УДК 351.746.1.:343.1
DOI https://doi.org/10.24144/2307-3322.2024.85.4.9

ЦИФРОВА КРИМІНАЛІСТИКА В ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ З ПРОТИДІЇ ЗЛОЧИННОСТІ

Гора І.В.,
доктор юридичних наук, професор,
головний науковий співробітник
науково-організаційного центру
Національної академії Служби безпеки України
ORCID: 0000-0003-2940-5338
e-mail: irvitgora@ukr.net

Колесник В.А.,
доктор юридичних наук, професор,
головний науковий співробітник
науково-організаційного центру
Національної академії Служби безпеки України
ORCID: 0000-0003-3570-8984
e-mail: valarko@urr.net

Попович І.І.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права
та правоохоронної діяльності
Ужгородського Національного університету
ORSID: 0000-0003-0608-2564

Гора І.В., Колесник В.А., Попович І.І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності.

Стаття присвячена розгляду питань цифровізації суспільних та інших процесів існування й розвитку держави, суспільства, його економічної, промислової, комунікаційної, інформаційної сфери, а разом з тим і впливом цифрових технологій на злочинність та діяльність правоохоронних органів, що здійснюють боротьбу з нею.

Зазначено, що використання цифрових технологій принесло багато позитивного в суспільну й виробничу практику, полегшило виконання багатьох завдань на виробництві, в сфері управління державними й виробничими та соціальними процесами, розширило можливості для якісного й швидкого зв'язку між людьми з використанням ними комп'ютерних систем і мереж, всесвітньої мережі Інтернет. Водночас використання передових наукових розробок і сучасних технологій з протиправною метою створило труднощі для своєчасного виявлення ознак підготовки злочинів, збирання доказів і здійснення доказування під час досудового розслідування. Певні труднощі в доказуванні вини злочинців зумовлені появою нових і мало вивчених на даний час доказів – електронних та їхніх джерел, з дослідженням доказової інформації в цифровій формі та з її використанням в доказуванні.

Виконанню завдань з протидії злочинності має стати на допомозі наука криміналістика та її новий напрям – криміналістика цифрова. Ці питання широко обговорюють сьогодні українські та зарубіжні науковці й практики. Деякі з них вважають цифрову криміналістику окремою наукою, що розробляє питання боротьби з кіберзлочинами та іншими, які вчинені з використанням комп'ютера. Втім автори статті, спираючись на думки вітчизняних і зарубіжних науковців, доводять, що цифрова криміналістика – це не окрема наука, а напрям традиційної науки криміналістики, положення якої охоплюють питання криміналістичної техніки, тактики й методики розслі-

дування злочинів. Її розробки спрямовані на пошук, дослідження й використання в доказуванні електронних доказів і цифрових слідів.

У висновку сформульовано авторське розуміння основних завдань нового для нас напряму цифрової криміналістики, розв'язання яких потрібне для оптимальної інтеграції електронних доказів до системи традиційних та забезпечення їх визнання судовою практикою.

Ключові слова: кримінальне провадження, досудове розслідування, кіберзлочини, криміналістичне забезпечення, протидія вчиненню злочинів, цифрова криміналістика, цифрові сліди, електронні докази, доказування.

Hora I.V., Kolesnyk V.A., Popovich I.I. Digital forensics in the provision of crime prevention activities.

The article is devoted to the consideration of issues of digitalization of social and other processes of existence and development of the state, society, its economic, industrial, communication, and information spheres, as well as the impact of digital technologies on crime and the activities of law enforcement agencies fighting against it. It was noted that the use of digital technologies brought a lot of positive things to social and industrial practice, facilitated the performance of many tasks in the production of products, in the field of management of state and industrial and social processes, expanded opportunities for high-quality and fast communication between people using computer systems and networks, the worldwide Internet. The use of advanced scientific developments and modern technologies for illegal purposes created difficulties for timely identification of signs of preparation of crimes, collection of evidence and implementation of evidence during pre-trial investigation. Certain difficulties in proving the guilt of criminals are due to the emergence of new and little-studied evidence – electronic and their sources, with the study of evidentiary information in digital form and its use in evidence.

