Дослідницька робота

Відкриті джерела кіберпростору як об'єкти судово-експертного дослідження

Михайло Щербаковський *

* Д-р юрид. наук, професор, Харківський національний університет внутрішніх справ, м. Харків, Україна, ORCID: https://orcid.org/0000-0003-1990-1231, e-mail: shcherbakovskyi@gmail.com

DOI: 10.32353/khrife.2.2024.02 УДК 343.98
Надійшло 23.05.2024 / Рецензовано 24.05.2024 / Прийнято до друку 26.06.2024 / Доступно онлайн 30.06.2024

Мета роботи — за допомогою сучасних загальних і спеціальних методів наукового пізнання дослідити процесуальний порядок формування цифрових доказів за відкритою інформацією з кіберпростору в контексті доказування під час кримінального провадження й обґрунтувати можливість судово-експертного дослідження кіберпростору для отримання кримінально-релевантної орієнтувальної та доказової інформації у формі висновку експерта. Показано, що комп'ютерні дані й електронна (цифрова) інформація є синонімами та поділяються на дві групи: нейтральні, що не мають значення для кримінального провадження, і кримінально-релевантні, які містять сліди правопорушення та дані про осіб, предмети, події, факти тощо, що мають орієнтувальне або доказове значення. Доведено, що кіберпростір є окремим носієм кримінально-релевантної електронної (цифрової) інформації, яка за певних правових процедур стає джерелом доказів у кримінальному провадженні. Така інформація, перетворена на доступну для сприйняття учасниками процесу форму, належить до цифрових доказів. Обґрунтовано, що передбачені процесуальним законом слідчі дії найчастіше непридатні для пошуку кримінально-релевантної інформації з відкритих джерел кіберпростору. Аргументовано, що основним процесуальним способом формування доказів на основі комп'ютерних даних із відкритих джерел кіберпростору має стати проведення судової експертизи електронних комунікацій, об'єктом якої є вихідні дані

про об'єкт пошуку, кіберпростір, а предметом — факти й відомості про цей об'єкт. Методичними засадами експертного дослідження у цьому разі є інструменти розвідки відкритих баз даних OSINT, а для фіксування інформації — рекомендації Berkeley Protocol з урахуванням чинного законодавства України. Комп'ютерні дані, вилучені з відкритих джерел кіберпростору, набувають доказового значення завдяки висновку судового експерта, який є джерелом доказів.

Ключові слова: *кіберпростір; відкриті джерела інформації; комп'ютерні дані; цифрові докази; судова експертиза; висновок експерта.*

Постановка наукової проблеми

Поява інтернету як глобальної мережі зумовила якісно новий рівень розвитку інформаційних послуг у світі і стала технологічним підґрунтям для загального обміну інформацією. Інформаційні ресурси — чи не найважливіша цінність для функціювання сучасного суспільства. На жаль, кіберпростір використовують також у злочинних цілях як засіб скоєння правопорушень і як сховище кримінально-релевантної інформації, зокрема доказової. Кіберпростір є екстериторіальними інформаційними теренами, де відбуваються глобальні процеси соціальних комунікацій, що мають міжнародний характер. Виникнувши як суто технічний засіб передавання інформації, інтернет (як складова кіберпростору) перетворився на важливе соціальне явище, яке привертає увагу фахівців різних наук, зокрема юридичної [1].

Поява кіберпростору змінила процес доказування. Інформація, вилучена з електронно-цифрових засобів, що постійно розвиваються, призвела до появи цифрових доказів. Зважаючи на вимоги часу, до Кримінального процесуального кодексу України [2] (далі — *КПК України*) у 2022 р. внесено зміни: комп'ютерні дані визнано різновидом документів як джерел доказів (ст. 99) [3]. У процесуальному законі відсутнє визначення термінів «комп'ютерні дані», «цифрові докази», не наведено порядку їх пошуку, огляду, фіксування, вилучення та зберігання, що спричиняє численні дискусії серед науковців, помилки під час кримінального провадження в роботі із цифрової інформацією, невизнання в судовому розгляді допустимими й достовірними доказів, сформованих на її основі. Саме тому в сучасних умовах постає питання про використання цифрової інформації як доказів. Іноді така інформація — єдиний спосіб досягнення завдань

1 Гетьман А. П., Атаманова Ю. Є., Мілаш В. С. та ін. Правове регулювання відносин у мережі Інтернет : монографія / за ред. С. В. Глібка, К. В. Єфремової. Харків, 2016. С. 8. URL: https://ndipzir.org.ua/archives/5224 (дата звернення: 20.05.2024).

2 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

3 Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#n11 (дата звернення: 20.05.2024).

кримінального провадження. Поміж актуальних питань варто також назвати визначення процесуального джерела такого роду доказів.

Практика свідчить, що криміналістично значущу інформацію мають не лише сліди комп'ютерних злочинів, спрямованих на протиправне втручання в роботу комп'ютерів, комп'ютерних програм, мереж, несанкціоновану модифікацію комп'ютерних даних тощо, а будь-які комп'ютерні дані про протиправні суспільно небезпечні дії, що їх містять не тільки фізичні носії, а й відкриті джерела кіберпростору (вебсайти, месенджери, соціальні мережі тощо). У відомому *Berkeley Protocol*, розробленому для дослідження відкритих цифрових джерел, зазначено, що інформація, яку вони містять, є загальнодоступною, будь-який представник громадськості може її переглянути, придбати або запросити, не потребуючи спеціального правового статусу або дозволу на несанкціонований доступ [4].

Зауважимо, що інформаційний масив відкритих джерел кіберпростору ефективно використовують у непроцесуальній формі в межах оперативно-розшукової діяльності як різновид ініціативного оперативного пошуку [5]. В іноземній правоохоронній практиці також застосовують так звану розвідку за допомогою судово-експертних знань — *Forensic intelligence*, одним із завдань якої є пошук інформації з відкритих джерел інтернету [6]. Водночас (незважаючи на стрімкий розвиток процесів обміну інформацією в кіберпросторі) у вітчизняній практиці розслідування кримінальних правопорушень залишається нерозв'язаною низка правових питань щодо можливостей та особливостей пошуку й фіксування, використання інформації з відкритих джерел кіберпростору у кримінальному процесуальному доказуванні.

Мета статті

Дослідити процесуальний порядок формування цифрових доказів на підставі інформації з кіберпростору, доступ до якої не обмежений, у контексті доказування під час кримінального провадження й обґрунтувати можливості судово-експертного дослідження кіберпростору для отримання кримінально-релевантної орієнтувальної та доказової інформації у формі висновку експерта.

