УДК 343.982.4

ГУЦАЛЮК М.В., *кандидат юридичних наук., с.н.с., доцент,*
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.
АНТОНЮК П.Є., *кандидат юридичних наук.,* професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ.
ORCID: https://orcid.org/0000-000-1269-6992.

ПРОЦЕСУАЛЬНА СПРОМОЖНІСТЬ ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ (ЦИФРОВОЇ) ІНФОРМАЦІЇ ЯК ДОКАЗУ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Анотація. *Правоохоронні органи та суди дедалі частіше у своїй діяльності досліджують фактичні дані (докази), зафіксовані в електронній (цифровій) формі, які зберігаються на технічних носіях інформації. Водночас національне кримінальне процесуальне законодавство не містить чіткого визначення поняття "електронні докази", що призводить до неоднозначної практики їх оцінки та використання в процесі доказування при розслідуванні кримінальних правопорушень. Аналіз судової практики також свідчить про різні підходи до оцінки належності і допустимості електронних доказів (фактичних даних, зафіксованих в електронній (цифровій) формі) у різних видах судочинства. У статті обґрунтовується необхідність визначення категорії "електронні докази" у Кримінальному процесуальному кодексі України та пропонується розробка нової парадигми теорії електронних доказів.*

Ключові слова: *електронні докази, кіберзлочин, комп'ютерні дані, спеціаліст, копіювання інформації, джерело доказів, електронна (цифрова) інформація, фактичні дані.*

Summary. *Law enforcement agencies and courts are increasingly investigating factual data (evidence) recorded in electronic (digital) form, which are stored on technical media. At the same time, the national criminal procedure legislation does not contain a clear definition of the term "electronic evidence", which leads to ambiguous practices of their evaluation and use in the process of proving in the investigation of criminal offenses. The analysis of judicial practice also shows different approaches to assessing the relevance and admissibility of electronic evidence (factual data recorded in electronic (digital) form) in different types of proceedings. The article substantiates the need to define the category of "electronic evidence" in the Criminal Procedure Code of Ukraine and proposes the development of a new paradigm of electronic evidence theory.*

Keywords*: electronic evidence, cybercrime, computer data, specialist, copying information, source of evidence, electronic (digital) information, factual data.*

Постановка проблеми. На початку 21 століття у зв'язку зі значним зростанням кількості інформації та необхідності її опрацювання і передачі в усіх розвинутих країнах світу почали активно використовувати електронні (технічні та програмні) засоби обробки інформації, які зберігають та передають її в електронній формі. Відповідно дослідження International Data Corporation (IDC) кількість такої інформації (колективні дані світу) подвоюється кожні півтора року, і у 2025 році становитиме 175 зеттабайта (трильйон гігабайт) [1].

Різноманітні електронні ресурси зберігаються в хмарних центрах обробки даних, в системах стільникового зв'язку, комп'ютерах, смартфонах, пристроях Інтернету речей (IoT) тощо.

Перехід суспільства в глобальному масштабі до цифрових технологій, геометричне зростання кількості даних, а також кількості користувачів Інтернет, яких у світі вже понад 5 млрд., при відсутності належного правового врегулювання суспільних відносин у цих сферах, посилює безпекові ризики, несе загрозу кібербезпеці держав, зокрема у: банківській сфері, господарській діяльності, захисті персональних даних, функціонуванні об'єктів критичної інфраструктури тощо.

Кіберзлочинність є однією зі значних загроз кібербезпеці. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Згідно Конвенції про кіберзлочинність крім злочинів, які безпосередньо стосуються конфіденційності, цілісності та доступності комп'ютерних даних і систем (Розділ XVI Кримінального Кодексу України (далі – КК України), до кіберзлочинів відноситься також шахрайство та підробка, що пов'язані з використанням комп'ютерів, злочини пов'язані з розміщенням у мережах протиправної інформації, злочини щодо авторських і суміжних прав тощо [3].

Таким чином, до кіберзлочинів в сучасному розумінні відноситься багато видів кримінально протиправної діяльності, в яких використовуються комп'ютерні технології: торгівля наркотиками через Інтернет, зброєю через Даркнет, поширення дитячої порнографії, кібершахрайство, фішинг тощо. Доходи від такої протиправної діяльності постійно зростають і відповідно до досліджень компаній Herjavec Group та Cybersecurity Ventures збитки від кіберзлочинності у 2021 році становили ***6 трлн.*** доларів США, порівняно з 3 трлн. у 2016 році.