The science of criminology and its new direction - digital criminology - should help in the fulfillment of tasks to combat crime. These questions are widely discussed today by Ukrainian and foreign scientists and practitioners. Some of them consider digital forensics as a separate science that deals with the fight against cybercrimes and crimes that are committed using a computer. However, the authors of the article, relying on the opinions of domestic and foreign scientists, prove that digital forensics is not a separate science, but a direction of the traditional science of forensics, the provisions of which cover issues of forensic techniques, tactics and methods of crime investigation. Its developments are aimed at the search, research and use in proving electronic evidence and digital traces.

The author's understanding of the main tasks of digital forensics is formulated, the solution of which is necessary for the optimal integration of electronic evidence into the system of traditional evidence and ensuring their recognition by judicial practice.

Key words: criminal proceedings, pre-trial investigation, cybercrime, forensic support, crime prevention, digital forensics, digital traces, electronic evidence, proof.

Постановка проблеми. Прийдешнє тисячоліття і його перше століття справедливо вважають ерою інформаційних технологій. Суспільство вийшло на новий і раніше небачений рівень віртуального простору, що дає людям можливість спілкуватись будь-коли і на будь-якій відстані одне від одного, скорочує час на створення, передавання та пошук інформації, керування за її допомогою виробничими й іншими процесами навіть без особистої присутності людини. Водночас як і будь-які науково-технічні новації, віртуальна реальність приховує в собі небезпеки, пов'язані з використанням її як поля для злочинної діяльності, незаконного збагачення, порушення майнових, особистих прав та свобод громадян. Визнаючи протиправний і навіть злочинний характер окремих дій у віртуальному просторі, виявити факт вчинення кримінального правопорушення, довести провину і покарати злочинця іноді доволі складно. Багато в чому це пов'язано з тим, що віртуальний простір, цифрові технології зберігають в собі багато незвіданих до сьогодні таємниць та можливостей для зловживання. Не лише вітчизняне, а й законодавство багатьох іноземних країн не встигає за регламентацією діяльності та розробленням заходів боротьби з правопорушеннями, які відбуваються в інформаційно-комунікаційному просторі.

Мережа Інтернет та віртуальна реальність стали справжньою хворобою нашого століття. Здолати небезпеку і позбавитись наслідків кіберзлочинності з кожним роком стає все більш складно, а інтернет-залежність в суспільстві зростає. Стрімкий процес інформатизації, цифровізації, що відбувається в нашій країні, не лише розкриває шляхи для розвитку творчих можливостей і

здібностей людини в обстановці вільного доступу до будь-якої інформації, але й дедалі більше починає створювати загрози особистій, національній, міжнародній безпеці. Розповсюдження й використання з протиправною метою інформації сепаратистського, терористичного, екстремістського характеру підриває спокій населення, створює загрозу його добробуту, а сьогодні в умовах відкритої воєнної агресії рф становить серйозну проблему як для окремої людини, так і для всього суспільства, держави, співдружності держав. Не дарма такі проблеми стають темою для наукових досліджень, що розкривають питання інформаційного простору і безпеки в ньому. Процеси цифровізації зачіпають не лише технологічний сектор економіки та цифрові корпорації, а й доволі різноманітні сфери діяльності фізичних та юридичних осіб. Ними пронизані усі найбільш значущі сфери існування сучасного суспільства і держави, вони стали невід'ємною частиною життєдіяльності кожної людини. Масштабний перехід сучасного суспільства на «цифру» зупинити вже не можна і на цьому шляху немає вороття, адже це є цінним для користувача, вигідним для бізнесу, значущим для регулятора [1, с. 87].

Цифровізація вплинула не лише на злочинну діяльність, сформувавши новий простір для вчинення злочинів – цифрове середовище, давши їй в руки нові знаряддя злочину й можливості застосування нових способів вчинення низки злочинів, викликавши механізм утворення принципово нових цифрових слідів, але й суттєво змінила роботу правоохоронців із виявлення та досудового розслідування кримінальних правопорушень. Це вимагає використання оперативним працівником, слідчим, експертом нових і надсучасних комп'ютерних засобів, їх надійного програмного забезпечення, знання можливостей і порядку збирання електронних доказів, розуміння особливостей їх перевірки, оцінки, зберігання та використання в доказуванні. Сьогодні від нового криміналістичного напряму – цифрової криміналістики вимагається вивчення цих питань і розроблення науково обґрунтованих криміналістичних рекомендацій із забезпечення роботи представників правничих професій, а не лише правоохоронців в умовах цифровізації суспільства, економіки, державного управління.