Методи дослідження

Методологічне підґрунтя дослідження — сучасні загальні та спеціальні методи наукового пізнання. Теоретичний аналіз і синтез (індукція, дедукція, порівняння, аналогія, абстрагування, класифікація) використано для дослі-

4 Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva, 2022. P. 8. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 20.05.2024).

5 Волошина М. О., Шендрик В. В. Сучасні способи оперативного пошуку первинної оперативно-розшукової інформації підрозділами кримінальної поліції. *Південноукраїнський правничий часопис.* 2019. № 4. Ч. 1. С. 14. DOI: 10.32850/sulj.2019.4.1.3 (дата звернення: 20.05.2024).

6 Ribaux O., Baechler S., Rossy Q. Forensic Intelligence and Traceology in Digitalized Environments: The Detection and Analysis of Crime Patterns to Inform Practice / Handbook of Security. Ed. by M. Gill. 3rd ed. 2022. Pp. 91—94. DOI: 10.1007/978-3-030-91735-7_47 (дата звернення: 20.05.2024).

дження й узагальнення матеріалів із літературних джерел, позицій авторів з окремих питань, що належать до предмета дослідження; системно-структурний метод сприяв розгляду й виокремленню понять інформаційних технологій у процесі доказування, формально-юридичний — розкриттю особливостей і критеріїв проведення слідчих дій та судових експертиз. Названі методи використано як взаємопов'язані та взаємодоповнювальні, що сприяло повноті дослідження й обґрунтованості сформульованих наукових висновків і пропозицій.

Аналіз основних досліджень і публікацій

Проблеми збирання, дослідження й використання електронної (цифрової) інформації, комп'ютерних даних, цифрових доказів під час досудового розслідування кримінальних правопорушень досліджували: Г. Авдєєва, П. Антонюк, Н. Ахтирська, С. Гонгало, А. Гутник, М. Гуцалюк, В. Динту, А. Коваленко, І. Краскова, О. Крицька, Т. Матюшкова, А. Новицький, О. Малахова, Я. Найдьон, Ю. Орлов, Д. Пашнєв, О. Самойленко, А. Скрипник, Є. Скулиш, О. Старенький, А. Столітній, І. Тітко, О. Торбас, В. Уваров, Є. Хижняк, Д. Цехан, С. Чернявський, В. Школьний та ін. У криміналістичних публікаціях зазвичай увагу акцентовано на отриманні комп'ютерних даних як слідів злочину та на їхньому перетворенні на цифрові докази під час розслідування правопорушень, учинених найчастіше із застосуванням комп'ютерних технологій (кіберзлочинів) [7]. Сліди правопорушень, залишені в пам'яті комп'ютерів, планшетів, телефонів та інших засобів і виявлені під

7 Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук. Запоріжжя, 2008. 245 с. ; Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук. Київ, 2007. 217 с. ; Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Київ, 2020. 104 с. ; Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. … канд. юрид. наук. Харків, 2008. 191 с. ; Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук. Київ, 2009. 222 с. ; Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук. Київ, 2005. 218 с. ; Бутузов В. М., Гавловський В. Д., Скалозуб Л. П., Скулиш Є. Д., Тітуніна К. В., Романюк Б. В. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. 404 с. ; Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж : дис. … канд. юрид. наук. Київ, 2004. 217 с. ; Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за ред. А. Ф. Волобуєва. Одеса, 2020. 372 с. ; Теплицький Б. Б., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. та ін. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз : наук.-практ. посіб. Київ, 2019. 168 с. ; Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. … канд. юрид. наук. Київ, 2021. 268 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/02fe1a3e-438b-4f1c-8800-3e745db75e8b/content (дата звернення: 20.05.2024).

час огляду й обшуку, направляють для проведення комп'ютерно-технічної експертизи. У цьому разі пошуку, вилученню та дослідженню піддають тільки той обсяг комп'ютерних даних, який містять носії, що потрапили в орбіту розслідування як речові докази або додатки до протоколів слідчих (розшукових) або негласних слідчих (розшукових) дій. Тож розробляють рекомендації щодо огляду саме цих засобів комп'ютерної техніки. Окрім того, серед вітчизняних науковців спостерігається тенденція до адаптування старих рекомендацій з візуального огляду до нових умов розвитку техніки. Водночас увагу сконцентровано не на способах вилучення інформації, а на процедурі фіксування огляду відповідних пристроїв у протоколі, їх опечатуванні та транспортуванні. На жаль, порядок виявлення, фіксування й вилучення з кіберпростору інформації, доступ до якої не обмежено, використання її у кримінальному провадженні до сьогодні залишається малодослідженим питанням у криміналістиці й не врегульованим кримінальним процесуальним законодавством.

З урахуванням криміногенних тенденцій у сфері електронних інформаційних технологій, постійного розвитку технічних електронних (комп'ютерних) засобів, програмного забезпечення, прогалин і протиріч у законодавстві, що регулює цю сферу суспільних відносин, потребують розв'язання питання щодо розроблення нових та оновлення наявних криміналістичних методів збирання цифрових доказів. Одним з актуальних напрямів дослідження є розроблення рекомендацій із пошуку кримінально-релевантної електронної (цифрової) інформації з відкритих джерел кіберпростору, її фіксування та вилучення для подальшого використання у доказуванні під час досудового розслідування й розгляду кримінальної справи в суді.

Викладення основного матеріалу дослідження

Для розкриття особливостей пошуку та використання інформації з відкритих джерел кіберпростору під час розслідування кримінальних правопорушень стисло розглянемо основні пов'язані із цим процесом поняття — *комп'ютерні дані, електронна (цифрова) інформація, носії інформації, сліди правопорушень, цифрові докази, процесуальні засоби збирання цифрових доказів*.

Інформацію в контексті злочинів, скоєних з використанням комп'ютерних технологій, науковці визначають як «віртуальну», «цифрову», «електронну», «електронно-цифрову», «машинну», «бінарну», «комп'ютерну» тощо. Відсутність єдиного усталеного терміна не є ключовою проблемою у цій сфері, хоча й має, безумовно, вагоме наукове та практичне значення. Для уточнення цього поняття звернімося до законодавства. У законах України й міжнародних нормативах наведено такі визначення:

- *«інформація — будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»* [8];
- дані — це *«інформація, яка подана у формі, придатній для її оброблення електронними засобами»* [9];

8 Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.05.2024).

9 Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 20.05.2024).

