудовому розслідуванні' (дис. д-ра. юрид. наук. Національна академія прокуратури України, Дніпропетровський державний університет внутрішніх справ, 2018) 127

[3] Див. зокрема: Скрипник А. В. 103–108; Гутник А. В., Хитра А. Я. *Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія* (ЛьвДУВС, 2022) 12–17

реальності є надто шкідливим чинником, що визначає неоднорідність правозастосовної практики щодо «допущення» цифрової інформації у доказову площину конкретної справи, а отже збільшує ризики для всебічного, повного та об'єктивного встановлення обставин справи, а значить й ухвалення по ній справедливого судового рішення. У зв'язку з цим, на наше переконання, необхідним є формування стратегічного (концептуального) підходу до нормативної регламентації правового режиму цифрових доказів (далі – ЦД).

Аналіз останніх досліджень і публікацій. Дослідженню електронних доказів присвячені роботи Г. К. Авдєєвої, В. М. Бутузова, С. Й. Гонгало, І. О. Крицької, В. В. Лисенка, М. Ю. Літвінова, В. О. Мещерякова, М. В. Салтевського, А. В. Скрипника, А. В. Столітнього, М. Є. Шуміло, В. Ю. Шепітька та ін. Водночас наукова розвідка юридичної літератури свідчить про відсутність розробки стратегії унормування інституту електронних доказів у кримінальному процесуальному законі.

Метою статті є визначення основних аспектів стратегії унормування електронних доказів в кримінальному провадженні України.

Виклад основного матеріалу. Структура цього дослідження обумовлена вирішенням таких завдань, як обґрунтування доцільності інституціоналізації ЦД, ідентифікації та систематизації основних практичних викликів (можливих небезпек), пов'язаних з оперуванням ЦД, формулювання основних стратегічних та тактичних аспектів інституціоналізації ЦД у національному кримінальному процесуальному законодавстві. Тож для досягнення поставленої мети, преш за все, видається необхідним вдатися до наукової розвідки питання специфіки цифрової інформації та її носіїв.

Щодо специфіки ЦД[1]. Цифровій (електронній) інформації, під якою тут і далі будемо розуміти призначені для обробки засобами цифрової техніки дискретні дані, представлені в доступній для сприйняття людиною формі[2], притаманні такі іманентні ознаки: електронне (електронно-цифрове) середовище її існування (цифрова інформація існує в іншому, відмінному від аналогового вимірі); позбавленість суб'єктивності (така інформація створена за допомогою апаратних та програмних засобів, підкорюється детермінованим правилам, заданих програмою); закодованість (неможливість безпосереднього сприйняття людиною, потребує її перетворення на доступну для сприйняття людиною форму), з чого випливає, що у своїй повноті ЦД з'являється під час відтворення змісту файлу; мобільність чи мінливість (можливість просто і швидко змінити свою об'єктивну форму, передаватись на будь-які відстані); «невловний характер інформації, легкість внесення змін або знищення); тиражованість (здатність зберігатися в аутентичному вигляді під час копіювання або інших операцій) та ін[3].

Цифрові докази відрізняються від інших тим, що вони створені за допомогою електронних пристроїв, зберігаються та розповсюджуються лише за допомогою електронних носіїв інформації та комп'ютерних або телекомунікаційних мереж. Вони стають доступними для сприйняття людиною лише після обробки засобами електронної техніки з відповідним програмним забезпеченням[4].

У спрощеному (практичному) вигляді під цифровими (електронними) доказами ми розуміємо будь-яку інформацію, яка зберігається або передається у цифровій формі та має значення для кримінального провадження. До речі дослідження А. В. Ратновою питання правового режиму електронних доказів як засобів доказування у правових системах різних країн світу виявило, що у Європейських країнах використовується аналогічний до вище наведеного підходу до розуміння електронного доказу (будь-який тип інформації, що має доказове значення та зберігається на будь-якому цифровому пристрої або передається у двійковій або цифровій формі (Португалія); інформація, яка зберігається або передається у цифровій формі та має значення кримінального розслідування (Німеччина), будь-яка доказова інформація, яка створюється, зберігається або передається у цифровій

[1] *Примітка.* У цьому дослідженні ми не ставимо за мету формування термінологічного апарату. Тому нами використовується поняття як цифрових так і електронних доказів, або цифрових (електронних) доказів для позначення цифрової інформації яка має доказове значення в кримінальному провадженні.

[2] Скрипник А. В.

[3] Скрипник А. В. 94–98

[4] Авдєєва Г. 'Проблеми використання електронних доказіву протидії кіберзлочинності' *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) ХНУВС, 2020. <http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9089/Protydiia%20kiberzlochynnosti%20ta%20torhivli%20liudmy_2020.pdf?sequence=1&isAllowed=y> (дата звернення: 23.09.2023)

формі за допомогою електронних пристроїв та має значення для досудового розслідування кримінальних правопорушень (Франція)[1].

Одне з визначень поняття «електронні докази» дав проєкт Evidence, який діє під егідою USAID, згідно з яким електронні докази – це будь-які дані, отримані від аналогового пристрою та/або цифрового пристрою потенційного значення, які генеруються, обробляються, зберігаються або передаються за допомогою будь-якого електронного пристрою. Цифрові докази – це електронні докази, які формуються або перетворюються в числовий формат[2]. Як влучно зазначає Д. О. Московчук це визначення важливе, оскільки воно уточнює різні визначення, запропоновані багатьма вченими, а також усуває деякі їх неясності, а також воно враховує всі можливі варіанти електронних доказів і демонструє глибоку міждисциплінарну природу цього поняття. Наведене вище визначення електронних доказів має ширше застосування, ніж будь-які інші. Отже, електронні докази – це інформативний цифровий компонент, який приймає багато форм, наприклад електронний лист, зображення, аудіо та фотографії, за допомогою яких можна пов'язати сторони, свідків, експертів та інших учасників справи[3].

З огляду на викладене цілком поділяємо позицію щодо віднесення ЦД до окремого виду доказів у кримінальному провадженні. Як раціонально та ґрунтовно зазначає О. П. Метелев, 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 й просторі, а також кримінальні процесуальні процедури та 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[4].

Щодо доцільності нормативного врегулювання інституту ЦД.

Питання унормування інституту ЦД по-різному вирішено у країнах світу. Як зазначає Д. О. Московчук у своєму компаративістському монографічному дослідженні, присвяченому електронним доказам у цивільному судочинстві, різні правові системи по-різному відреагували на появу феномену цифрової інформації. «Деякі системи запровадили нове законодавство, яке конкретно стосується електронних доказів, як зробила це Україна декілька років тому. Інші системи намагаються встановити «найбільшу відповідність» наявним доказовим концепціям і, де це можливо, застосовували чинні правила аналогічно, наприклад, чи є електронний доказ прийнятним, залежить від того, чи був він подібним до доказу (паперового) документа чи доказу шляхом візуального огляду. ..Там, де вводиться нове законодавство, акцент робиться на відмінності між електронними та традиційними формами доказів. … Там, де використовуються аналогічні підходи, акцент робиться на подібності між традиційними та електронними доказами, а це, своєю чергою, може призвести до неналежного застосування правил доказування..»[5].

КПК на відміну від інших процесуальних кодексів України фактично не визнає електронні (цифрові) докази як самостійні засоби доказування (процесуальні джерела доказів)[6]. Водночас за-

[1] Ратнова А. В. 'Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні'(дис. доктора філософії, Львівський державний університет внутрішніх справ, 2021) 248.

[2] Biasiotti M. A., Cannataci J. A., Bonnici J. P. M., Turchi F. 'Introduction: opportunities and challenges for electronic evidence' *In: Handling and exchanging electronic evidence across Europe*. (Springer, Cham, Switzerland, 2018) 5

[3] Московчук Д. О. 'Електронні докази у країнах континентального та загального права: порівняльно – правове дослідження' (дис. доктора філос., Національний університет «Одеська юридична академія», 2023) 73–74

[4] Метелев О. П. 'Цифрові докази як окремий вид доказів у кримі- нальному процесі' (2018) 10 Досудове розслідування: актуальні проблеми та шляхи їх вирішення. 100–104

[5] Московчук Д. О. 46

[6] *Примітка.* Зміни щодо електронних доказів, унесені Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 03.10.2017 р. № 2147VIII.

конодавець визнав об'єктивність існування окремого різновиду інформації у спосіб віднесення в ч. 2 ст. 99 КПК України до документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, також матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі *комп'ютерних даних*). За певних умов електронний документ може виступати як речового доказу, крім того, цифрові об'єкти можуть бути предметом накладення арешту в порядку статті 170 КПК (віртуальні активи). До того ж цифрова інформація може бути включена в орбіту доказування в кримінальному процесі як неодмінний додаток до протоколу слідчих чи негласних слідчих (розшукових) дій.

Утім таке точкове згадування про електронну інформацію як засіб доказування не вносить визначеність стосовно низки питань, пов'язаних із «цифровим доказуванням». Тож КПК на сьогодні виявився не адаптованим до світової цифрової революції. Адже «…під час доказової діяльності у кримінальному провадженні все частіше застосовуються новітні технології фіксації слідів злочину, встановлення осіб, які його вчинили, проте не завжди отримані відомості використовуються як докази в суді, можуть бути покладені у підґрунтя судового рішення. Чинники, які негативно позначаються на правозастосовній практиці, пов'язані перш за все із відсутністю належного законодавчого інструментарію; …крім того, діалектичну єдність із процесом правозастосування має юридична термінологія, що міститься в законі або якою оперує правова доктрина. Тим часом слід констатувати відсутність єдності в підходах до розуміння таких понять, як «комп'ютерний доказ», «цифровий доказ», «цифрова інформація», «електронний документ», «комп'ютерна інформація», «електронний носій інформації», «документ, виготовлений за допомогою комп'ютерних технологій» тощо»[1]. І якщо найменування нового виду доказів, чи то комп'ютерними, електронними, цифровими тощо не є принциповим, відсутність нормативного алгоритму їх фіксації, оцінки та збереження є надто шкідливим для перспективи доказової валентності зібраних цифрових даних.