Метою дослідження виступає надання відомостей щодо впливу процесу цифровізації на злочинну діяльність та її антипод – діяльність правоохоронних органів, що здійснюють боротьбу з нею, сучасних підходів вітчизняних й зарубіжних науковців та практиків до збирання й оцінки та використання електронних доказів, розуміння поняття «цифрова криміналістика», визначення її ролі й місця в системі криміналістичних знань.

Стан опрацювання проблематики. В наукових працях останнього десятиліття широко висвітлюються питання виявлення й дослідження комп'ютерних засобів, електронних доказів та їх джерел, цифрових слідів та особливостей використання спеціальних знань в досудовому розслідуванні злочинів, які вчиняються з використанням комп'ютерних засобів, інформаційно-комунікаційних технологій, в сфері обігу комп'ютерної інформації. Розглядались і питання ролі криміналістики та її нового напряму – цифрової криміналістики в забезпеченні пошуку, фіксації та дослідження цифрових слідів вчинення злочину, використання електронних документів та інших цифрових доказів у доказуванні. Такі й пов'язані з ними питання неодноразово висвітлювали в своїх публікаціях вітчизняні криміналісти, фахівці в галузі кримінального процесу, теорії оперативно-розшукової діяльності, зокрема: В. Гавловський, М. Думчиков, І. Заяць, А. Колодіна, В. Коновалова, К. Латиш, Ю. Орлов, Д. Пашнєв, С. Перлін, О. Полотай, Р. Степанюк, В. Теплицький, В. Хахановський, В. Шевчук, В. Шепітько та ін. Водночас одним з гострих і таких, що вимагають поглибленого дослідження, залишається питання використання комп'ютерних засобів та інформаційно-комунікаційних технологій в діяльності оперативних працівників, слідчих, детективів, встановлення ролі й значення цифрової криміналістики в забезпеченні діяльності правоохоронних органів з протидії кіберзлочинності. Актуальність дослідження таких питань має не лише теоретичне, а й суто прикладне значення для забезпечення криміналістичними розробками діяльності осіб та органів, що здійснюють боротьбу зі злочинністю.

Виклад основного матеріалу. Комп'ютеризація та цифрова інформатизація є засобами трансформації соціальної динаміки, сприяння модернізації способу життя людини та перетворення в іншу, цифрову форму методів виробництва, економіки, управління, державних і недержавних сфер життєдіяльності. Визначаючи поняття цифровізації, вітчизняні науковці звертають увагу передусім на цифрові системи, здатні до автономної дії, з аналітичними та прогнозними функціями, що роблять вибір за людину та самостійно вирішують поставлені перед нею завдання. Ними зазначається, що оцифрування – це ще не штучний інтелект, але й не суто людське мислення. У

цьому контексті інформатизація є невід'ємною частиною цифровізації. Цифровізація – це процес впровадження цифрових технологій у населення, підприємства та суспільство, незворотній і незамінний, корисний і допоміжний елемент у загальному процесі еволюції суспільної цивілізації. Діджиталізація (цифрові технології) прийшла на зміну старим електронним засобам зв'язку – телефону, факсу, телеграфу. Це означає не лише зміну способів спілкування, але й зміну того, що ми повідомляємо. Нові цифрові технології дозволяють створювати величезні обсяги інформації та поширювати її серед майже необмеженої кількості людей [2, с. 42].