- *«цифровий контент (електронна (цифрова) інформація) — будь-які відомості чи дані в електронній (цифровій) формі, що містять об'єкти авторського права та/або суміжних прав і можуть зберігатися та/або поширюватися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі Інтернет»* [10];
- комп'ютерні дані — *«будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою»* [11].

Аналіз наведених формулювань дає підстави вважати, що синонімічно використано поняття «інформація» і «дані», «електронна (цифрова) інформація» і «комп'ютерні дані». Зазначимо, що комп'ютерні дані або електронна (цифрова) інформація містять як змістовну (факти), так і керівну (виконання функцій) складові. Окрім того, особливість комп'ютерних даних полягає в тому, що необхідність інтерпретувати інформацію для сприйняття людиною закладено в їхній природі: вони за визначенням зашифровані бінарним (цифровим) кодом і в первозданному вигляді їх здатні прочитати лише засоби комп'ютерної техніки. Однак цю сутнісну відмінність комп'ютерних даних від аналогових нівельовано тим, що засоби, на яких їх зберігають, декодують інформацію у звичний для людського сприйняття аудіовізуальний вигляд (як текст, зображення, фото, звук, відео та ін.).

Будь-які комп'ютерні дані можна диференціювати у дві групи за змістом і значенням для процесу кримінального провадження. *Перша група* — нейтральні до скоєного правопорушення відомості, що не мають значення для кримінального провадження. Кіберпростір і сучасні фізичні носії комп'ютерної інформації містять значну кількість файлів різного формату й розміру одночасно, серед яких лише одиниці можуть стосуватися певного кримінального правопорушення.

Тому *другу групу* становить кримінально-релевантна електронна (цифрова) інформація, що містить:

а) дані про відомих або розшукуваних осіб, організації, підприємства, місцевість, транспортні засоби й інші предмети, події, факти тощо, які мають орієнтувальне або доказове значення у кримінальному провадженні;

б) сліди, що виникають на етапах підготовки, учинення або приховування правопорушення.

У криміналістичній літературі наведено численні визначення електронних (цифрових) слідів як результатів протиправної діяльності, автори яких акцентують увагу на різних їхніх особливостях. Так, А. Коваленко розуміє електронні (цифрові) сліди кримінального правопорушення як комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних

10 Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 20.05.2024).

11 Конвенція про кіберзлочинність : прийнята Ком. міністрів Ради Європи 08.11.2001 р. ; ратифік. Законом України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 20.05.2024).

з учиненням кримінального правопорушення [12]. Автор привертає увагу до криміналістичної природи слідів як змін, що відбулися внаслідок кримінального правопорушення. Г. Авдєєва та С. Стороженко пишуть, що електронні цифрові сліди — це матеріальні невидимі сліди, які можна виявити, зафіксувати й вивчити за допомогою цифрових електронних пристроїв і які містять будь-яку криміналістично значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях. Водночас матеріальними носіями вважають електронні або цифрові пристрої: телефони, смартфони, комп'ютери, портативні пристрої геолокації (*GPS, Glonass*), цифрові фотоапарати, відеореєстратори, вебкамери, мережеві маршрутизатори, платіжні системи та ін. [13] Автори наголошують на тому, що сліди правопорушень містяться винятково на електронних (цифрових) пристроях. А. Скрипник уважає, що електронно-цифровий слід — це будь-яка криміналістично значуща комп'ютерна інформація, тобто відомості (повідомлення, дані), зафіксовані в електронно-цифровій формі на матеріальному носії або передані каналами зв'язку за допомогою електромагнітних сигналів [14]. Останнє визначення нам здається більш точним, оскільки передбачає наявність кримінально-релевантної інформації не тільки на звичних носіях, які можна візуально спостерігати.

На нашу думку, до окремого носія кримінально-релевантної електронної (цифрової) інформації належить кіберпростір — інформаційне середовище, у якому відомості перебувають у вигляді символів, образів, сигналів і які призначені для перенесення інформації у просторі й часі. Законодавцем визначено: «*Кіберпростір — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних*» [15]. За глосарієм Комітету із систем національної безпеки США, кіберпростір — це взаємозалежна мережа інфраструктур інформаційних технологій, яка містить інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори й контролери у критичних галузях [16].

Із криміналістичних позицій кіберпростір — це сховище, сфера існування

12 Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2022. Вип. 4 (100). С. 230. DOI: 10.33766/2524-0323.100.226-236 (дата звернення: 20.05.2024).

13 Авдєєва Г. К., Стороженко С. В. Електронні сліди : поняття та види. *Там само*. 2017. Вип. 1 (77). С. 170. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/44/42 (дата звернення: 20.05.2024).

14 Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. … д-ра філос. у галузі права. Харків, 2021. С. 74.

15 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.05.2024).

16 Committee on National Security Systems (CNSS). Glossary. CNSSI No. 4009. April 6, 2015. P. 40. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (дата звернення: 20.05.2024).

криміналістично значущої інформації, яка за певних правових процедур стає основою джерел доказів у кримінальному провадженні. О. Самойленко називає аксіомою те, що сліди злочину в кіберпросторі відбиваються одночасно в багатьох апаратних засобах комп'ютерної техніки, комп'ютерної мережі або телекомунікаційної мережі, мережі електрозв'язку [17]. На думку Д. Цехана, кіберпростір означає нове техніко-соціальне середовище, яке створено на базі високих інформаційних технологій та об'єднує персональні комп'ютери в інтернет-мережу [18].

Особливість кіберпростору зумовлена такими чинниками: наддержавний і децентралізований характер, відсутність єдиної організації, яка би сповна координувала й контролювала його функціювання; технологічна незахищеність, відкрите середовище комунікації; можливість анонімної діяльності в комп'ютерних мережах, спрощені процедури реєстрації користувачів, майже цілковита відсутність достовірних ідентифікаторів особистості [19]. У характеристиці сутності кіберпростору можна виокремити дві основні складові. *Перша* — інформаційно-технологічний простір, що містить інтернет із його ресурсами (інтернет речей, англ. *Internet of Things, IoT*) і послугами, *друга* — соціальний простір з користувачами, які у ньому комунікують.