Очікується, що глобальні витрати на кіберзлочинність зростатимуть на 15 відсотків щорічно протягом наступних п'яти років, досягнувши ***10,5 трил.*** доларів США ***до 2025 року***. Це найбільша передача економічного багатства в історії, що загрожує стимулам для інновацій та інвестицій, перевищує збиток, завданий природними катаклізмами за рік, більш прибуткова, ніж незаконна глобальна торгівля всіма основними наркотичними засобами [4].

В Україні аналогічно до загальносвітової тенденції кількість кіберзлочинів також постійно зростає. Так, у 2021 році порівняно з 2020 роком за інформацією офіційної статистичної звітності Офісу Генерального прокурора кількість кримінальних правопорушень, передбачених розділом XVI КК України (Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку) збільшилася на 32,5 % (2021 р. – 3310, 2020 р. – 2498). При цьому кількість тяжких злочинів збільшилася на 47,9 % (2021 р. – 2549, 2020 р. – 1723). У 3,2 рази збільшилася кількість кримінальних правопорушень, передбачених Розділом XVI КК України, що вчинені групою осіб (2021 р. – 187, 2020 р. – 58) [5].

З метою забезпечення необхідного рівня кібербезпеки крім різноманітних заходів кіберзахисту практично в усіх країнах світу сьогодні не лише створюються спеціальні підрозділи, співробітники яких спеціалізуються на виявленні, документуванні та розслідуванні кіберзлочинів, але й формується відповідне законодавство, що дозволяє забезпечити ефективну протидію кіберзлочинності, в тому числі й на міжнародному рівні.

На відміну від інших країн, в Україні досі актуальною залишається проблема використання значного обсягу інформації, зафіксованій в електронній формі, як доказів у кримінальному провадженні і не лише при розслідуванні кіберзлочинів. Особливої

значущості окреслена проблема набуває при розслідуванні військових злочинів, вчинених на території України, з подальшим представленням результатів розслідування в міжнародні інституції.

Інформація, зафіксована в електронній (цифровій) формі, може легко змінюватися, знищуватися, передаватися, копіюватися. 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, у свою чергу, 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 монітору чи роздруківці принтеру до різного виду фактичних даних.

Таким чином, електронна форма інформації означає її існування та збереження у вигляді "комп'ютерних даних", які, відповідно до Конвенції про кіберзлочинність означають 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 [3].

Тому усвідомлення специфічної природи електронної (цифрової) інформації, особливостей її створення, зберігання, перетворення, а також врахування таких особливостей в Кримінальному процесуальному кодексі (далі – КПК України) шляхом запровадження окремої процесуальної категорії електронних доказів надасть можливість використовувати фактичні дані, існуючі в цифровому форматі, у такій сфері суспільних відносин, як кримінальне провадження.

Результати аналізу наукових публікацій. Дослідження питань використання інформації, зафіксованої в цифровій формі (електронних доказів) в судочинстві проводилися зарубіжними науковцями та практиками ще з кінця минулого століття. Сьогодні у розвинутих країнах розроблені посібники, відповідні методичні рекомендації та наукові праці. Серед авторів, які приділили свою увагу дослідженню електронних доказів, слід зазначити Nigel Jones, Esther George, Uwe Rasmussen, Stephen Mason, Daniel Seng та інші. Проблемні аспекти використання інформації, зафіксованої в електронній формі, як доказу ставали предметом уваги й вітчизняних дослідників, таких як: Н.М. Ахтирська, П.Д. Біленчук, В.Д. Гавловський, О.А. Самойленко, В.Г. Хахановський та інші.

Проте невдалі спроби законодавця якимось чином ситуативно врегулювати проблему нормативної визначеності електронної (цифрової) інформації та використання її в процесі доказування при розслідуванні кримінальних правопорушень стають приводом для продовження наукового обговорення специфічної природи таких фактичних даних і їх місця в системі процесуальних джерел доказів у кримінальному провадженні.

Метою статті є обґрунтування необхідності внесення змін в Кримінальний процесуальний кодекс України щодо унормування категорії "електронні докази", а також процедури їх збирання, дослідження та використання при розслідуванні кримінальних правопорушень.

Виклад основного матеріалу. Так, в ч. 1 ст. 237 КПК України законодавець зазначає, що "З метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та *комп'ютерних даних*". Далі, в ч. 2 зазначеної норми роз'яснюється, що "*Огляд комп'ютерних даних* проводиться слідчим, прокурором

шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі)".