По суті, цифровізація – це ніщо інше ніж перетворення будь-якої інформації у цифрову форму, коли має місце заміна аналогових (фізичних) систем збирання й обробки даних технологічними електронними системами. У широкому смислі – це процес перенесення до цифрового середовища функцій і діяльності, які раніше виконувалися людьми та організаціями. На даний час фіксується перехід окремих цифрових технологій штучного інтелекту від реалізації пілотних проектів на новий етап розвитку до широкомасштабного впровадження в технологічні процеси та виведення на ринок масових цифрових продуктів. Водночас цифровізація діяльності правоохоронних органів в цілому та окремих напрямів оперативної, процесуальної й криміналістичної та експертної діяльності, зокрема, є невід'ємною запорукою підвищення ефективності виявлення й досудового розслідування кримінальних правопорушень та їхнього розгляду судом. Сучасне технічне оснащення дає змогу оперативного, в розумінні – швидкого й своєчасного виявлення й розкриття злочинів силами оперативних і слідчих підрозділів. Цифровізація діяльності з виявлення й досудового розслідування кримінальних правопорушень – це перехід на новий рівень роботи працівників правоохоронних органів. Процес цифровізації правоохоронної діяльності містить в собі не лише технічне оснащення, а й забезпечення підключення до різноманітних інформаційних баз даних у віддаленому доступі, використовуючи для цього можливості глобальної мережі. Водночас це вимагає створення умов для навчання працівників оперативних, слідчих, експертних підрозділів не лише роботі з використанням сучасного обладнання, але й засвоєння ними знань, що потрібні для збирання, збереження й використання електронних доказів та їх носіїв.

Цифровізація сфери судочинства означає все більш широке використання в ній цифрових даних, сучасних електронних засобів цифрової обробки, фіксації й зберігання відомостей, які мають значення для виконання завдань кримінального судочинства. Разом з тим, реалізація наданих кримінальним процесуальним законодавством можливостей збирання органами досудового розслідування доказів при розслідуванні окремих злочинів, вчинених на шкоду інформаційній та кібербезпеці держави, зіштовхується з низкою суттєвих труднощів й проблем, які потребують свого нагального вирішення. Мова йде про отримання доказів, відомості про які відображені у цифровій формі, а також їх електронних носіїв. При розслідуванні таких злочинів виникає необхідність у пошуковій діяльності, спрямованій на виявлення, оцінку і лише потім на вилучення цифрової інформації і її носіїв за наявності достатніх підстав вважати, що вона має суттєве значення для встановлення фактичних даних як доказів. До того ж, трапляються випадки, коли фактичне вилучення первинних носів такої цифрової інформації значно ускладнене, або й взагалі неможливе. Ось чому правоохоронна практика та науки кримінально-правового циклу, що обслуговують таку діяльність, повинні враховувати й сучасні реалії та пов'язані з ними наслідки цифровізації економіки, соціально-політичної сфери, державного управління, освіти, культури, побуту.

Це в повній мірі стосується й тієї інформації, яка отримується працівниками оперативно-розшукових підрозділів ще до початку здійснення кримінального провадження або ж після початку досудового розслідування і може бути передана у встановленому порядку слідчому, прокурору для оцінки ними доказового значення й визначення потреби використання в доказуванні. Справа в тому, що така інформація за своїми якісними характеристиками не збігається з жодним із традиційних об'єктів пошуку. Відмінність полягає у її нематеріальній природі, у той час як усі інші об'єкти пошуку є матеріальними. І навіть пошук ідеальної інформації, що зберігається в пам'яті особи, пов'язаний насамперед із відшуканням такої фізичної особи. Фіксуючи виявлену інформацію в її цифровій формі на матеріальному носії, оперативний працівник та слідчий можуть вилучати дані, які мають значення для справи, проте зміст повинен залишатися незмінним. Самі по собі електронні носії не відображують і не містять ніяких слідів злочину. І лише з того моменту, коли слідчий зафіксував на них шукану інформацію, набувають процесуальну значимість. Доказове значення при розслідуванні конкретного кримінального провадження буде мати сама інформація, яка зафіксована на відповідних електронних носіях. Тим більше, що відповідно

до чинного КПК України слідчий при проведенні окремих слідчих та негласних слідчих (розшукових) дій може застосовувати кілька різноманітних способів фіксації доказової інформації, зокрема й у цифровій формі. Отже, слідчий, прокурор для отримання доказів може використовувати інформацію в цифровій формі, яка зафіксована ним особисто або надана йому оперативними працівниками чи іншими особами у встановленому для цього порядку.