Інформація у кіберпросторі існує у якісно іншому вимірі, кардинально відмінному від аналогового. На противагу об'єктам-носіям, які можна візуально спостерігати й ідентифікаційні ознаки яких (найменування, тип, марка, модель та ін.) можна визначити, кіберпростір таких ознак не має. Натомість комп'ютерні дані мають певні фіксовані характеристики — такі, як обсяг (розмір), формат (вид інформації), відомості про місце знаходження (реквізити розміщення), час (створення, модифікування, використання, знищення) та ін. Інформацію можна зафіксувати із зазначенням її даних — найменування вебсайту, сторінки, соціальної мережі, часу виявлення та ін. Зауважимо, що особливістю комп'ютерних даних є їхнє відділення від носія. Саме тому копіювання інформації з кіберпростору призводить до зміни носія, але дані водночас залишаються незмінними.

Цілком очевидно: для того щоб комп'ютерні дані надалі використовувати у кримінальному провадженні як докази, їх слід отримати в передбаченому процесуальним законом порядку. Необхідність використовувати електронну (цифрову) інформацію в доказуванні своєю чергою породило термін «цифровий доказ». За п. 3.5 Міжнародного стандарту *ISO/IEC* 27037:2017, цифровий доказ (англ. *Digital Evidence*) — це *«інформація або дані, збережені або передані*

17 Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса, 2020. С. 111. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6d9682a6-f1ab-49a5-a609-6ca96ce3c96f/content (дата звернення: 20.05.2024).

18 Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса, 2011. С. 30.

19 Хижняк Є. С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права*. 2017. № 79. С. 160. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/d43d895a-0cc7-4c06-9705-3b48054ecd84/content (дата звернення: 20.05.2024).

у бінарному вигляді, на які можна посилатися як на докази» [20]. Провідні західноєвропейські вчені в галузі кібербезпеки розглядають електронні докази (англ. *Electronic Evidence*) як будь-яку інформацію, що створюють, зберігають або передають у цифровій формі, яку згодом можна використати як доказ [21]. Вітчизняні науковці під цифровими доказами розуміють фактичні дані, які представлені у цифровій (дискретній) формі й зафіксовані на будь-якому типі носія та які після опрацювання комп'ютером стають доступними для сприйняття людиною [22]. Не вдаючись у тривалу наукову дискусію, зауважимо, що відсутність у кримінальному судочинстві поняття «цифровий доказ» породжує не лише різне його трактування правниками, а й неоднозначний підхід до нього в судовій практиці [23].

Незважаючи на наявну проблемну ситуацію, законодавець передбачив певний перелік слідчих дій, спрямованих на формування джерел доказів, змістом яких є електронна (цифрова) інформація. Так, відповідно до КПК України: комп'ютерні дані можна виявити в разі тимчасового доступу до електронних інформаційних систем, комп'ютерних систем або їхніх частин, мобільних терміналів систем зв'язку (ст. 160), обшуку (ст. 236), огляду (ст. 237), знятті інформації з електромереж — комунікаційних (ст. 362) або інформаційних (ст. 363); під час проведення процесуальних дій допускається повне копіювання інформації з об'єктів огляду, обшуку, доступу; за результатами проведених процесуальних дій формуються джерела доказів — речові докази (ст. 98) або документи (ст. 99); за потреби для виявлення кримінально-релевантної інформації призначають комп'ютерно-технічну експертизу (ст. 242) щодо вилучених речових доказів або носіїв інформації, які є додатками до протоколів слідчих і негласних слідчих (розшукових) дій (ст. 105) [24]. Аналізування названих процесуальних дій свідчить, що не всі їх можна застосувати для пошуку кримінально-релевантної інформації з відкритих джерел кіберпростору: наприклад, можна зняти тільки інформацію, передану за допомогою відповідних мереж, а за результатами копіювання інформації під

20 ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) : прийнято наказ. ДП «УкрНДНЦ» від 06.12.2017 р. № 400. [Чинний від 01.01.2019]. Київ, 2018. 31 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 20.05.2024).

21 Jones N., George E., Mérida F. I., Rasmussen U., Völzow V. Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0. Cybercrime Division Directorate General of Human Rights and Rule of Law. Strasbourg, France. 15 Dec 2014. P. 11. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf (дата звернення: 20.05.2024).

22 Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази / за ред. канд. юрид. наук, доц. О. Денькович, д-р права, проф. Г. Шмельцер. [Електрон. вид.] Львів, 2022. С. 133. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 20.05.2024).

23 Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 1 (30). С. 126—143. DOI: 10.32353/khrife.1.2023.07 (дата звернення: 20.05.2024).

24 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

час огляду, обшуку, тимчасового доступу вилучити лише ті комп'ютерні дані, які вміщено в електронних засобах (ст. 160, 236, 237, 362 і 363 КПК України) [25].

У межах традиційного підходу безпосередньо виявити необхідну для розслідування інформацію із відкритих джерел кіберпростору можна у процесуальний спосіб лише в разі огляду або пошуку під час обшуку ввімкнених комп'ютерних засобів. Огляд комп'ютерних даних здійснюють: а) на місці події як складову огляду комп'ютерних засобів; б) як окрему слідчу дію під час огляду тих самих засобів, вилучених як речові докази; в) під час огляду інформації, скопійованої на спеціально підготовлений носій, який є додатком до протоколу відповідної слідчої дії. У літературних джерелах наведено докладні рекомендації щодо слідчого огляду комп'ютерних даних, спрямованого на ознайомлення із публічно доступними ресурсами інтернету [26], вилучення інформації із хмарного середовища [27], огляд вебсторінок [28], пошук у соцмережах і за IP-адресами [29] тощо. Варто зауважити, що такий огляд допустимий, оскільки здобуття відомостей з електронних інформсистем або їхніх частин, доступ до яких не обмежено їхнім власником (володільцем, утримувачем) або не пов'язано з подоланням системи логічного захисту, не потребує дозволу слідчого судді (ст. 264 КПК України) [30].

Уважаємо, що під час проведення огляду або обшуку можливість пошуку комп'ютерних даних у кіберпросторі із відкритих публічних джерел інформації обмежена й залежить від двох аспектів. У простій ситуації, коли необхідно ознайомитися, наприклад, із відкритою вебсторінкою на ввімкненому пристрої, огляд цілком прийнятний. У складних ситуаціях, коли обмежено вихідні дані щодо об'єкта пошуку, не відомі інформація, яку можна знайти в кіберпросторі, та її обсяг, такий огляд проводити недоцільно. Це обумовлено наведеними далі чинниками. *По-перше,* пошук інформації у відкритих джерелах передбачає застосування різноманітних спеціальних програмних інструментів і певної методики дослідження — виявлення за первинними відомостями певного інформаційного контенту, аналізування нової здобутої інформації, з'ясування додаткових відомостей, знову пошук за новими даними, аналізування додатково виявленої інформації, співставлення

25 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

26 Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія Юридичні науки.* 2023. Вип. 4. С. 55. DOI: 10.32999/ksu2307-8049/2023-4-9 (дата звернення: 20.05.2024).