Проблематика визначеності нормативного регулювання питань використання цифрових (електронних) доказів вже давно ставилась як серед вчених, так і практиків. Адже «…чинним законодавством України встановлюються лише загальні принципи застосування електронного виду доказів, порядку їх збору та способів дослідження в електронній формі, а тому на практиці виникає чимало питань щодо їх використання[2]». В цьому сенсі влучно зазначено в одному з міжнародних джерел: «правила, які суттєво регулюють розслідування традиційних злочинів на основі фізичних фактів, призводять до проблематичних результатів при застосуванні до розслідування злочинів на основі використання інформаційно-комунікаційних технологій»[3].

Нагадаємо що ця проблематика була поставлена у Моніторинговому звіті за 2021 рік, підготовленому Директоратом правосуддя та кримінальної юстиції Міністерства юстиції України[4]. Звернімо увагу також на рекомендації, що сформульовано у Звіті щодо України, підготовленому Офісом Програми з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Маркко Куннапу і пана Марка Юріча, про чинне законодавство і проєкти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них (2016/DGI/JP/3608 3 листопада 2016 року). Відпо-

---

У ст. 96 Господарського процесуального кодексу України, ст. 99 Кодексу адміністративного судочинства України, ст. 100 Цивільного процесуального кодексу України (далі – ЦПК України) законодавцем закріплено єдину позицію та визначено, що електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет). Загалом в ЦПК України (як і в ГПК України та КАС України) докази поділено на: письмові (ст. 95 ЦПК України), речові (ст. 97 ЦПК України) та електронні (ст. 100 ЦПК України).

[1] Шумило М. Є., Раймундас Ю., Капліна В. А. 'Інформаційна теорія доказів та проблеми Використання електронних засобів доказування у кримінальному провадженні' (2019) 26 (2) Вісник Національної академії правових наук України 139

[2] Сіренко О. В, Короткова Є. О. 'Досвід упровадження системи електронного кримінального провадження в Україні та ЄС' (2021) 3 Юридичний науковий електронний журнал <http://lsej.org.ua/3_2021/87.pdf> (дата звернення: 23.09.2023)

[3] 'Electronic evidence – Belgium'(EJN Forum) <https://www.ejnforum.eu/cp/e-evidence-fiche/230/0> (дата звернення: 23.09.2023)

[4] Міністерство юстиції України. Директорат правосуддя та кримінальної юстиції. Моніторинговий звіт за 2021 рік / відпов. ред. к.ю.н. Олійник О. М. <https://minjust.gov.ua/m/monitoring-vprovadjennya-ta-analiz-efektivnosti-npa.> 234–247

відно до рекомендацій 9–10 цього Звіту «наявність конкретних критеріїв щодо визначення електронних доказів може й не бути абсолютною необхідністю, проте є дуже цінною. По-перше, запровадження такої дефініції значно спростило б процес розробки конкретних процесуальних заходів. Це особливо важливо, оскільки інші правила КПК, пов'язані з доказами, не відповідають концепції електронних доказів, адже всі наявні процесуальні заходи орієнтовані на доказ як на фізичний або матеріальний об'єкт. По-друге, запровадження поняття «електронних доказів» збільшить правову чіткість і передбачуваність закону. Створення спеціальних законів про електронні докази та відповідні процесуальні заходи дозволять установити правила щодо прийнятності електронних доказів»[1].

Тож потреба унормування в КПК комплексу питань щодо використання електронних доказів у кримінальному провадженні є нагальною, а воєнний стан ще більш актуалізував її.

Щодо основних праксеологічних викликів – орієнтирів формування нормативної стратегії «цифрового доказування» в кримінальному провадженні

На практиці проблемні питання у контексті «цифрового доказування» є наскрізними та виникають майже на кожному з етапів пізнавально-практичної діяльності. Тож проілюструємо деякі з них.

Окремим практичним викликом до інституціоналізації електронних доказів є ризики пошуку та *використання інформації з відкритих джерел*. Так у зв'язку із необхідністю розслідування воєнних злочинів, учинених на території України, для забезпечення притягнення до кримінальної відповідальності винних осіб у національній та міжнародній юрисдикціях актуальним є використання в кримінальному провадженні цифрових даних, що містяться у відкритих джерелах інформації (як-то: контент у соцмережах, відео-, фотоконтент, супутникові знімки, карти та інша онлайн-інформація) як доказів у відповідних провадженнях.

Проте сьогодні у роботі органів досудового розслідування є певні складнощі щодо системного розуміння фіксації відповідної цифрової інформації із джерел відкритого доступу. Серед таких проблем: можливість застосування моніторингу та користувацького пошуку в соціальних мережах, результати зняття інформації з електронних інформаційних систем, правова оцінка скриншотів, співвідношення оригіналу доказу та його копії[2]. Адже, як влучно зауважено, єдиним в Україні офіційним документом, який стосується ЦД є Національний стандарт України ДСТУ ISO/IEC 27037:2017[3]. У ньому викладені настанови щодо ідентифікації, збирання, здобуття та збереження ЦД, однак, законодавчого закріплення ці рекомендації поки що не мають[4].

Корисним інструментом у цьому аспекті є представлений у 2020 р. Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини «Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права» (Протокол Берклі), який містить стандарти й методологічні підходи до збирання, збереження та аналізу інформації у відкритому доступі, яка може слугувати доказом у кримінальному провадженні[5]. Втім зазначений документ здебільшого є інструментом збирання та фіксації цифрової інформації, у якому викладені алгоритми пошуку, накопичення, аналізу та збереження цифрової інформації з відкритих джерел із дотриманням принципів об'єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини та ін.

---

[1] Звіт щодо України, підготовлений Офісом Програми з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Маркко Куннапу і пана Марка Юріча, про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них (2016/DGI/JP/3608 3 листопада 2016 року). <https://rm.coe.int/16806f3743.> Цит. За: Шило О. Г., Шило А. В. 'До питання впровадження в Україні електронного кримінального провадження' *Правові засади діяльності правоохоронних органів*: збірник наукових статей, тез доповідей та повідомлень за матеріалами VII Міжнародної науково-практичної конференції (10–11 грудня 2020 року, Харків) Вип. 36. 109–111.

[2] 'Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел' (Судова влада України, 7 червня 2022) <https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/?fbclid=IwAR38uhyaCGNZyG19U7Wjs3l20JCS3uuPfSCwOeUx4BFW9iWWysF6297brsY> (дата звернення: 8.06.2022)

[3] ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT). Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Чинний від 01.01.2019 р., УкрНДНЦ, Київ, 2018. 31 с.

[4] Авдеєва Г. К.

[5] Berkeley Protocol on Digital Open Source Investigations. United Nations Human Right. New York and Geneva, 2022. 102 p. https://www.ohchr.org/sites/default/files/2022–04/OHCHR_BerkeleyProtocol.pdf. (дата звернення: 23.09.2023)

Питання ж *оцінки електронних доказів*, отриманих з відкритих джерел, за відсутності нормативних орієнтирів залишаються відкритими. Як зазначає суддя Верховного Суду (далі – ВС) О. Яновська, «ми можемо зіткнутися із ситуацією, коли принцип безпосередності дослідження цифрових доказів судом не зможе бути дотриманий. Наприклад, є відкриті дані, вони певним чином фіксуються, але потім у відкритих джерелах вони змінюються або зникають. У такій ситуації потрібно застосовувати рекомендацію щодо архівації даних, які містяться у відкритих джерелах. Слідчі, відповідні спеціалісти та судді повинні чітко розуміти цей алгоритм дій. На жаль, на сьогодні, ми не можемо оперувати таким алгоритмом, що давав би відповідь на запитання про те, якою має бути послідовність збереження даних, що містяться у відкритих джерелах, щоб у суді не виникало питань щодо достовірності таких даних»[1].

До того ж очевидною є граничність правомірності збору даних із відкритих джерел із порушенням конвенційних прав та свобод людини[2]. В цьому сенсі Протокол Берклі за своєю суттю є також цінним дороговказом, певною дорожньою картою щодо оцінки та управління ризиками, які супроводжують збір інформації у відкритому доступі, зокрема й ризиками правомірності такого збирання у контексті дотримання прав особи. Так, його метою задекларовано надання методологічної допомоги слідчим, які використовують дані у відкритому доступі, щодо, зокрема, ..(e) Зведення до мінімуму будь-якого ризику заподіяння шкоди особі, організаціям та третім особам; (f) Посилення захисту прав людини, включаючи право на конфіденційність. В пункті п. 62 Протоколу Берклі акцентовано на тому, що слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні поважати права людину, та повинні бути особливо чутливим до права на недоторканість приватного життя, яка часто підіймається в контексті цифрової інформації. Наприклад, порушенням права на приватне життя є одна з небагатьох підстав, за якими судді можуть виключити докази в Міжнародному кримінальному суді. Нарешті, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні знати про загальну заборону несанкціонованого доступу до даних та мереж. Наприклад, це включатиме використання просоченого пароля, знайденого в наборі даних, що порушується для доступу до обмежених матеріалів, а також отримання несанкціонованого доступу до обмеженої інформації за допомогою обману та інших форм соціальної інженерії[3][4].