Сьогодні проблеми цифровізації суспільних та всіх інших відносин, в яких бере участь людина, мають безпосереднє відношення до криміналістики як науки та криміналістичної діяльності. Адже, як зазначають науковці й практики, комп'ютерні дані, що відбиваються в електронному вигляді на різних інформаційних ресурсах та носіях, стають джерелом криміналістично значущої інформації, отримання якої і стає завданням правоохоронних органів. Методи збору такої інформації суттєво відрізняються від традиційних методів отримання доказових даних. Але вони можуть надати інформацію щодо готування злочинів, їх виявлення, збору інформації щодо осіб в кримінальному провадженні, бази відомостей, необхідних при підготовці до проведення різного роду слідчих дій тощо [3, с. 74]. Джерелом таких відомостей можуть бути отримані органом досудового розслідування й зафіксовані у цифровій формі відомості з локальних комп'ютерних мереж, з глобальної мережі Інтернет, із створюваних окремими відомствами та службами інформаційних банків даних тощо. Цифрова форма фіксації таких відомостей не лише придатна для використання слідчим в кримінальному провадженні для доказування фактичних обставин, що мають значення для розслідування, але й надає можливість її перевірки та підтвердження повноти, встановлення відсутності чи наявності її спотворення, внесення змін, часткового знищення первинних відомостей тощо.

Стрімкий розвиток цифрових технологій в Україні супроводжується значною динамікою злочинів у даній сфері. На це вказують вітчизняні науковці, про це свідчить практика протидії злочинності. Так звані «кіберзлочини» є найбільш динамічнішою групою суспільно небезпечних діянь, адже з кожним роком стають усе більше масовими й небезпечнішими. Щороку вчиняються десятки тисяч злочинів з використанням інформаційно-телекомунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. Також необхідно враховувати й те, що в сучасних умовах до легального економічного обігу активно надходять нетрадиційні види майна, у тому числі інтернет-сайти, електронні гроші, технології мобільного зв'язку тощо. В результаті виникають усе нові види злочинних посягань, що передбачають використання сучасних інформаційних технологій на умовах раптовості й анонімності [4, с. 99]. У протиправній діяльності зловмисники широко використовують сучасні засоби й технології зв'язку, електронні платіжні системи, можливості Інтернет-сервісів, що забезпечують анонімізацію особи у цифровому просторі, залишаючи при цьому складні для виявлення й дослідження слідчим та спеціалістами й експертами цифрові сліди. Здебільшого цифрова трансформація зачіпає такі сфери кримінального бізнесу як незаконний обіг наркотиків, зброї, нелегальний гральний бізнес, викрадання грошей з використанням систем дистанційного банківського обслуговування, легалізації (відмивання) доходів, отриманих протиправним шляхом, ухилення від сплати податків, злочини корупційної спрямованості [1, с. 88].

Сьогодні цифрові технології і комунікативні ресурси мережі Інтернет активно використовуються із метою умисного поширення негативних інформаційних впливів, деструктивної пропаганди та інших інформаційних операцій, що створює безпосередню загрозу заподіяння шкоди не лише окремій особі, але і безпеці держави. Разом із тим, тяжкість наслідків для життєво важливих національних інтересів, що можуть настати внаслідок зазначених суспільно небезпечних дій, значно зростає в умовах воєнного стану або в період збройного конфлікту, а в реаліях сьогодення – в умовах повномасштабного вторгнення в Україну військ країни-агресора.

Активна цифровізація суспільних відносин та усіх сфер людської діяльності, а разом з тим і технічна оснащеність кримінальних структур призводять до необхідності розробок окремих теорій і вчень, спрямованих на: забезпечення використання правоохоронними органами цифрової техніки в ході виявлення й розслідування злочинів, а також на виявлення, фіксацію, дослідження та використання цифрових слідів й іншої цифрової інформації та інформаційно-технологічних пристроїв. Особливо перспективними для наукової розвідки на сьогодні є актуальні проблеми криміналістики, пов'язані із кіберпростором. Як слушно підкреслює В. Шепітько, особливості криміналістики полягають в тому, що вона використовує сучасні можливості науки й техніки, дані природничих та технічних наук з метою правозастосування. Фактично криміналістика на-

повнює належним змістом процесуальну форму, весь процес руху до відновлення істини, досягненню справедливості у кримінальному судочинстві [5, с. 167]. Цифровізація ставить перед криміналістами нові завдання з виявлення й вивчення нових закономірностей наслідків діяльності людини, що пов'язані з новітніми процесами використання інноваційних цифрових технологій.