27 Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : кол. моногр. Львів, 2022. С. 134. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%D0%93%D1%83%D1%82%D0%BD%D0%B8%D0%BA%2C%20%D0%A5%D0%B8%D1%82%D1%80%D0%B0_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_21_06_2022.pdf (дата звернення: 20.05.2024).

28 Малахова О. В. До питання огляду сторонами кримінального провадження змісту Інтернет-сторінок. *Вісник кримінального судочинства*. 2017. № 2. С. 65. URL: https://vkslaw.knu.ua/images/verstka/2_2017_Malahova.pdf (дата звернення: 20.05.2024).

29 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. С. 34—37.

30 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2024).

її з попередніми відомостями та ін. [31] Для отримання корисної інформації цей процес може повторюватись багаторазово. Водночас слідчий огляд передбачає проведення операцій, дій і сприйняття отриманих результатів, зрозумілих усім учасникам слідчої дії. Однак маніпуляції, які в разі пошуку інформації проводить спеціаліст під час огляду комп'ютерних даних на підставі спеціальних знань з використанням технічних і програмних засобів [32], неочевидні та здебільшого недоступні іншим учасникам слідчої дії. *По-друге,* огляд (пошук) даних у кіберпросторі, зважаючи на описану вище процедуру, може забрати багато часу (кілька годин, днів або тижнів) і перевищити розумні строки проведення слідчої дії. Окрім того, для фіксування пошуку комп'ютерних даних рекомендовано здійснювати безперервне відеофіксування екрана пристрою [33], що доцільно лише для першої зі згаданих ситуацій. *По-третє,* якщо пошук здійснюють з електронного пристрою — речового доказу, який оглядають, то втручання у його інформаційну структуру незворотно змінює початкові комп'ютерні дані.

Проведений аналіз свідчить, що усталена парадигма кримінального процесу поводження з комп'ютерними даними полягає у пошуку, виявленні та перетворенні електронної (цифрової) інформації на аналогову, щодо якої застосовують традиційний огляд. Ці дії мають на меті відшукати й вилучити комп'ютерні дані з носіїв — електронних засобів, які можна візуально сприймати: персональних комп'ютерів, ноутбуків, планшетів, флешнакопичувачів, телефонів та ін. Специфіка «цифрової допомоги» залученого спеціаліста в пошуку інформації полягає в тому, що з огляду на об'єктивні причини більшість дій він здійснює приховано, тим самим фактично підміняючи слідчого в основній, пізнавальній частині слідчої (розшукової) дії. Зміни процесуального закону, пов'язані з уведенням комп'ютерних даних, переважно обмежено правилами ретельного опису технічних засобів, програм вилучення та зберігання комп'ютерних даних як різновиду документів або речових доказів. Однак пошук інформації з відкритих джерел кіберпростору не відповідає наведеній парадигмі.

Іноземні дослідники зазначають, що в межах цифрової криміналістики повне вилучення та збереження всіх відомостей, які потенційно можуть стати доказами, неможливе: наприклад, для соцмереж через їхню сильно розпорошену природу, величезні розміри та спільне володіння даними. До того ж процес пошуку даних у соцмережах за своєю суттю є ітеративним (повторюваним), ручний пошук у них неможливий і тому потребує розроблення спеціальних автоматизованих методів [34]. У зв'язку з появою нових видів доказів у протоколі «Про розширення співпраці та розкриття електронних доказів»,

31 Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса, 2024. С. 64—81. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content (дата звернення: 20.05.2024).

32 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. С. 20—40.

33 Коваленко А. В. Організація і тактика … . URL: https://lj.journal.kspu.edu/index.php/lj/article/view/393/361 (дата звернення: 20.05.2024).

34 Arshad H., Omlara E., Abiodun I., Aminu A. A Semi-Automated Forensic Investigation Model for Online Social Networks. *Computers & Security*. Oct 2020. Vol. 97. Art. 101946. P. 3. DOI: 10.1016/j.cose.2020.101946 (дата звернення: 20.05.2024).

ухваленому Радою Європи (2022), зазначено, що слід удосконалювати не тільки матеріальне кримінальне право (відповідно до нових правопорушень), а й кримінально-процесуальне право та способи розслідування [35]. Саме тому сьогодення потребує впровадження нових підходів у процес доказування з використанням комп'ютерних даних, що їх містять відкриті джерела інформації в кіберпросторі.

На підставі викладеного вважаємо, що основним процесуальним способом формування доказів на основі комп'ютерних даних із відкритих джерел кіберпростору має стати проведення судової експертизи. У період переходу до цифрового розслідування об'єктами дослідження експерта слід визначити:

а) вихідні пошукові відомості про об'єкт, інформацію про який слід знайти, що надає ініціатор проведення експертизи;

б) кіберпростір як сховище кримінально-релевантних комп'ютерних даних, що містять як доказову, так і орієнтувальну інформацію про об'єкт, який має значення для розслідування кримінального правопорушення.

Здавалося б, такий підхід відрізняється від традиційного, згідно з яким експертові для дослідження надають матеріальні або матеріалізовані об'єкти, які закріплені в матеріалах справи, передбачені кримінально-процесуальним законодавством як джерела інформації [36]. Однак, *по-перше*, кіберпростір функціонує на підставі сумісних (з'єднаних) комунікаційних систем, які мають матеріальне походження; *по-друге*, як обумовлює законодавець, об'єктами експертизи є «явища та процеси» [37], що відбуваються, зокрема, у кіберпросторі; *по-третє*, жодних заперечень проти експертного дослідження такого об'єкта не виникне, якщо експертові надано носій, на який під час огляду скопійовано всю наявну на конкретну мить у кіберпросторі інформацію щодо предмета розслідування. Проте дослідження Міжнародної корпорації даних (англ. *International Data Corporation, IDC*) показало, що у 2020 р. в усьому світі передбачали створити й використати величезний обсяг даних — 44 зетабайт (44×10^{21}) [38]. Зрозуміло, що з технічних позицій неможливо існування окремого знімного носія, що містив би весь обсяг інформації кіберпростору.