Тож необхідність не лише доктринального, а й нормативного розв'язання питання щодо належного механізму документування та зберігання цифрової інформації сьогодні є вкрай актуальною особливо в умовах об'єктивної потреби розслідування воєнних злочинів та оперування значним масивом інформації із відкритих джерел.

Щодо оригінальності ЦД у контексті перспективи допустимості в доказуванні

Як вже раніше нами зазначалось, одним з неоднозначним на практиці виявилось питання щодо допустимості використання в доказуванні скопійованої електронної інформації[5]. Адже з огляду на встановлені законом правила доказування, спрямовані на забезпечення правдивості фактичних даних, на яких може ґрунтуватися обвинувачення, процесуальним джерелом доказів, за загальним правилом, має бути його оригінал. Зокрема, оригіналом електронного документа закон визнає його *відображення*, якому надається таке ж значення,

[1] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел' (Судова влада України, 7 червня 2022) <https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/?fbclid=IwAR38uhyaCGNZyG19U7Wjs3l20JCS3uuPfSCwOeUx4BFW9iWWysF6297brsY> (дата звернення: 8.06.2022)

[2] *Примітка.* Крім того, у цьому сенсі варто звернути увагу на рішення ЄСПЛ «Сегерстед-Віберг проти Швеція» («Segerstedt-Wiberg v. Sweden»), в якому дії поліції зі збирання інформації, яка є відкрито доступною для користувачів мережі Інтернет, кваліфіковано як порушення права на недоторканність приватного життя, гарантовану ст. 8 Конвенції про захист прав людини і основоположних свобод. Систематичне збирання інформації розцінюється як втручання в приватне життя у зв'язку з тим, що особа, яка розміщує інформацію, розраховує на зберігання відомостей і відсутність моніторингу за її профілем Case of Segerstedt-Wiberg and Others v. Sweden. 6 June 2006 (Application no. 62332/00) URL: https://www.legal-tools.org/doc/f44dcc/pdf/. (дата звернення: 23.09.2023)

[3] *Примітка.* Соціальна інженерія – це акт обману окремої особи для розкриття конфіденційної інформації шляхом спілкування з нею для завоювання впевненості та довіри. [Національний інститут стандартів і технологій Сполучених Штатів]

[4] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 23.09.2023)

[5] Глинська Н. В. 'Щодо використання цифрової інформації в кримінальному провадженні: окремі аспекти' *Використання цифрової інформації в розслідуванні кримінальних правопорушень*: матеріали міжнар. наук.-практ. круглого столу, (м. Харків, 12 груд. 2022 р.) 18–22 <http://surl.li/glknx> (дата звернення: 23.09.2023)

як документу (ч. 3. ст. 99 КПК). Отже, оригіналом електронного документа закон визнає аналоговий документ, доступний для візуального сприйняття. Водночас принципова відмінність середовищ існування паперових й електронних документів (аналогове та електронне) об'єктивно унеможливлюють застосування ідентичних критеріїв оригінальності таких різновидів документів та стандартів належної процедури їх копіювання.

Тож таке нормативне формулювання на думку сучасних дослідників в контексті електронних документів є таким, що не відповідає природі носію цифрової інформації та не узгоджується із розумінням оригіналу електронного документа, відображеного у Законі України «Про електронні документи та електронний документообіг» (який є спеціальним (профільним), а отже й пріоритетним для врегулювання цифрових відносин в кримінальному провадженні), з положень якого випливає, зокрема, що «*відображення* даних вважається електронною або паперовою копією електронного документа та потребує засвідчення у порядку, встановленому законом (ч. 5, 6 ст. 7). За загальним правилом, оригіналом електронного документа визнається примірник документа з обов'язковими реквізитами, у т. ч. з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги» (ч. 2 ст. 7)[1]. У цьому сенсі на підтримку заслуговує положення Проєкту Закону «Про внесення змін до Кримінального процесуального кодексу України щодо уточнення окремих положень з метою забезпечення захисту прав учасників кримінального провадження» (реєстр № 9211 від 17.04.2023) щодо унормування електронного документа як окремого різновиду документа як джерела доказів (п. 1 ч. 2 ст. 99 КПК) та визначення положення про те, що оригіналом документа є сам документ, а оригіналом електронного документа – його електронний примірник відповідно до Закону України «Про електронні документи та електронний документообіг», або візуальне відображення електронного документа на папері, яке засвідчене в порядку, встановленому законодавством» (ч. 3 ст. 99 КПК). З огляду на позначене таке уточнення положень КПК слугуватиме визначності на практиці стосовно оригінальності електронного документа як різновиду ЦД.

[1] Скрипник А. В. 122.

При цьому як оригінал може бути визнані судом й дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста (ч. 4 ст. 99 КПК). З огляду на специфіку способів формування електронної інформації з такої нормативної регламентації не зрозумілим залишається процедура виготовлення дубліката електронного документа, а відповідно й порядок верифікації тотожності оригіналу та дубліката електронного документа), а також у якій формі має бути скопійована інформація під час проведення процесуальних дій: паперовій чи електронній.

Позначена правова невизначеність обумовила наявність діаметрально протилежних правових позицій ВС. Так, зокрема, у постанові Касаційного кримінального суду ВС (далі – ККС ВС) від 11 березня 2020 р. по справі № 149/745/14 490 суд підтримав визнання недопустимим не лише використання у доказуванні копій відеофонограм, зроблених під час НС(Р)Д, а й протоколів як похідних від них доказів. У той самий час у постанові ККС ВС від 15 січня 2020 р. по справі № 161/5306/16-к визнано можливим подання до суду дублікатів матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі електронних), виготовлених слідчим, прокурором із залученням спеціаліста.

У рішенні від 29 березня 2021 р. по справі № 554/5090/16-к ВС висловив позицію про те, що один і той самий електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами – CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень.

Правова невирішеність позначених та інших питань, пов'язаних із оцінкою оригінальності ЦД як гарантії його достовірності, створює значні

ризики для перспективи використання відповідної інформації в доказуванні. Адже забезпечення оригінальності ЦД як гарантії його достовірності є актуальною щодо всіх інших його різновидів (електронний документ – це лише один вид джерела цифрової інформації). Тож у ракурсі загальної правової вимоги подання будь-якого доказу в оригіналі (за виключенням чітко встановлених законом випадків, як то копія інформація, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал) належна правова процедура може бути не дотримана хоча б з огляду на специфіку цифрової інформації, яка за способом вираження поділяється на два види: 1) інформація, представлена у двійковій формі; 2) інформація, інтерпретована за допомогою програмного забезпечення у текст, звук, зображення тощо. І лише другий різновид інформації може бути безпосередньо досліджений в суді (наприклад у спосіб відкриття електронних пристроїв, на яких зберігаються файли-носії цифрової інформації, дослідження інтернет-сторінки тощо).

Утім й тут є свої застереження, що впливають на достовірність цифрової інформації, що досліджується. Адже «специфічна природа інформації в електронному вигляді полягає в тому, що вона є доступною для сприйняття людиною не безпосередньо, а тільки після обробки її спеціальними програмними засобами (наприклад текстовим редактором «Word»), які, своєю чергою, функціонують під управлінням операційної системи на певному комп'ютерному пристрої. Тобто перегляд різними програмними засобами фізично однакової інформації у вигляді бітів (мінімальна одиниця кількості інформації) на жорсткому диску призведе на екрані монітора чи роздруківці принтера до різного виду фактичних даних»[1].

Щодо специфіки дослідження ЦД та оцінки з точки зору його достовірності.

Електронні докази з огляду на їх мінливість та мобільність легше змінити чи підробити без залишення слідів на носієві, ніж традиційні форми доказів. Адже зворотний бік цифрового прогресу суспільства полягає у можливості фальсифікації будь-якої електронної інформації – від відео- та телефонних розмов до присутності в режимі реального часу. Так, зламати паролі від гаджетів – це не рівень складності навіть для студентів 2-го курсу технічного ВНЗ. При цьому довести, що акаунт зламали, дуже складно. Якщо хакер має достатньо знань, то сліди втручань у роботу пристроїв будуть знищені. З огляду на це, наявність будь-яких сумнівів щодо автентичності цифрового доказу вимагає фахової процесуальної перевірки.

Тож питання забезпечення й перевірки їх достовірності, а значить й допустимості є вкрай актуальними для кримінального судочинства.

Пізнання в кримінальному процесі, що здійснюється у формі доказування, спрямоване на одержання достовірного знання про обставини кримінального провадження, тобто одержання доказів не лише належних та допустимих, але й достовірних. Про це прямо зазначено у ч. 1 ст. 94 КПК, де закріплено положення про те, що слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, *достовірності,* а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення. Традиційно в науці кримінального процесу під достовірністю доказу розуміють «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»[2], «правильністю відображення в доказах фактів об'єктивної дійсності, яка є предметом досудового розслідування або судового розгляду. Іншими словами – це відповідність доказу дійсності[3]. Недостовірних доказів у кримінальному процесі не існує, оскільки

[1] Гуцалюк М. В., Антонюк П. Є. 'Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні' 2022 2(41) ІНФОРМАЦІЯ І ПРАВО 118.