Для того, щоб суб'єкту розслідування забезпечити відображення інформації, яку містять комп'ютерні дані, та зафіксувати її у протоколі, він повинен сам ознайомитися з нею, іншими словами, сприйняти її за допомогою органів сприйняття, як і інші об'єкти матеріального середовища, які можуть сприйматися ним в ході огляду – місцевість, приміщення, речі, документи.

Але, з урахуванням природи інформації, зафіксованої в електронній формі, і навіть самого поняття "комп'ютерні дані" (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* [3], таке сприйняття безпосередньо суб'єктом розслідування фізично неможливе [6].

Більш того, намагаючись відтворити певні комп'ютерні дані у протоколі огляду, як то передбачає законодавець, суб'єкт розслідування вже фактично вносить певні зміни в таку інформацію, залишаючи "цифровий слід" (digital footprint) [7] в результаті своєї діяльності, тобто незворотньо змінює фактичні дані, зафіксовані у цифровій формі.

Спірним є також питання, чим в процесуальному аспекті стає така інформація-комп'ютерні дані, після її огляду. З урахуванням способів їх відображення, запропонованих законодавцем, комп'ютерні дані стають документом в розумінні ч. 2 ст. 99 КПК України. Але визначальним для процесуальної категорії "документ" є його ***матеріальна*** природа (ч. 1 ст. 99 КПК України) – властивість, якою комп'ютерні дані не володіють у звичному для нас сенсі: ми не маємо можливості сприймати їх без спеціальних технічних засобів, які перетворюють такі фактичні дані. Тобто, по своїй суті комп'ютерні дані не можуть бути ані об'єктом огляду як слідчої (розшукової) дії, ані документом як процесуальної категорії.

У зв'язку з цим вимушені констатувати, що наполегливе ігнорування законодавцем специфічної сутності електронної (цифрової) інформації та намагання ситуативно вирішити проблемні питання, пов'язані з використанням такої інформації в процесі доказування в кримінальних провадженнях, яке проявляється у чисельних змінах та доповненнях кримінальних процесуальних норм, призводить лише до поглиблення проблеми процесуальної забезпеченості електронної (цифрової) інформації як доказів.

Так, законодавець декларуючи, що "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, визнаються судом як оригінал документа" (ч. 4 ст. 99 КПК України), тим самим стверджує, що крім комп'ютерних даних в зазначених ресурсах наявна й інша інформація, відмінна від комп'ютерних даних.

В ч. 2 ст. 159 КПК України законодавець зазначає, що "тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом *зняття копії інформації*, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення". Таким чином, законодавець підтверджує відмежування поняття "комп'ютерні дані" від іншої інформації, що міститься в електронних ресурсах.

Аналогічна логіка законодавця прослідковується й в ч. 2 ст. 168 КПК України при встановленні порядку тимчасового вилучення майна, де, в тому числі, законодавець зазначає можливість слідчого чи прокурора у разі необхідності виготовити за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. При цьому копіювання такої інформації, відповідно до встановленого порядку, здійснюється із залученням спеціаліста.

Проведений аналіз норм демонструє неузгодженість кримінальних процесуальних норм між собою і, як наслідок, можливість інтерпретації певних процесуальних категорій, зокрема "комп'ютерні дані", "копія інформації з електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку" тощо.

Крім того, на нашу думку, умова обов'язкового залучення спеціаліста для копіювання електронної (цифрової) інформації демонструє визнання законодавцем специфічної природи такої інформації та необхідність фахових професійних знань у суб'єкта, який здійснює її збирання. Але, разом з тим, законодавець не встановлює жодних кваліфікаційних вимог до такого фахівця (на відміну від інших випадків обов'язкового залучення спеціаліста до кримінального провадження), що по суті знецінює роль залученого спеціаліста та зводить його участь у процесуальних діях, пов'язаних з копіюванням інформації, до формальності [6, с. 42-43].

Важливо розуміти, що в сучасних умовах інформатизації абсолютно всіх видів суспільної діяльності електронна (цифрова) інформація, що може містити відомості про подію кримінального правопорушення та становити інтерес для його розслідування – це не лише звичні електронні документи, матеріали фото-, звуко- та відеозапису в соціальних мережах тощо, а й величезний масив електронної інформації, що відображає роботу телекомунікаційних, мережевих та супутникових систем, як-то різноманітні пристрої штучного інтелекту, охоронні та пропускні системи, платіжні термінали, навігаційні системи, інформаційні ресурси у вигляді певних реєстрів тощо.

Можна впевнено стверджувати, що на сьогоднішній день розслідування всіх без виключення кримінальних правопорушень так чи інакше пов'язане з використанням цифрової (електронної) інформації, особливо з огляду на запровадження Інформаційно-телекомунікаційної системи досудового розслідування (ст. 106^1 КПК України).