Розглянута ситуація схожа з призначенням експертизи, коли об'єкт, який підлягає дослідженню, не можна безпосередньо надати експертові. У цьому разі (відповідно до Закону України «Про судову експертизу» [39] та Інструкції про

35 Convention on Cybercrime. Protocol on Xenophobia and Racism. Second Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence. Council of Europe. April 2022. Art. 1. URL: https://www.bmeia.gv.at/fileadmin/user_upload/Vertretungen/OEV_Strassburg/Dokumente/Cybercrime_-_Rechtstexte.pdf (дата звернення: 20.05.2024).

36 Сімакова-Єфремян Е. Б. Комплексні судово-експертні дослідження: теорія та практика : монографія. Харків, 2016. С. 147.

37 Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 20.05.2024).

38 Jones N., George E., Mérida F. I., Rasmussen U., Völzow V. Op. cit. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf (дата звернення: 20.05.2024).

39 Про судову експертизу … . URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 20.05.2024).

призначення та проведення судових експертиз та експертних досліджень [40]) ініціатор проведення експертизи забезпечує доступ експерта до об'єкта. У випадку з кіберпростором ініціатор проведення експертизи, окрім вихідних даних, зазначає доступний експертові об'єкт дослідження без його звичного безпосереднього надання.

Відповідно до наявної системи судових експертиз комп'ютерні дані досліджує комп'ютерно-технічна або експертиза електронних комунікацій. Ми вважаємо, що комп'ютерно-технічна експертиза не може досліджувати кіберпростір, оскільки експерт аналізує обмежену інформацію, яка фізично перебуває на матеріальному об'єкті, наданому ініціатором експертові: стаціонарні персональні комп'ютери; ноутбуки; планшети; диски, флешнакопичувачі, мобільні телефони й інші носії цифрової інформації [41]. Предмет комп'ютерно-технічної експертизи обмежений фактами щодо технічного стану й інформації у наданих на дослідження електронних носіях [42]. На нашу думку, пошук і виявлення доказової інформації з відкритих джерел у кіберпросторі доцільно здійснювати в межах експертизи електронних комунікацій і її нового виду — інформаційної. В. Коршенко називає кіберпростір різновидом інформаційних об'єктів експертизи електронних комунікацій, що містять інформацію у форматах баз даних, файлах реєстрації, аудіо-, відео-, текстових та інших форматах, яка перебуває на матеріальних носіях і яку приймають, обробляють і передають за допомогою телекомунікаційних засобів, систем і мереж [43]. Предмет експертизи електронних комунікацій можна визначити як факти, відомості про об'єкти пошуку: відомих осіб, якщо надано персональні дані, або невідомих осіб, якщо є тільки зображення зовнішності, а також про транспортні засоби й інші предмети, ділянки місцевості або споруди, про організації, зв'язки між ними та інші дані. Методичними засадами експертного дослідження доречно обрати пошукові інструменти розвідки відкритих баз даних *OSINT* (англ. *Open Source Intelligence*), а для фіксування інформації — рекомендації, викладені у *Berkeley Protocol*, з урахуван-

40 Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 20.05.2024).

41 Теплицький Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ.* 2021. № 3 (120). Т. 26. С. 30. DOI: 10.33270/01211203.28 (дата звернення: 20.05.2024).

42 Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2023. Вип. 2 (102). С. 294. DOI: 10.33766/2524-0323.102.289-305 (дата звернення: 20.05.2024).

43 Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореф. дис. … канд. юрид. наук. Харків. 2017. 22 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/ae3bf4b6-9291-451f-bc4c-ccb5091a79e8/content (дата звернення: 20.05.2024).

ням чинного законодавства [44]. Водночас особливістю експертного дослідження є не лише пошук інформації за ключовими ознаками, а й моніторинг, тобто перегляд конкретного контенту протягом певного часу. Здобуті комп'ютерні дані можуть стати вихідним матеріалом для подальшого проведення інших судових експертиз — портретної, фототехнічної, лінгвістичної, у сфері інтелектуальної власності та ін.

Проведення дослідження з відкритих публічних джерел кіберпростору особливо актуально під час війни в Україні з метою з'ясувати обставини порушення законів і звичаїв війни, ідентифікувати загарбників, довести факти колабораційної діяльності, державної зради, пропаганди війни [45]. Показовим прикладом можливості отримання важливої інформації про об'єкт пошуку в кіберпросторі є результати *OSINT*-секції групи «Інформаційний спротив», фахівці якої з'ясували дані російського воєнного злочинця — старшого матроса, кулеметника, який воює на Запорізькому напрямі: його прізвище, поштову адресу, номер паспорта, номери особистих телефонів, адресу електронної пошти, сторінки у соцмережах [46].

Висновки

Кіберпростір є носієм кримінально-релевантної електронної (цифрової) інформації, яка перебуває у відкритих джерелах. Така інформація або комп'ютерні дані, перетворені у доступну для сприйняття учасниками кримінального провадження форму, належать до цифрових доказів. Основним процесуальним способом формування доказів на підставі комп'ютерних даних із відкритих джерел кіберпростору має стати проведення судової експертизи електронних комунікацій. Об'єктом експертизи є вихідні дані про об'єкт пошуку та кіберпростір, а предметом — факти й відомості про об'єкти пошуку. Зважаючи на чинне законодавство України, методичними засадами такого експертного дослідження мають стати інструменти розвідки відкритих баз даних *OSINT* і рекомендації *Berkeley Protocol* для фіксування здобутих даних. Особливість електронної (цифрової) інформації, вилученої з відкритих джерел кіберпростору, полягає в тому, що вона набуває доказового значення завдяки висновку судового експерта, який є джерелом доказів.

Open Sources of Cyberspace as Objects of Forensic Research

Mykhailo Shcherbakovskyi

The purpose of this research paper is to use modern general and special methods of scientific cognition to investigate the procedural procedure for the formation of digital evidence based on open information from cyberspace in the context of evidence during criminal proceedings and to substantiate possibility of forensic expert research of cyberspace to obtain criminally relevant indicative and evidentiary

44 Торбас О. О. Зазнач. твір. С. 51—53, 65—99. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content (дата звернення: 20.05.2024).

45 Ragni Ch. Digital Evidence in international Criminal Proceedings and Human Rights Challenges. *Law in the Age of Modern Technologies* : International Scientific Conference on International, EU and Comparative Law Issues. Nov 2023. Art. 7:1—16. Pp. 5—6. DOI: 10.25234/eclic/28255 (дата звернення: 20.05.2024).