[2] Ковальчук С. О. 'Вчення про речові докази у кримінальному про-цесі: теоретико-правові та практичні основи'(дис. д-ра юрид. наук, Національний університет «Одеська юридичнаакадемія», 2018) 133

[3] Тацій В. Я., Грошевий Ю. М.,. Капліна О. В,. Шило О. Г (ред) *Докази і доказування. Кримінальний процес: підручник*. (Право, 2013) 190

недостовірні фактичні дані не можуть становити зміст доказу, утворювати доказ. Термін «достовірний» тлумачиться в українській мові як такий, що не викликає сумніву, цілком вірний, точний та є синонімом прикметника «вірогідний» – який не викликає сумніву; достовірний. Достовірність доказу в кримінальному провадженні є його ознакою, яка характеризується повною відповідністю одержаних відомостей про факти реальним подіям, що відбувалися[1]. На останній аспект слід особливо звернути увагу.

Існування *частково допустимого доказу* апріорі є неприпустимим з огляду на цілісність доказу як «кванту» процесуального доказування. Закладене в ст. 84 КПК розуміння доказу як фактичних даних, що можуть існувати лише за умови їх закріплення у вичерпному встановленому законом переліку джерел (їх носіїв), відповідає доктринальній «інформаційній» концепції доказу, що ґрунтується на єдності доказу та джерела (відомостей та їх носія).

Такий висновок має безпосереднє практичне значення. Адже на практиці відомі випадки визнання електронного доказу частково достовірним, з огляду, наприклад, лише часткового збігу електронної інформації про хід проведення НС(Р)Д із її фіксацією у протоколі відповідної процесуальної дії. Втім штучне виділення певних частин електронного доказу, які містяться у його джерелі (наприклад, сторінки протоколу) як окремих засобів доказування, є таким, що суперечить встановленій законом вимоги *цілісності доказу* як об'єктивної єдності всього його змісту та форми.

Доказ або відтворює реальну картину, або ні. Факти й обставини у кримінальному провадженні повинні бути встановлені з повною достовірністю, оскільки тільки з достовірних фактів можуть бути зроблені висновки про обґрунтованість обвинувачення. Тож лише цілісне сприйняття доказу в об'єктивній єдності його змісту та форми може надати достовірну «картину» обставин, що підлягають дослідженню. На підтвердження цього також можна зазначити, що один і той самий доказ може бути та обвинувальним, і виправдувальним за своїм характером, втім, це не дає право його розділяти на частини – умовно обвинувальну та виправдувальну.

Як відомо, питання достовірності доказової інформації виникають протягом всього кримінального провадження. Так, розпочинаючи з етапу збирання цифрової інформації до завершення досудового розслідування з огляду на вимогу законності та публічності слідчій, дізнавач, прокурор опікуються про якість перспективних ЦД, перевіряючи їх цілісність у спосіб проведення додаткових перевірочних процесуальних дій (за потреби призначають експертизу), зіставлення цифрової інформації з іншими фактичними даним та ін. Утім *кульмінаційне* значення правильної оцінки достовірності ЦД набуває під час судового розгляду, коли вирішується питання, чи може такий доказ бути покладений с основу проміжного чи підсумкового судового рішення.

Загалом ЦД в залежності від характеру даних (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо, вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та ін.) досліджуються в порядку, передбаченому для дослідження документів (ст. 358 КПК) чи в порядку дослідження відео-, звукозапису (ст. 359 КПК). Спеціального нормативного алгоритму перевірки достовірності цифрової інформації та її носія закон не містить.

І хоча, як оптимістично зауважує Г. К. Авдєєва «…судові рішення останніх 2–3 років відрізняються від попередніх більш детальним розглядом і поясненням технічних характеристик цифрових доказів, що надає більше шансів для визнання допустимим доказом копії інформації у цифровій формі…судді детально оцінюють достовірність висновків експерта та досліджують цифрові докази безпосередньо (в т.ч. – інформацію з мобільних телефонів)»[2], все ж таки сучасна «цифрова» судова практика характеризується неоднорідністю щодо розв'язання ключових питань оцінки допустимості електронної інформації у кримінальному провадженні, зокрема, щодо механізму підтвердження скриншотів, усунення сумнівів справжності доказу, оцінки ризиків ідентифікації особи учасника дистанційного провадження. Залишається проблемним питання ідентифікації особи, яка створила та поширила той чи інший електронний

[1] Гутник А. В., Хитра А. Я. 90

[2] Авдєєва Г. 'Цифрові докази у кримінальному провадженні' *OMUL, CRIMINOLOGIA, ȘTIINȚA* Conferința științifică internațională ediția a II-a Chișinău, 24 martie 2023 <https://ibn.idsi.md/sites/default/files/imag_file/370-374_5.pdf> (дата звернення: 23.09.2023)

документ, що може слугувати електронним доказом»[1].

До проблемних питань, зумовлених оцінюванням процесуальних джерел в електронній формі, які виникають під час розгляду кримінальних проваджень, суддя ВС С. Кравченко також відносить правову оцінку тверджень щодо цілісності електронного доказу, що міститься на диску або флешкарті, відмінностях між одними та іншими файлами, оцінку скриншоту. При цьому суддя наголошує на необхідності унормування поняття та видів електронних доказів, доповнивши перелік процесуальних джерел доказів, і розмежувати поняття електронного документа як офіційного документа та інших документів, які подаються в електронній формі.

Водночас позначена нормативна неврегульованість не знімає з суду обов'язків врахування специфіки дослідження цифрової інформації з метою забезпечення використання на підтвердження своїх рішень лише якісних доказів. В цьому сенсі судді ВС, наголошуючи на актуальності унормування зазначених питань в КПК, обґрунтовано акцентують на затребуваність навіть у межах чинної правової регламентації відповідального та спеціалізованого підходу суддів під час оцінки допустимості використання цифрової інформації у кримінальному провадженні. Так, зокрема, суддя ККС ВС Надія Стефанів звернула увагу на міжнародний документ «*Керівні принципи щодо електронних доказів*», що розроблений Радою Європи у 2019 році та стосується одержання й обробки електронних доказів у цивільній та адміністративній юрисдикціях. При цьому спікерка наголосила на можливості та доцільності застосування цих керівних принципів суддями всіх юрисдикцій, зокрема кримінальної, задля того, щоб будь-які докази, прийняті до судового провадження, були належними та допустимими. «Судді відповідають за підвищення власних професійних знань стосовно використання електронних доказів. Суддя сам має дбати про те, щоб бути в курсі всіх останніх новин щодо документів і стандартів та застосовувати їх відповідно до чинного процесуального законодавства», – акцентувала суддя. За словами Надії Стефанів, судді виконують ключову роль під час оцінювання електронних доказів, *саме від їхньої компетенції та правильного рішення залежить, чи буде окремий електронний доказ відігравати провідну роль у вирішенні конкретної справи.* Вона переконана, що суддя має розуміти, що таке диск, відеофайл, аудіозапис, що таке цифровий документ. Уся відповідна термінологія має бути розроблена та стати предметом підвищення кваліфікації кожного судді[2]. Інакше кажучи, в сучасних умовах глобальної діджиталізації суспільства правник має володіти хоча б мінімальним рівнем цифрових знань.

До речі пункт 19 зазначених Керівних принципів щодо електронних доказів орієнтує суддів при оцінці достовірності ЦД враховувати *всі належні фактори щодо походження та справжності електронних доказів*. Специфічність цифрової інформації обумовлює відповідну специфічність й порядку формування ЦД, особливості його перевірки та оцінки. В контексті перевірки й оцінки такого доказу з точку зору його цілісності (аутентичності, справжності) потрібними є додаткові критерії, такі, зокрема, як аутентифікованість (властивість відомостей в електронній формі, що дозволяє визначити їхню справжність, що засвідчується цілісністю та надійністю електронної системи, у якій створений та зберігався документ), ідентифікованість (властивість відомостей в електронній формі, що дозволяє визначити суб'єкта створення або модифікації (наприклад, IP-, або MAC-адреса користувача), верифікованість (властивість відомостей в електронній формі, що дозволяє визначити дату, місце. Спосіб їхнього створення, модифікації), незмінність (збереження цілісності відомостей в електронній формі) і відтворюваність (властивість відомостей в електронній формі, що дозволяє продемонструвати інформацію у доступний для сприйняття спосіб) та ін. [3]

Звичайно здебільшого оцінка цифрового доказу з огляду позначених та інших критеріїв є завданням сучасної цифрової криміналістикиз арсеналом дотичних методик. Втім певні ознаки електронних документів, що дозволяють оцінити їх справжність, набувають суто процесуального значення як такі, що мають бути взяти до уваги

[1] Колотило О. 'Правове регулювання електронного кримінального провадження' (2020. 27 квітня) Юридична газета <https://yur-gazeta.com/ publications/ practice/kriminalne-pravo-ta-proces/pravove-regulyuvannya-elektronnogokriminalnogo-provadzhennya.html> (дата звернення: 23.09.2023)

[2] 'Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду'(Судова влада України, 28 жовтня 2021) <https://court.gov.ua/press/news/1202385/> (дата звернення: 23.09.2023)

[3] Скрипник А. С.100–101

безпосередньо судом у перебігу здійснюваної оцінки доказу.

У цьому сенсі зазначимо, що до основних особливостей електронного документа в сучасній процесуальній літературі відносять обов'язкову складову будь-якого електронного документа – метадані[1]. «Метадані» це термін, який походить від англійського слова «metadata» (*meta, грец. – «після», data, англ. – «інформація»,»відомості», «дані»)* означає дослівно «дані про дані». 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*. Даний перелік є необмеженим та залежить від типу файлу, програми-створювача документа тощо.