І, зважаючи на особливості природи та сутності електронної (цифрової) інформації, фактичні дані, зафіксовані у такій формі, поряд з "традиційними" доказами повинні відповідати умовам належності та допустимості для встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження. А це означає, в тому числі, чітку процесуальну визначеність як процесуального місця такої інформації, так і порядку її збирання, оцінки й перевірки.

У зв'язку з цим, ми наполягаємо на необхідності запровадження окремої процесуальної категорії для інформації, зафіксованої та існуючої в цифровій (електронній) формі – електронні докази [6, с. 44], які, за умови належної процесуальної процедури їх збирання, визначеної КПК України для всіх сторін кримінального провадження, виступатимуть процесуальними джерелами доказів. Належна процедура їх збирання, на наше переконання, повинна враховувати специфічну природу таких доказів та передбачати їх отримання сторонами кримінального провадження без внесення змін в зміст фактичних даних (тобто певним фахівцем, кваліфікація якого буде чітко визначена). А їх оцінка та перевірка (фізичне сприйняття учасниками кримінального

провадження) повинні бути можливими лише через проведення експертизи або дослідження спеціальним суб'єктом.

Безумовно, такі зміни мають стати можливими лише після комплексної роботи по узгодженню між собою всіх норм КПК України, пов'язаних з запропонованою категорією, та врегулювання окремих аспектів на рівні підзаконних нормативно-правових актів (як то чітке визначення повноважень власників, користувачів та розпорядників електронних реєстрів, розмежування понять інформації та носіїв інформації, встановлення кваліфікаційних вимог до певних фахівців, визначення експертних спеціальностей тощо).

Але лише така комплексна та системна робота по забезпеченню процесуальної спроможності використання в процесі доказування по кримінальних провадженнях електронної (цифрової) інформації, на наше глибоке переконання, здатна забезпечити допустимість та належність таких фактичних даних як доказів. В протилежному випадку ми будемо ставати свідками чергових судових прецедентів та безпорадності правоохоронних органів у забезпеченні виконання функцій кримінального провадження в Україні.

Нагальна необхідність забезпечення процесуальної спроможності електронних доказів в кримінальному провадженні України продиктована також схваленням Радою Європи 17 листопада 2021 року Другого додаткового протоколу до Конвенції про кіберзлочинність про посилене міжнародне співробітництво. Документ був підписаний представниками 22 країн світу та став відкритий для підписання під час Конференції у Римі 12 – 13 травня 2022 року [9]. Оскільки Другий додатковий протокол скерований на забезпечення ефективності заходів кримінального правосуддя щодо кіберзлочинів та збору доказів в електронній формі в рамках міжнародного співробітництва, то унормування понятійного апарату щодо таких доказів та відповідної процесуальної процедури використання їх в процесі доказування на державному рівні виступатиме запорукою узгодженості та злагодженості в міжнародному правовому просторі під час надання взаємної правової допомоги.

Висновки.

Забезпечення процесуальної спроможності електронних доказів в кримінальному провадженні України можливе за умови введення зазначеної дефініції в Кримінальний процесуальний кодекс та визначення у підзаконних нормативних актах чітких процедур їх отримання, опрацювання та зберігання у тому числі з врахуванням положень Другого додаткового протоколу до Конвенції про кіберзлочинність.

Необхідність проведення зазначеної нормотворчої діяльності чітко зазначена у Плані реалізації Стратегії кібербезпеки України відповідно до Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року, введеного в дію Указом Президента України від 1 лютого 2022 року № 37/2022.

Унормування питань щодо електронних доказів в кримінальних провадженнях дозволить більш ефективно проводити боротьбу з кіберзлочинністю, яка в умовах військової агресії є одним з небезпечних елементів гібридної війни.

Використана література

1. IDC: Expect 175 zettabytes of data worldwide by 2025. URL: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

2. Про основні засади забезпечення кібербезпеки України: науково-практичний коментар Закону України. Станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

3. Про кіберзлочинність: Конвенція Ради Європи (Ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV (2824-15). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

4. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

5. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 11.01.2022).

6. Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерела доказів в кримінальному провадженні. *Криміналістичний вісник*. 2020. № 1(32). С. 37-49. DOI: 10.37025/1992-4437/2020-33-1-37.

7. Digital footprint. URL: https://en.wikipedia.org/wiki/Digital_footprint#cite_note-1

8. Електронні (цифрові) докази 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.

9. Enhanced cooperation and disclosure of electronic evidence. URL: https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~