Беззаперечним є визнання науковцями й практиками того, що криміналістика є наукою, яка постійно удосконалюється. З появою нових видів, нових способів та знарядь вчинення злочинів з'являються нові завдання, а з ними й нові напрями в криміналістиці. Оскільки сучасна злочинність навчилася використовувати комп'ютерні засоби, електронні пристрої, інформаційні технології з їх програмним забезпеченням, цифрову інформацію у своїх злочинних цілях, предметом криміналістичних досліджень доволі часто стають різноманітні цифрові об'єкти. Все частіше виникає необхідність в об'єктивній оцінці електронної інформації й проведенні низки комплексних досліджень таких специфічних цифрових об'єктів, котрі допоможуть виявити злочинця. Важливим є також розуміння специфіки тієї інформації, котра на сьогодні отримала визначення – «цифрова». Усе це в сукупності дає змогу забезпечити однаковий підхід до збирання й вивчення, зниження ймовірної кількості помилок, що припускаються правоохоронцями при оцінці зібраних доказів. Також важливим є й вміння оперативних працівників і слідчих правильно поводитися з електронними пристроями, створеною й збереженою в них цифровою інформацією, вилучати й зберігати їх, досліджувати та правильно оцінювати й використовувати в доказуванні інформацію, носіями котрої вони є.

Сьогодні криміналістика є наукою, розробки якої займають особливе й одне з чільних місць в процесі протидії сучасній злочинності. Вивчаючи закономірності механізму вчинення злочину й відображення його слідів у матеріальних та ідеальних, а на тепер – і у віртуальних, цифрових образах, криміналістика вивчає одночасно з цим і закономірності антиподу злочинної діяльності – діяльності з протидії їй. Вивчення взаємодіючих у механізмі вчинення злочинів об'єктів призводить до потреби врахування оперативним працівником, слідчим, експертом закономірностей механізму та особливостей утворення різноманітних слідів, у тому числі й таких нових як цифрові. Саме постійне удосконалення криміналістики на основі використання досягнень найрізноманітніших наук, що трансформувалися в арсеналі криміналістичних засобів і технологій роботи з будь-якою юридично значущою інформацією, створює умови для дослідження цих проблем. Криміналістична методологія, яка дає змогу реалізувати науково-технічний, інформаційно-технічний потенціал криміналістики, виходить з такої структури інформаційного каналу: відомості про механізм вчинення діяння у широкому смислі його розуміння та його відображення в матеріальному середовищі; сукупність джерел доказової інформації; інформаційні технології доказування.

Необхідно зазначити, що протидія злочинності засобами криміналістики може бути ефективною лише тоді, коли методи вивчення злочинності та реагування на неї будуть змінюватися разом із зміною вимог часу. Ось чому на сьогодні стало можливим виділити окремий напрям у розвитку криміналістики як науки – поява «цифрової криміналістики». У окремих джерелах для позначення цього напряму використовують й інші терміни – «комп'ютерна» або «комп'ютерна системна криміналістика» чи «мережева криміналістика». У той же час деякі вчені навіть розглядають комп'ютерну криміналістику як самостійну прикладну науку для розслідування злочинів, пов'язаних з комп'ютерною інформацією, дослідження цифрових доказів, пошуку, отримання та фіксування цих доказів, розроблення методів отримання і фіксації таких доказів й інших цифрових слідів. Такий підхід вважаємо доволі спірним і позбавленим належного обґрунтування.