Тож метадані електронного документа (структуровані закодовані дані, які характеризують електронний документ) мають важливе значення під час кримінального провадження, зокрема, у контексті перевірки електронного доказу на його повноту і цілісність, *з однієї сторони, та допустимість, належність – з іншої.*

Викладеним ми проілюстрували лише один вектор дослідження цифрового доказу з точки зору його правдивості. Втім якщо слідкувати запропонованимнауковцями алгоритму встановлення достовірності будь-якого доказу (визначення достовірності (1) джерела, (2) методу отримання фактичних даних; (3) достовірності з урахуванням інших матеріалів кримінального провадження[2]) встановлення достовірності джерела цифрового доказу може полягати у перевірці інших питань, як то технічної справності носія цифрової інформації, встановленні інформації про власника вебсайт, облікового запису у соціальній мережі, встановлення місцезнаходження технічного пристрою у період, який становить інтерес тощо[3].

Звичайно це неповний перелік питань, перевірка яких може постати у конкретній ситуації встановлення достовірності цифрового доказу, а вибірковість обумовлена викликами сучасної правозастосовної практики.

Викладене також свідчить про нагальну необхідність проведення наукової розвідки щодо вимог (стандартів) до механізму збирання, зберігання та оцінки цифрових доказів з урахуванням їх специфіки, які мають процесуальне значення та підлягають унормуванню.

Щодо основних ризиків оперування цифровими доказами під час кримінального провадження та стратегії керування ними на законодавчому рівні.

Якщо систематизувати вищенаведені та інші практичні виклики (ризики), що постають перед кримінальним провадженням у зв'язку з об'єктивною необхідністю оперування в доказуванні цифровою інформацією, умовно можна виділити наступні їх блоки.

А) Ризики недостовірності цифрової інформації;

Б) Ризики неправильної оцінки цифрової інформації;

В) Ризики втрати, пошкодження ЦД;

Г) Ризики перспективи недопустимості ЦД;

Д) Ризики непропорційного втручання в права та свободи людини.

І хоча серед чинників, що сприяють вказаним негативним явищам є також обставини об'єктивного та суб'єктивного характеру, що знаходяться поза межами кримінальних процесуальних відносин (як то загальний державний рівень інформаційної безпеки, рівень матеріально-технічного оснащення органів кримінальної юстиції, цифрова компетентність слідчих, дізнавачів, прокурорів та суддів тощо), здебільшого потенціал їх мінімізації (керування ризиками) знаходиться в необхідних законодавчих рішеннях стосовно «цифрової» модернізації кримінального процесуального законодавства. Як влучно зазначає Д. О. Московчук «… юридичні, а не фактичні питання можуть збільшити прірву між електронними та традиційними документами та вимагати доповнення законодавства, необхідного для того, щоб електронні документи також були «документами

[1] Гутник А. В., Хитра А. Я. 204

[2] Благута Р. І., Гуцуляк Ю. В., Дуфенюк О. М. та ін. *Докази та доказування у кримінальному провадженні: навч. посібник* (ЛьвДУВС, 2018) 59

[3] Гутник А. В., Хитра А. Я .93

в законі»[1]. Видається це судження є цілком релевантним й стосовноінших форм цифрових доказів як «доказів в законі».

Основними аспектами нормативної стратегії інституціоналізації цифрових доказів в кримінальному процесуальному законодавстві України мають бути наступні елементи.

1. Визнання ЦД окремим джерелом доказів в кримінальному провадженні.

2. Модернізація кримінального процесуального механізму збирання електронних доказів.

3. Запровадження спеціальних стандартів зберігання електронної інформації.

4. Унормування спеціальних критеріїв оцінки ЦД (потребує проведення наукової розвідки щодо критеріїв оцінки цифрових доказів з точки зору їх допустимості, які мають процесуальне значення та підлягають унормуванню).

5. Встановлення імперативної вимоги участі фахівця як під час збирання цифрової інформації, так і під час її дослідження в суді.

Зазначені елементи стратегій унормування інституту ЦД потребують свого окремого дослідження. На цих сторінках лише вибірково торкнемось їх окремих аспектів.

Щодо окремих аспектів унормування цифрового доказу як окремого джерела.

Вищезазначені специфічні риси цифрової інформації цілком логічно обумовлюють специфіку самих носіїв такої інформації, до яких, як справедливо наполягають сучасні дослідники слід відносити не фізичний носій інформації (моноблоки, мобільні пристрої (мобільні телефони, планшети, комп'ютери), цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, звуко- та відеозаписи тощо), а окремий файл, який міститься на фізичному носії чи в електронній мережі та має доказове значення[2]. Як влучно зазначає А. В. Коваленко, потребує перегляду в електронних реаліях закріплений у ч. 1 ст. 99 КПК України принцип прив'язки документа до матеріального носія інформації. За такого підходу, документом у процесуальному значенні має вважатися не окремий електронний файл, що містить відомості, які мають значення для кримінального провадження, а фізичний носій електронної інформації, що містить згаданий файл. До того ж сучасні фізичні носії електронної інформації здатні містити мільйони файлів різного формату та розміру одночасно, лише одиниці з яких можуть стосуватися певного кримінального провадження[3].

Таке розуміння джерел електронного доказу є вкрай важливим з точки зору упередження одного з ключових ризиків, що супроводжує процесуальну діяльність зі збирання електронної інформації – непропорційне втручання у права та свободи людини в перебігу кримінальної процесуальної діяльності. Зокрема, нормативним стандартом у площині предметності судового контролю має бути уможливлення надання дозволу на відшукання чи вилучення не певного накопичувача цифрових даних (флеш накопичувача, карти пам'яті тощо), а саме конкретних файлів, що містять потрібну для провадження інформацію.

Щодо окремих аспектів модернізації кримінального процесуального механізму збирання електронних доказів.

Як показує аналіз практики непоодинокими є випадки висунення стороною захисту розумних сумнівів щодо достовірності методу отримання та копіювання цифрової інформації органом досудового розслідування, можливих маніпуляцій сторони обвинувачення із джерелом цифрової інформації з огляду на невиправдано тривалий проміжок часу з моменту його фактичного вилучення та процедури копіювання інформації, зазначення стороною обвинувачення правдивих відомостей у протоколі відповідної процесуальної дії (СРД, НС(Р)Д). Як правило збирання цифрової інформації відбувається під час проведення обшуку й огляду або ж шляхом її копіювання з інформаційного простору або цифрового носія інформації, або ж шляхом вилучення носія цифрової інформації (електронного гаджета) та подальшого копіювання. Втім, як влучно зазначає О. П. Метелев на відміну від процедур вилучення речей і документів, вищеозначена процедура вилучення цифрових носіїв інформації під час обшуку й огляду законодавцем не формалізована та не визначена, що може призвести до зловживань, зокрема з боку правоохоронців, які в разі отримання доступу до того чи іншого цифрового носія інформації стають

[1] Московчук Д. О. 49–50

[2] Сприпник А. В. 110–111; 121; Коваленко А. В. 'Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання' (2018) 4. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка 239; Алєксєєва-Процюк Д. О. 'Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування' (2018) 2 Науковий вісник публічного та приватного права 247–253

[3] Коваленко А. В. 239

власниками особистої значущої інформації (тексти повідомлень у соціальних мережах, паролі систем електронних платежів тощо)[1].

На упередження таких випадків видається слушною ідея унормування як окремої слідчої дії, що спрямована на збирання цифрових доказів у справі «електронне копіювання» з опрацюванням і визначенням особливих процесуальних правил і стандартів, зміст яких урахував би сучасні зміни, які відбулися в суспільстві, а також в інформаційному просторі[2].

У сенсі стандартів процедури копіювання електронної інформації фахівці доречно звертають увагу на те, що сам по собі факт формального виконання вимоги КПК України щодо залучення спеціаліста для проведення відповідної процедури копіювання ще не гарантує тотожності копії інформації оригіналу, а значить й справжності сформованого у такий спосіб електронного доказу. Адже «…залучений стороною обвинувачення спеціаліст має володіти необхідними знаннями та навичками у сфері інформаційних технологій та бути здатним правильно реалізувати процес копіювання, що має включати верифікацію (перевірку) цілісності та справжності інформації з наданням відповідних гарантій. Варто звернути увагу на окремі випадки формального виконання слідчими вимог ч. 4 ст. 99 КПК України щодо залучення спеціаліста при копіюванні інформації, що має електронну форму, з одночасним недотриманням технічних аспектів щодо гарантування цілісності та справжності інформації, що може дискредитувати виготовлену копію. Таким чином, очевидною стає необхідність дотримання технічного аспекту процесу копіювання інформації, значення якого важко переоцінити[3]. З огляду на необхідність системних змін в підході до копії електронної інформації як доказу в кримінальному провадженні, що передбачають гарантування цілісності та справжності інформації не «церемоніальним» залученням спеціаліста, а наданням гарантій незмінності первинної інформації з урахуванням вимог ДСТУ ISO/ IEC 27037:2017. Тож доцільним видається доповнення ч. 4 ст. 99 КПК України нормою щодо обов'язку спеціаліста підтвердити цілісність та справжність створеної копії інформації[4].