46 Воює на Запорізькому напрямку: OSINT-секції групи «ІС» встановила дані воєнного злочинця / Інформаційний спротив. 07.05.2024. URL: https://sprotyv.info/news/voyu%d1%94-na-zaporizkomu-napryamku-osint-sekczi%d1%97-grupi-is-vstanovila-dani-vo%d1%94nnogo-zlochinczya/ (дата звернення: 20.05.2024).

information in the form of a conclusion an expert It is shown that computer data and electronic (digital) information are synonymous and are divided into two groups: neutral that have no significance for criminal proceedings, and criminally relevant, which contain traces of an offense and data about persons, objects, events, facts etc., which have indicative or evidential value. It has been proven that cyberspace is a separate carrier of criminally relevant electronic (digital) information, which under certain legal procedures becomes a source of evidence in criminal proceedings. Such information, transformed into a form accessible to process participants, belongs to digital evidence. It is substantiated that investigative actions provided for by the procedural law are most often unsuitable for searching for criminally relevant information from open sources of cyberspace. It is argued that the main procedural method of forming evidence based on computer data from open sources of cyberspace should be conducting a forensic examination of electronic communications, the object of which is the initial data about the search object, cyberspace, and the subject — facts and information about this object. object In this case, methodological principles of the expert research are the intelligence tools of open OSINT databases, and for recording information, the recommendations of the Berkeley Protocol, taking into account the current legislation of Ukraine. Computer data extracted from open cyberspace sources acquire probative value through the opinion of a forensic expert who is a source of evidence.

***Keywords**: cyberspace; open sources of information; computer data; digital evidence; forensic science; forensic expert conclusion.*

Фінансування
Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному або некомерційному секторах.

Відмова від відповідальності
Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію або підготовку рукопису.

Учасники
Автор зробив свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і бере на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів
Автор заявляє, що у нього відсутній конфлікт інтересів, що стосується цієї теми; хоча Михайло Щербаковський є членом консультативної ради збірника, він не брав участі в ухваленні рішення щодо оприлюднення, і цю статтю піддано повному процесу експертної перевірки та редагування.

References

Arshad, H., Omlara, E., Abiodun, I., Aminu, A. (2020). A Semi-Automated Forensic Investigation Model for Online Social Networks. *Computers & Security*. Vol. 97. Art. 101946. DOI: 10.1016/j.cose.2020.101946.

Avdieieva, H. K., Storozhenko, S. V. (2017). Elektronni slidy : poniattia ta vydy [Electronic traces : concepts and types]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka.* Vyp. 1 (77). URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/44/42 [in Ukrainian].

Avdeeva, G., Żywucka-Kozlowska, E. (2023). Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics.* Issue 1 (30). Pp. 126—143. DOI: 10.32353/khrife.1.2023.06.

Berkeley Protocol on Digital Open Source Investigations (2022)/ Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.

Bilousov, A. S. (2008). *Kryminalistychnyi analiz obiektiv kompiuternykh zlochyniv* [Forensic analysis of objects of computer crimes] :

dys. ... kand. yuryd. nauk. Zaporizhzhia [in Ukrainian].

Borysova, L. V. (2007). *Transnatsionalni kompiuterni zlochyny yak obiekt kryminalistychnoho doslidzhennia* [Transnational computer crimes as an object of forensic research] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Butuzov, V. M., Havlovskyi, V. D., Skalozub, L. P., Skulysh, Ye. D., Titunina, K. V., Romaniuk, B. V. (2011). *Orhanizatsiino-pravovi ta taktychni osnovy protydii zlochynnosti u sferi vysokykh informatsiinykh tekhnolohii* [Organizational, legal and tactical foundations of combating crime in the field of high information technologies] : navch. posib. / za red. B. V. Romaniuka, Ye. D. Skulysha. Kyiv [in Ukrainian].

Committee on National Security Systems (CNSS). Glossary (2015). CNSSI No. 4009. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

Hetman, A. P., Atamanova, Yu. Ye., Milash, V. S. ta in. (2016). *Pravove rehuliuvannia vidnosyn u merezhi Internet* [Legal regulation of relations on the Internet] : monohrafiia / za red. S. V. Hlibka, K. V. Yefremovoi. Kharkiv. URL: https://ndipzir.org.ua/archives/5224 [in Ukrainian].

Holovkin, B. M., Denkovych, O. I., Lutsyk, V. V., Tsekhan, D. M. (2022). *Kiberzlochynnist ta elektronni dokazy* [Cybercrime and Electronic Evidence] / za red. kand. yuryd. nauk, dots. O. Denkovych, d-r prava, prof. H. Shmeltser. [Elektron. vyd.] Lviv. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf [in Ukrainian].

Hutnyk, A. V., Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni* [Criminal procedural and forensic bases for the use of electronic documents in evidence] : kol. monohr. Lviv. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%D0%93%D1%83%D1%82%D0%BD%D0%B8%D0%BA%2C%20%D0%A5%D0%B8%D1%82%D1%80%D0%B0_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_21_06_2022.pdf [in Ukrainian].

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [Use of electronic (digital) evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Kyiv [in Ukrainian].

Jones, N., George, E., Mérida, F. I., Rasmussen, U., Völzow, V. (2014). *Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0. Cybercrime Division Directorate General of Human Rights and Rule of Law*. Strasbourg, France. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf.

Khyzhniak, Ye. S. (2017). Poniattia virtualnykh slidiv ta yikh znachennia u protsesi rozsliduvannia zlochyniv [The concept of virtual traces and their importance in the process of investigating crimes]. *Aktualni problemy derzhavy i prava.* № 79. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/d43d895a-0cc7-4c06-9705-3b48054ecd84/content [in Ukrainian].

Korshenko, V. A. (2017). *Teoretychni ta metodychni osnovy sudovoi telekomunikatsiinoi ekspertyzy* [Theoretical and methodical foundations of forensic telecommunications examination] : avtoref. dys. ... kand. yuryd. nauk. Kharkiv. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/ae3bf4b6-9291-451f-bc4c-ccb5091a79e8/content [in Ukrainian].

Kovalenko, A. V. (2022). Poniattia ta sutnist elektronnykh (tsyfrovykh) slidiv kryminalnoho pravoporushennia [Concept and essence of electronic (digital) traces of a criminal offense]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka.* Vyp. 4 (100). DOI: 10.33766/2524-0323.100.226-236 [in Ukrainian].

Kovalenko, A. V. (2023). Orhanizatsiia i taktyka provedennia ohliadu kompiuternykh danykh [Organization and tactics of computer data review]. *Naukovyi visnyk*

Khersonskoho derzhavnoho universytetu. Seriia Yurydychni nauky. Vyp. 4. DOI: 10.32999/ksu2307-8049/2023-4-9 [in Ukrainian].