Разом з тим головним завданням криміналістики як галузі наукових знань та кожного з її наукових напрямів було і залишається забезпечення спрямованої на встановлення істини в судочинстві діяльності органів досудового розслідування, оперативних підрозділів, суду найефективнішими й найсучаснішими засобами, прийомами і методами, що використовуються винятково з метою сприяння об'єктивному й справедливому судочинству.

Зарубіжні науковці і фахівці в галузі професійної правової освіти звертають увагу на те, що цифровий слід повсякденного життя людей став величезним і, відповідно, ймовірність того, що незаконна діяльність залишить цифрові сліди як докази, дуже висока. Потреба в судових слідчих, які мають компетенцію в розслідуванні кіберзлочинів, зросла і це призвело до появи багатьох програм академічної освіти та сертифікації, пов'язаних із цифровою криміналістикою [6, с. 1–10]. Поява нових форм кіберзлочинності також вимагає адаптивних моделей процесу розслідування, нових технологій і передових методів для боротьби з такими інцидентами. Крім зростання кі-

берзлочинності очікується, що докази в доволі значній кількості справ про різні злочини будуть цифровими. Саме цифрові докази лежать в основі майже всіх сучасних місць злочинів. Наприклад, мобільні електронні пристрої стали основним джерелом цифрових доказів, оскільки майже всі наші сучасні комунікації здійснюються через них [7]. Вказується зарубіжними науковцями й на те, що електронні листи, постачальники хмарних послуг, онлайн-платежі та переносні пристрої часто використовуються слідчими для отримання цифрових доказів за різних обставин. Стандартизація процесів цифрової криміналістики для хмарних технологій, мобільних пристроїв, Інтернету речей, дронів тощо стає пріоритетною, оскільки вони є невід'ємною частиною майже всіх сучасних цифрових розслідувань. Консенсус щодо розробки цих стандартів і скоординованих зусиль, докладених протягом останніх кількох років для протидії кіберзлочинності, має бути використаним для уніфікації законодавства в різних юрисдикціях і сприяння цифровим розслідуванням. Загальна відповідь на проблему та використання тих самих заходів створили б сильну протидію кіберзлочинності та покращили час реагування на інциденти безпеки та їх аналіз [8].

Асоціацією Головного Поліцейського Офісу Англії, Уельсу і Північної Ірландії (*англ*. – ACPO) у 2012 році підготовлено практичне керівництво для роботи з цифровими доказами, в якому зазначено, що при роботі з такими доказами треба дотримуватись певних принципів: 1 – жодних дій з боку правоохоронних органів чи їх агентів, що могли б змінити цифрові дані, на які згодом можна посилатись у суді; 2 – за потреби отримання доступу до вихідних даних особа повинна бути компетентною у цьому та бути в змозі дати пояснення релевантності (істотності) та значенню наслідків своїх дій; 3 – аудиторський слід або інший запис усіх процесів, застосованих до цифрових доказів, має бути створеним та збереженим, а третя сторона повинна мати можливість перевірити ці процеси і досягти такого ж результату; 4 – особа, відповідальна за розслідування, несе загальну відповідальність за законність отримання доказів та дотримання цих принципів. Також зазначено, що усі цифрові докази підпорядковуються тим самим правилам і законам, які застосовуються до документальних доказів. З метою дотримання принципів роботи з цифровими доказами необхідно зафіксувати електронні пристрої, на яких докази було отримано для забезпечення збереження вихідних даних і з тим, щоб третя сторона мала можливість це перевірити [9, с. 6].

Згодом Агентством Європейського Союзу з мережевої та інформаційної безпеки (*англ*. – ENISA) у 2014 році видано базовий посібник із збирання цифрових доказів для працівників служб першого реагування на кіберінциденти. В ньому серед іншого зазначено, що загрози кібербезпеці та кібератаки не знають кордонів. З цієї причини необхідна ефективна співпраця між спільнотами на всіх рівнях, щоб сприяти обміну інформацією та знаннями, необхідними для зменшення вразливості та ефективного реагування на кіберінциденти. Захист цифрових доказів є завданням і відповідальністю правоохоронних органів, а спеціалісти можуть зробити свій внесок у цю роботу, допомагаючи зберегти їх під час виявлення кіберзлочину. Збір цифрових доказів – це, як правило, наука, де під час процесу потрібно приймати спеціальні рішення на основі факторів, які неможливо визначити заздалегідь [10, с. 2-3]. Розроблення таких та подібних до них криміналістичних засобів і рекомендацій по роботі з електронними доказами має становити одне із завдань цифрової або як її ще називають в деяких інших зарубіжних країнах – комп'ютерної криміналістики як напряму в галузі криміналістичних знань.