Видається поміж унормування відповідних процедурних вимог до коректності фіксації цифрової інформації, одним зі стандартів проведення копіювання цифрових даних має бути темпоральний – мінімальний проміжок часу з моменту вилучення носія цифрової інформації до її копіювання та фіксації як запобіжник можливим маніпуляціям зі змістом такої інформації. Упередженню можливих спорів щодо цілісності цифрових доказів також слугуватиме вимога якомога докладного протоколювання процесів аутентифікації (встановлення справжності) та всіх інших дій з цифровими доказами (вилучення з детальним описом електронного пристрою, вказівкою його власника та осіб, які мали до нього доступ, способів і засобів вилучення інформації, копіювання на зовнішній носій, дослідження з описом методів і засобів тощо), на що влучно наголошують науковці Національного інституту юстиції США[5].

Щодо окремих аспектів запровадження спеціальних стандартів зберігання електронної інформації

Задля дотримання принципу безпосередності дослідження доказу в суді *стратегічним вектором* нормативної інституалізації цифрових доказів є запровадження спеціальних стандартів зберігання електронної інформації.

Вказаний аспект відображений у листі-орієнтуванні Офісу Генерального прокурора стосовно збереження цифрової інформації з відкритих джерел від 28 серпня 2021 року. В цьому документі наголошено, зокрема про те, що з метою забезпечення доступності інформації у відкритих джерелах слід здійснювати її цифрове зберігання – архівацію, яке дає змогу захистити та зберегти інформацію з плином часу, включаючи її справжність, доступність, ідентичність, постійність, рендеринг (візуалізацію) та зрозумілість. Саме ці індикатори цифрової інформації, як зазначено у Протоколі

[1] Метелев О. П. 'Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження' (2020) Науковий вісник Ужгородського національного університету <https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/02/41.pdf> (дата звернення: 23.09.2023)

[2] –

[3] Каланча І. Г. Гаркуша А. М. 'Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти' (2021) 8 Юридичний науковий електронний журнал <http://www.lsej.org.ua/8_2021/79.pdf> (дата звернення: 23.09.2023)

[4] –

[5] Sean E. Goodison, Robert C. Davis and Brian A. Jackson 'Digital Evidence and the U. S.' CriminalJustice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Research report (Rand Corporation). RAND Corporation, 2015 32 <https://www.ojp.-gov/pdffiles1/nij/grants/248770.pdf.> 13 (дата звернення: 23.09.2023)

Берклі, підлягають захисту та збереженню. При цьому під час копіювання електронної інформації за обов'язкове визнано залучення спеціаліста, який має вищу освіту у сфері інформаційних систем та технологій, для визнання надалі судом інформації, що міститься в електронному документі, виготовленому в такий спосіб, як оригіналу.

Протокол Берклі пропонує зберігати цифровий матеріал таким чином, щоб зберегти його автентичність, і документувати ланцюг забезпечення збереження, що збільшить ймовірність того, що він може бути прийнятий як доказ у суді.

Що ж до законодавства, то чинний КПК не деталізує питання зберігання цифрових доказів, як і решту інших «цифрових» питань доказування. Яскравим прикладом є стаття 265 КПК (Фіксація та збереження інформації, отриманої з електронних комунікаційних мереж за допомогою технічних засобів та в результаті зняття відомостей з електронних інформаційних систем), у змісті якої відображене лише загальне положення про те, що «прокурор вживає заходів для збереження знятої інформації».

Не містить якихось спеціальних вимог до зберігання цифрової інформації і єдиний на сьогодні у царині «спроб» унормування цифрових доказів в кримінальному провадженні проєкт Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів (№4004 від 01.09.2020. У статті 100–2 зазначеного Проєкту розробники зазначили про те, що «оригінали або копії електронних доказів зберігаються у суді в матеріалах кримінального провадження» (ч. 1), а «.сторона кримінального провадження, якій наданий електронний доказ, зобов'язана зберігати його у стані, придатному для використання у кримінальному провадженні» (ч. 2.) При цьому «електронні докази, які отримані або вилучені слідчим, прокурором, оглядаються, фіксуються за допомогою фотографування або відеозапису та докладно описуються в протоколі огляду із залученням спеціаліста. Зберігання електронних доказів стороною обвинувачення здійснюється в порядку, визначеному Кабінетом Міністрів України (ч. 2).

Утім на сьогодні такий поряд є загальним та з огляду на позначену специфіку цифрової інформації не є корисним для убезпечення надійності збереження та цілісності такої інформації упродовж тривалого часу.

Адже цифрова інформація є надто вразливою через те, що може бути легко змінена чи знищена. Саме ця його риса, на думку науковців, зумовлює «необхідність створення спеціальних правил фіксації електронної інформації, способів збереження та приєднання їх до матеріалів справи. Зокрема, на рівні з традиційними правилами поводження із документами необхідно враховувати технічні особливості збирання, зберігання та використання інформації»[1].

При цьому ризики надійного зберігання електронних доказів здебільшого зводяться як до факторів технічного характеру (як то енергозалежність пристроїв (у разі розрядки пристрою або недостатності пам'яті система накладає (записує) нову інформацію замість попередньої, а це значить, що й докази можуть бути знищені); комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів (високий рівень вологості, висока температура) та електромагнітних хвиль тощо)), так і до можливих протиправних дій, спрямованих за знищення чи спотворення цифрової інформації. Тож гарантії надійності збереження електронної інформації полягають не лише у площині високої якості технологій, а й у задані нормативного алгоритму такого зберігання, зокрема, архівації інформації, фіксації ланцюга збереження доказу у відповідному протоколі (фіксування покрокового шляху огляду, збереження та архівації цифрової інформації з мережі Інтернет тощо).

Цінні дороговкази у контексті зберігання електронних доказів містяться в Керівних принципах Комітету міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях, прийнятих *30 січня 2019 на 1335-му засіданні заступників Міністрів)*. Видається при унормуванні інституту електронних доказів у кримінальному провадженні мають бути сприйняті такі положення Керівних принципів: – електронні докази повинні зберігатися зі стандартизованими метаданими, аби контекст їх створення був зрозумілим (п. 26); зрозумілість і доступність збережених електронних доказів повинні гарантуватися з плином часу, враховуючи еволюції інформацій-

[1] Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень (2017) 4 (58) Держава та регіони 82

них технологій (п. 27); архівація електронних доказів відповідно до національного законодавства; електронні архіви повинні відповідати всім вимогам безпеки та гарантувати цілісність, автентичність, конфіденційність і якість даних, а також повагу до приватності (п. 28); архівування електронних доказів має здійснюватися кваліфікованими фахівцями (п. 29); дані мають переписуватися на нові носії для зберігання, коли це необхідно для збереження доступності електронних доказів (п. 30).

Щодо окремих аспектів залучення фахівця під час дослідження цифрового доказу в суді

З огляду на викладені положення щодо специфіки встановлення цілісності цифрових доказів у суді та відповідного спектру питань технічного характеру, необхідність з'ясування яких для цього може постати перед судом у конкретній правовій ситуації, об'єктивною є потреба залучення особи зі спеціальними технічними знаннями та навичками. Як відомо, в кримінальній процедурі залучення спеціальних знань є допустимими у двох формах: 1) залучення спеціаліста; 2) призначення експертизи. Звичайно проведення судової експертизи є найбільш кваліфікованою та ґрунтовною формою використання спеціальних знань обізнаної особи у кримінальному провадженні. Втім проведення експертизи є затратною за часовими та грошовими ресурсами процесуальною дією, тому більш оперативною та компромісною формою «спеціальної допомоги» у кримінальній процедурі є залучення спеціаліста (ст. 71, 360 КПК).

І хоча чинний КПК імперативно це не «нав'язує» спеціальну допомогу суду у ситуації, коли виявились розумні сумніви щодо достовірності цифрового доказу, видається таке залучення є розумним та вкрай необхідним. Так, для перевірки цілісності файлу, тобто того, чи був він змінений у цифровому вигляді, маніпульований чи модифікований, доцільно піддати його цифровій судовій експертизі, яку іноді називають цифровим слідчим аналізом[1].

Нагальність цифрової допомоги особи, обізнаної з цифрових питань, під час дослідження автентичності електронного доказу в суді продиктована, з одного боку, вище наведеною специфікою цифрової інформації та, з іншого, об'єктивно недостатнім рівнем цифрової компетентності правника. Адже для будь-якого неупередженого стороннього спостерігача очевидно, що за розумним припущенням прокурор, захисник чи суддя як правники за освітою об'єктивно не можуть надати достовірні, повні, вичерпні та зрозумілі відповіді з технічних питань, зокрема, визначити метадані електронного документа, оцінити дотримання процедури копіювання електронної інформації тощо. З іншого боку, такою, що відповідає сучасній правовій реальності інформаційного суспільства, є презумпція обізнаності суду щодо необхідності врахування під час дослідження електронних доказів та визначення їх достовірності всіх належних факторів щодо їх походження та справжності. Зазначене обумовлює визнання за правило використання при такому дослідженню спеціальних знань. Як зазначав у 2013 році Д. Цехан, прогресивними у контексті використання «цифрових доказів» у кримінальному провадженні є положення ст. 360 КПК України, якою дозволяються суду скористуватись під час дослідження доказів усними консультаціями чи письмовими роз'ясненнями спеціаліста, наданими на підставі його спеціальних знань, оскільки під час дослідження судом «цифрових доказів» існує необхідність пояснення особливостей алгоритму програмування чи обробки даних, а також специфіки комп'ютерної системи»[2]. Втім з урахуванням, з одного боку, стрімкого зростання спектра цифрової інформації, що потрапляє в царину кримінального процесуального доказування, та відповідно рівня складності питань її достовірності, та з іншого боку – явно недостатнього рівня сучасної цифрової компетентності правників, питання щодо участі спеціаліста під час дослідження цифрового доказу в суді стає не рекомендацією, а правилом.