Malakhova, O. V. (2017). Do pytannia ohliadu storonamy kryminalnoho provadzhennia zmistu Internet-storinok [On the issue of reviewing the content of Internet pages by the parties to the criminal proceedings]. *Visnyk kryminalnoho sudochynstva*. № 2. URL: https://vkslaw.knu.ua/images/verstka/2_2017_Malahova.pdf [in Ukrainian].

Motliakh, O. I. (2005). *Pytannia metodyky rozsliduvannia zlochyniv u sferi informatsiinykh kompiuternykh tekhnolohii* [Issue of the methodology of the investigation of crimes in the field of information computer technologies] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Mykhalchuk, T. V. (2009). *Vykorystannia informatsii, otrymanoi telekomunikatsiinym shliakhom, u rozsliduvanni zlochyniv* [Use of information obtained by telecommunications in the investigation of crimes] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Palamarchuk, L. P. (2004). *Kryminalistychne zabezpechennia rozsliduvannia nezakonnoho vtruchannia v robotu elektronno-obchysliuvanykh mashyn (kompiuteriv), system ta kompiuternykh merezh* [Forensic support of the investigation of illegal interference in the operation of electronic computing machines (computers), systems and computer networks] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Ragni, Ch. (2023). Digital Evidence in international Criminal Proceedings and Human Rights Challenges. *Law in the Age of Modern Technologies : International Scientific Conference on International, EU and Comparative Law Issues.* Art. 7:1—16. DOI: 10.25234/eclic/28255.

Ribaux, O., Baechler, S., Rossy, Q. (2022). Forensic Intelligence and Traceology in Digitalized Environments: The Detection and Analysis of Crime Patterns to Inform Practice / *Handbook of Security*. Ed. by M. Gill. 3rd ed. DOI: 10.1007/978-3-030-91735-7_47.

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* [The basics of the methodology of investigating crimes committed in cyberspace] : monohrafiia / za zah. red. A. F. Volobuieva. Odesa. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6d9682a6-f1ab-49a5-a609-6ca96ce3c96f/content [in Ukrainian].

Simakova-Yefremian, E. B. (2016). *Kompleksni sudovo-ekspertni doslidzhennia: teoriia ta praktyka* [Comprehensive forensic research: theory and practice] : monohrafiia. Kharkiv [in Ukrainian].

Skrypnyk, A. V. (2021). *Vykorystannia informatsii z elektronnykh nosiiv u kryminalnomu protsesualnomu dokazuvanni* [Use of information from electronic media in criminal procedural evidence] : dys. ... d-ra filos. u haluzi prava. Kharkiv [in Ukrainian].

Stepaniuk, R. L., Kolesnyk, V. H. (2023). Sudova kompiuterno-tekhnichna ekspertyza: stan i perspektyvy rozvytku [Forensic computer-technical expertise: status and prospects for development]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka.* Vyp. 2 (102). DOI: 10.33766/2524-0323.102.289-305 [in Ukrainian].

Teplytskyi, B. B. (2021). *Aktualni pytannia pryznachennia ekspertyzy kompiuternoi tekhniky i prohramnykh produktiv pid chas rozsliduvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system, kompiuternykh merezh i merezh elektrozviazku* [Actual issues of appointment of examination of computer equipment and software products during the investigation of crimes in the field of use of electronic computing machines (computers), systems, computer networks and telecommunications networks]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav.* № 3 (120). T. 26. DOI: 10.33270/01211203.28 [in Ukrainian].

Teplytskyi, B. B. (2021). *Tekhniko-kryminalistychne zabezpechennia rozsliduvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku* [Technical and forensic support for the

investigation of crimes in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks] : dys. ... kand. yuryd. nauk. Kyiv. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/02fe1a3e-438b-4f1c-8800-3e745db75e8b/content [in Ukrainian].

Teplytskyi, B. B., Sharai, L. H., Kovalov, K. M., Kuzmin, S. A. ta in. (2019). *Zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku: spetsialni pytannia kvalifikatsii, provedennia slidchykh (rozshukovykh) dii, pryznachennia kompiuterno-tekhnichnykh sudovykh ekspertyz* [Crimes in the field of use of electronic computing machines (computers), systems and computer networks and telecommunications networks: special questions of qualification, conducting investigative (search) actions, appointment of computer and technical forensic examinations] : nauk.-prakt. posib. Kyiv [in Ukrainian].

Torbas, O. O. (2024). *OSINT pry rozsliduvanni kryminalnykh pravoporushen* [OSINT in the investigation of criminal offenses] : pidruchnyk. Odesa. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content [in Ukrainian].

Tsekhan, D. M. (2011). *Vykorystannia vysokykh informatsiinykh tekhnolohii v operatyvno-rozshukovii diialnosti orhaniv vnutrishnikh sprav* [The use of advanced information technologies in the operational and investigative activities of internal affairs bodies] : monohrafiia. Odesa [in Ukrainian].

Voiuie na Zaporizkomu napriamku: OSINT-sektsii hrupy «IS» vstanovyla dani voiennoho zlochyntsia (2024) [Fighting in the Zaporizhzhia direction: the OSINT section of the «IS» group established the data of a war criminal] / Informatsiinyi sprotyv. URL: https://sprotyv.info/news/voyu%d1%94-na-zaporizkomu-napryamku-osint-sekczi%d1%97-grupi-is-vstanovila-dani-vo%d1%94nnogo-zlochinczya/ [in Ukrainian].

Voloshyna, M. O., Shendryk, V. V. (2019). *Suchasni sposoby operatyvnoho poshuku pervynnoi operatyvno-rozshukovoi informatsii pidrozdilamy kryminalnoi politsii* [Modern methods of operative search of primary operational investigative information by units of the criminal police]. *Pivdennoukrainskyi pravnychyi chasopys.* № 4. Ch. 1. DOI: 10.32850/sulj.2019.4.1.3 [in Ukrainian].

Zhurba, A. I. (2008). *Osoblyvosti predmeta dokazuvannia u spravakh pro kompiuterni zlochyny* [Peculiarities of the subject of evidence in cases of computer crimes] : dys. ... kand. yuryd. nauk. Kharkiv [in Ukrainian].

Щербаковський, М. (2024). Відкриті джерела кіберпростору як об'єкти судово-експертного дослідження. *Теорія та практика судової експертизи і криміналістики*. Вип. 2 (35). С. 10—27. DOI: 10.32353/khrife.2.2024.02.