У контексті мінімального кваліфікаційного рівня «цифрового» фахівця у Листі-орієнтуванні Офісу Генерального прокурора стосовно збереження цифрової інформації з відкритих джерел від 28 серпня 2021 року наголошено на обов'язкове залучення під час здійснення цифрового зберігання інформації з відкритих джерелах спеціаліста, який має *вищу освіту у сфері інформаційних систем та технологій*, для визнання надалі судом інформації, що міститься в електронному докумен-

[1] Матвеєв В. 'Проблеми та виклики, пов'язані зі збором електронних доказів' (JUSTTALK) <https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv> (дата звернення: 23.09.2023)

[2] Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування (2013) 5 Науковий вісник Міжнародного гуманітарного університету. Юриспруденція 261

ті, виготовленому в такий спосіб, як оригіналу. При цьому, як дотично зазначають в сучасній криміналістичній літературі, стосовно *кваліфікаційних критеріїв цифрової обізнаності особи*, не існує такого поняття, як універсальний комп'ютерний експерт. Як комп'ютерного експерта можливо залучати осіб з наступними спеціальностями: а) комп'ютерні науки та інформаційні технології; б) інженер з технічного захисту інформації; в) комп'ютерна інженерія; г) системна інженерія; д) програмна інженерія; е) мережеві технології та системне адміністрування; ж) аналітика комп'ютерних систем. Природно, що зростання рівня й інтенсивності використання спеціальних знань призводить і до підвищення вимог до кваліфікації спеціаліста[1].

Тож з викладеного випливає принаймні два висновки: участь спеціаліста під час дослідження цифрового доказу в суді в разі наявності розумних сумнівів щодо його достовірності має бути обов'язковою; питання щодо компетентності та неупередженості залученого до дослідження цифрового доказу в суді має бути узгоджено сторонами.

Висновки. Підсумовуючи це дослідження зазначимо про те що, при унормуванні в КПК тих чи інших *стратегічних* аспектів інституту ЦД *тактично* важливим є дотримання балансу між, з одного боку – функціональною необхідністю закріплення специфіки механізму збирання, фіксації, зберігання та оцінки ЦД з огляду на їх природу, з іншого боку – дотримання стандарту лаконічності закону та відсутності зайвої деталізації («не перевантаження закону спеціальною термінологією»). Доречним в цьому сенсі є використання бланкетних норм з відсиланням до спеціальних законів, що визначають та деталізують цифрові технології (за їх наявності), а також унормування окремих аспектів на рівні підзаконних нормативно-правових актів (як то покрокова алгоритмізації дій щодо фіксації та збереження цифрової інформації, встановлення кваліфікаційних вимог до комп'ютерних фахівців тощо).

[1] Климчук М. П., Коміссарчук Ю. А., Марко С. І., Стецик Б. В. *Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб.* (Львівський державний університет внутрішніх справ, 2022) 26

REFERENCES

List of legal documents

Legislation

1. DSTU ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT). Informatsiini tekhnolohii. Metody zakhystu. Nastanovy dlia identyfikatsii, zbyrannia, zdobuttia ta zberezhennia tsyfrovykh dokaziv. Chynnyi vid 01.01.2019 r., UkrNDNTs, Kyiv, 2018. 31 s. (in Ukrainian)
2. Protokol Berkli z vedennia rozsliduvannia z vykorystanniam vidkrytykh tsyfrovykh danykh URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (in Ukrainian)
3. Berkeley Protocol on Digital Open Source Investigations. United Nations Human Right. New York and Geneva, 2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2022–04/OHCHR_BerkeleyProtocol.pdf (in English)

Reports

4. Zvit shchodo Ukrainy, pidhotovlenyi Ofisom Prohramy z kiberzlochynnosti na osnovi ekspertnoi pidtrymky nezalezhnykh ekspertiv Rady Yevropy pana Markko Kunnapu i pana Marka Yuricha, pro chynne zakonodavstvo i proekty zakoniv, shcho dopovniuiut rizni pytannia, poviazani z kiberzlochynnistiu ta elektronnymy dokazamy, ta vnosiat zminy do nykh (2016/DGI/JP/3608 3 lystopada 2016 roku). URL: https://rm.coe.int/16806f3743. (in Ukrainian)
5. Ministerstvo yustytsii Ukrainy. Dyrektorat pravosuddia ta kryminalnoi yustytsii. Monitorynhovyi zvit za 2021 rik / vidpov. red. k.iu.n. Oliinyk O. M. URL: https://minjust.gov.ua/m/monitoring-vprovadjennya-ta-analiz-efektivnosti-npa. 662 s. (in Ukrainian)

Bibliography

Authored books

1. Blahuta R. I., Hutsuliak Yu. V., Dufeniuk O. M. ta in. *Dokazy ta dokazuvannia u kryminalnomu provadzhenni: navch. posibnyk* [Evidence and proof in criminal proceedings: a study guide] (LvDUVS, 2018) 272 (in Ukrainian)
2. Hutnyk A. V., Khytra A. Ia. *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni: kolektyvna monohrafiia* [Criminal procedural and forensic basics of using electronic documents in evidence: a collective monograph] (LvDUVS, 2022) 204 (in Ukrainian)

3. Klymchuk M. P., Komissarchuk Yu. A., Marko S. I., Stetsyk B. V. *Sudova kompiuterno-tekhnichna ekspertyza u kryminalnomu provadzhenni : navch. posib*. [Forensic computer-technical expertise in criminal proceedings: training. manual] (Lvivskyi derzhavnyi universytet vnutrishnikh sprav, 2022) 112 (in Ukrainian)
4. Skrypnyk A. V. *Vykorystannia tsyfrovoi informatsii v kryminalnomu protsesualnomu dokazuvanni : monohrafiia* [Use of digital information in criminal procedural evidence: monograph] (Pravo, 2022) 408 (in Ukrainian)

Edited books

5. Tatsii V. Ia., Hroshevyi Yu. M.,. Kaplina O. V,. Shylo O. H (red) *Dokazy i dokazuvannia. Kryminalnyi protses: pidruchnyk* [Evidence and proving. Criminal procedure: a textbook] (Pravo, 2013) 824 (in Ukrainian)

Part of the books

6. Biasiotti MA, Cannataci JA, Bonnici JPM, Turchi F 'Introduction: opportunities and challenges for electronic evidence' *In: Handling and exchanging electronic evidence across Europe*. (Springer, Cham, Switzerland, 2018) pp 3–12. (in English)
7. Sean E. Goodison, Robert C. Davis and Brian A. Jackson 'Digital Evidence and the U. S.' CriminalJustice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Research report (Rand Corporation). RAND Corporation, 2015 32 <https://www.ojp.-gov/pdffiles1/nij/grants/248770.pdf.> 13 (in English)

Journal articles

8. Alieksieieva-Protsiuk D. O. 'Elektronni dokazy v kryminalnomu sudochynstvi: poniattia, oznaky ta problemni aspekty zastosuvannia' [Electronic evidence in criminal proceedings: current state and prospects of use] (2018) 2 Naukovyy visnyk publichnoho ta pryvatnoho prava 247–253 (in Ukrainian)
9. Hutsaliuk M. V., Antoniuk P. Ie. 'Protsesualna spromozhnist vykorystannia elektronnoi (tsyfrovoi) informatsii yak dokazu v kryminalnomu provadzhenni' [Procedural ability to use electronic (digital) information as evidence in criminal proceedings] 2022 2(41) INFORMATsIIa I PRAVO 116–122 (in Ukrainian)
10. Kalancha I. H. Harkusha A. M. 'Kopiia elektronnoi informatsii yak dokaz u kryminalnomu provadzhenni: protsesualnyi ta tekhnichnyi aspekty' [Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects] (2021) 8 Yurydychnyi naukovyi elektronnyi zhurnal <http://www.lsej.org.ua/8_2021/79.pdf> (in Ukrainian)
11. Kovalenko A. V. 'Elektronni dokazy v kryminalnomu provadzhenni: suchasnyi stan ta perspektyvy vykorystannia' [Electronic evidence in criminal proceedings: current state and prospects of use] (2018) 4. Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka. 237–245 (in Ukrainian)
12. Kolotylo O. 'Pravove rehuliuvannia elektronnoho kryminalnoho provadzhennia' [Legal regulation of electronic criminal proceedings] (27 kvitnia 2020) Yurydychna hazeta <https://yur-gazeta.com/ publications/practice/kriminalne-pravo-ta-proces/pravove-regulyuvannya-elektronnogokriminalnogo-provadzhennya.html> (in Ukrainian)
13. Metelev O. P. 'Tsyfrovi dokazy yak okremyi vyd dokaziv u krymi- nalnomu protsesi' [Collection of digital information as a separate method of obtaining evidence during criminal proceedings] (2018) 10 Dosudove rozsliduvannia: aktualni problemy ta shliakhy yikh vyrishennia. 100–104 (in Ukrainian)
14. Khyzhniak Ye. S. 'Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen' [Peculiarities of reviewing electronic documents during the investigation of criminal offenses] (2017) 4 (58) Derzhava ta rehiony 80–85 (in Ukrainian)
15. Sirenko O. V, Korotkova Ye. O. 'Dosvid uprovadzhennia systemy elektronnoho kryminalnoho provadzhennia v Ukraini ta YeS' [Experience of implementing the system of electronic criminal proceedings in Ukraine and the EU] (2021) 3 Yurydychnyi naukovyi elektronnyi zhurnal <http://lsej.org.ua/3_2021/87.pdf> (in Ukrainian)
16. Shumylo M. Ie., Raimundas Yu., Kaplina V. A. 'Informatsiina teoriia dokaziv ta problemy Vykorystannia elektronnykh zasobiv dokazuvannia u kryminalnomu provadzhenni' [Information theory of evidence and problems of using electronic means of evidence in criminal proceedings] (2019) 26 (2) Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy 137–152 (in Ukrainian)
17. Tsekhan D. M. 'Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia' [Digital evidence: concepts, features and place in the evidence system] (2013) 5 Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Yurysprudentsiia 256–264 (in Ukrainian)

Thesis

18. Stolitnii A. V. 'Elektronne kryminalne provadzhennia na dosudovomu rozsliduvanni' [] (dys. … d-ra. yuryd. nauk. Natsionalna akademiia prokuratury Ukrainy, Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav, 2018) 648 (in Ukrainian)

19. Moskovchuk D. O. 'Elektronni dokazy u krainakh kontynentalnoho ta zahalnoho prava: porivnialno – pravove doslidzhennia' [Electronic evidence in continental and common law countries: a comparative legal study] (dys. doktora filos., Natsionalnyi universytet «Odeska yurydychna akademiia», 2023) 210 (in Ukrainian)
20. Kovalchuk S. O. 'Vchennia pro rechovi dokazy u kryminalnomu protsesi: teoretyko-pravovi ta praktychni osnovy' [The doctrine of material evidence in the criminal process: theoretical-legal and practical foundations] (dys. d-ra yuryd. nauk, Natsionalnyi universytet «Odeska yurydychna akademiia», 2018) 626 (in Ukrainian)
21. Ratnova A. V. 'Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni' [Criminal procedural and forensic basics of using electronic documents in evidence] (dys. doktora filosofiї, Lvivskyy derzhavnyy universytet vnutrishnikh sprav, 2021) 248 (in Ukrainian)

Confarence papers

22. Avdieieva H. 'Problemy vykorystannia elektronnykh dokazivu protydiї kiberzlochynnosti' [Problems of using electronic evidence to combat cybercrime] Protydiia kiberzlochynnosti ta torhivli liudmy : zb. materialiv Mizhnarod. nauk.-prakt. konf. (27 travnia 2020 r., m. Kharkiv) KhNUVS, 2020. <http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9089/Protydiia%20kiberzlochynnosti%20ta%20torhivli%20liudmy_2020.pdf?sequence=1&isAllowed=y > (in Ukrainian)
23. 'Tsyfrovi dokazy u kryminalnomu provadzhenni' [Digital evidence in criminal proceedings] OMUL, CRIMINOLOGIA, ȘTIINȚA Conferința științifică internațională ediția a II-a Chișinău, 24 martie 2023 <https://ibn.idsi.md/sites/default/files/imag_file/370-374_5.pdf> (in Ukrainian)
24. Hlynska N. V. 'Shchodo vykorystannia tsyfrovoi informatsii v kryminalnomu provadzhennia: okremi aspekty' [Regarding the use of digital information in criminal proceedings: certain aspects] Vykorystannia tsyfrovoi informatsii v rozsliduvanni kryminalnykh pravoporushen: materialy mizhnar. nauk.-prakt. kruhloho stolu, (m. Kharkiv, 12 hrud. 2022 r.) 18–22 <http://surl.li/glknx> (in Ukrainian)
25. Shylo O. H., Shylo A. V. 'Do pytannia vprovadzhennia v Ukraini elektronnoho kryminalnoho provadzhennia Pravovi zasady diialnosti pravookhoronnykh orhaniv: zbirnyk naukovykh statei, tez dopovidei ta povidomlen za materialamy VII Mizhnarodnoi naukovo-praktychnoi konferentsii (10–11 hrudnia 2020 roku, Kharkiv) Vyp. 36. 109–111. (in Ukrainian)

Websites

26. 'Electronic evidence – Belgium'(EJN Forum) <https://www.ejnforum.eu/cp/e-evidence-fiche/230/0> (in English)
27. Matveiev V. 'Problemy ta vyklyky, poviazani zi zborom elektronnykh dokaziv' [Issues and challenges related to electronic evidence collection] (JUSTTALK) <https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv> (in Ukrainian)
28. Suddi VS obhovoryly z ekspertamy pytannia shchodo dopustymosti elektronnykh dokaziv, otrymanykh iz vidkrytykh dzherel' [Supreme Court judges discussed the admissibility of electronic evidence obtained from open sources with experts] (Sudova vlada Ukrainy, 7 chervnia 2022) <https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/?fbclid=IwAR38uhyaCGNZyG19U7Wjs3l20JCS3uuPfSCwOeUx4BFW9iWWysF6297brsY> (in Ukrainian)
29. 'Suddi KKS VS obhovoryly problemni pytannia dopustymosti elektronnykh dokaziv pid chas sudovoho rozghliadu' [«Judges of the Supreme Court discussed the problematic issues of the admissibility of electronic evidence during the trial»] (Sudova vlada Ukrainy, 28 zhovtnia 2021) <https://court.gov.ua/press/news/1202385/> (in Ukrainian)

Глинська Н. В., Клепка Д. І.
Основні аспекти стратегії унормування інституту цифрових доказів в кримінальному процесуальному законодавстві

Стаття присвячена визначенню основних аспектів стратегії унормування електронних доказів в кримінальному провадженні України. У роботі вирішуються такі завдання як обґрунтування доцільності інституціоналізації цифрових доказів, ідентифікації та систематизації основних практичних викликів (можливих небезпек), пов'язаних із оперуванням цифровими доказами, формулювання основних стратегічних та тактичних аспектів інституціоналізації цифрових доказів у національному кримінальному процесуальному законодавстві. У роботі доводиться, що потреба унормування в КПК комплексу питань щодо використання електронних доказів у кримінальному провадженні є нагальною, а воєнний стан ще більш актуалізував її.

Визначаються основні аспекти нормативної стратегії інституціоналізації цифрових доказів в кримінальному процесуальному законодавстві України, до яких віднесено: визнання цифрових доказів окремим джерелом доказів в кримінальному провадженні; модернізація кримінального процесуального механізму збирання електрон-

них доказів; запровадження спеціальних стандартів зберігання електронної інформації; унормування спеціальних критеріїв оцінки цифрових доказів (потребує проведення наукової розвідки щодо критеріїв оцінки цифрових доказів з точки зору їх допустимості, які мають процесуальне значення та підлягають унормуванню); встановлення імперативної вимоги участі фахівця як під час збирання цифрової інформації, так і під час її дослідження в суді.

Робиться висновок про те, що при унормуванні в КПК тих чи інших стратегічних аспектів інституту цифрових доказів тактично важливим є дотримання балансу між, з одного боку – функціональною необхідністю закріплення специфіки механізму збирання, фіксації, зберігання та оцінки цифрових доказів з огляду на їх природу, з іншого боку – дотримання стандарту лаконічності закону та відсутності зайвої деталізації («не перевантаження закону спеціальною термінологією»). Доречним в цьому сенсі є використання бланкетних норм з відсиланням до спеціальних законів, що визначають та деталізують цифрові технології (за їх наявності), а також унормування окремих аспектів на рівні підзаконних нормативно-правових актів (як то покрокова алгоритмізації дій щодо фіксації та збереження цифрової інформації, встановлення кваліфікаційних вимог до комп'ютерних фахівців тощо).

Ключові слова: *кримінальне процесуальне законодавство, цифрові докази, цифрова інформація, нормативна стратегія*

Glynska N. V., Klepka D. I.
Basic aspects of the normalization strategy
Institute of Digital Evidence in Criminal Procedure Law

The article is devoted to defining the main aspects of the strategy of normalization of electronic evidence in the criminal proceedings of Ukraine. The work solves such tasks as justifying the feasibility of institutionalization of digital evidence, identification and systematization of the main practical challenges (possible dangers) associated with the operation of digital evidence, formulation of the main strategic and tactical aspects of the institutionalization of digital evidence in the national criminal procedural legislation. The work proves that the need to standardize the set of issues related to the use of electronic evidence in criminal proceedings in the Criminal Procedure Code is urgent, and the state of war has made it even more urgent.

The main aspects of the normative strategy of institutionalization of digital evidence in the criminal procedural legislation of Ukraine are determined, which include: recognition of digital evidence as a separate source of evidence in criminal proceedings; modernization of the criminal procedural mechanism for collecting electronic evidence; introduction of special standards for storing electronic information; normalization of special criteria for the assessment of digital evidence (requires scientific research on the criteria for assessing digital evidence from the point of view of their admissibility, which have procedural significance and are subject to normalization); establishment of an imperative requirement for the participation of a specialist both during the collection of digital information and during its examination in court.

It is concluded that when normalizing certain strategic aspects of the institution of digital evidence in the CCP, it is tactically important to maintain a balance between, on the one hand, the functional necessity of establishing the specifics of the mechanism for collecting, recording, storing and evaluating digital evidence considering its nature, with on the other hand, compliance with the standard of brevity of the law and the absence of unnecessary detail («not overloading the law with special terminology»). In this sense, it is appropriate to use blanket norms with reference to special laws defining and detailing digital technologies (if they exist), as well as the normalization of certain aspects at the level of subordinate legal acts (such as the step-by-step algorithmization of actions regarding the recording and preservation of digital information, establishment of qualification requirements for computer specialists, etc.).

Keywords: *criminal procedural legislation, digital evidence, digital information, regulatory strategy.*

Стаття надійшла до редакції:22.09.2023 р.
Прийнята до друку: 20.11.2023 р.