Висновки. Реалізація наданих кримінальним процесуальним законодавством України можливостей збирання й використання електронних доказів при досудовому розслідуванні злочинів, що вчинені на шкоду інформаційній або кібербезпеці держави, підприємства, установи чи особи зіштовхується з низкою суттєвих труднощів й проблем, які потребують нагального вирішення. При розслідуванні таких злочинів виникає необхідність у пошуковій діяльності, спрямованій на встановлення й оцінку, вилучення й подальше використання в доказуванні цифрової інформації. У забезпеченні виконання завдань оперативних і слідчих підрозділів та діяльності з протидії злочинності важливу роль відіграють наукові положення й розробки криміналістики.

До нагальних завдань сучасної криміналістики та її нового напряму – цифрової криміналістики можна віднести: розробку моделі організації виявлення й розслідування кіберзлочинів та кримінальних правопорушень, що вчинені у сфері або з використанням сучасних інформаційно-комунікаційних технологій; окреслення дотичних до оперативної та слідчої діяльності принципів інформаційно-аналітичної роботи з цифровою інформацією; розроблення основ методики досудового розслідування кіберзлочинів та рекомендацій із збирання доказової й іншої значущої цифрової інформації з відкритих і обмежених доступом джерел; розгляд і вирішення питань взаємодії

та співробітництва міжнародних і національних правоохоронних органів у виявленні й розслідуванні кіберзлочинів та злочинів у глобальних мережах зв'язку; використання спеціальних знань та забезпечення проведення експертних досліджень в протидії кіберзлочинам. Криміналістиці потрібен науково обґрунтований арсенал нових криміналістичних засобів, напрацювання сучасного розуміння раніше вироблених понять, що дають змогу досліджувати інформаційні процеси, які протікають у двох видах діяльності – злочинній та тій, що пов'язана з її виявленням й досудовим розслідуванням і судовим розглядом кіберзлочинів та інших кримінальних правопорушень, вчинених в галузі комп'ютерних та інформаційно-комунікаційних технологій. На підсумок можна стверджувати, що сьогодні цифрова криміналістика розвивається разом із іншими напрямами традиційної вже науки, а за окремими з питань навіть випереджаючи цей розвиток, стаючи його своєрідним локомотивом, рушійною силою.

Зазначене висуває задачу досягнення процесуально й раціонально оптимальної інтеграції цифрових доказів до системи традиційних «аналогових», «матеріальних» та «ідеальних», забезпечення їх зіставлюваності та визнання судовою практикою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гора І.В., Колесник В.А., Попович І.І. До питання про цифрову криміналістику в системі криміналістичних знань. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2024. № 68. С. 86–91. DOI: https://doi.org/10.32782/2307-1745.2024.68.18.
2. Ціжма Ю.І., Лишак О.А., Ціжма О.А. Діджиталізація як сучасна рушійна сила вдосконалення судово-експертної діяльності. *Криміналістика і судова експертиза: міжвідом. наук.-метод. зб. / КНДІ судових експертиз*; редкол.: О.Г. Рувін та ін. Київ: Вид. Ліра-К, 2023. Вип. 68. С. 40–47.
3. Костенко М.В. Особливості інноваційного процесу у сфері криміналістики. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.)* / редкол.: В.Ю. Шепітько, В.А. Журавель, В.М. Шевчук, Г.К. Авдєєва. Харків: Право, 2019. С. 72–75.
4. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія / І.В. Гора, В.А. Колесник, В.В. Малюк, В.О. Ходанович, А.М. Черняк, Л.І. Щербина. Київ: 7БЦ, 2023. 512 с.
5. Шепитько В. Роль криминалистики в состязательном судебном процессе. *Criminalistics and forensic expertology: science, studies, practice. Vilnius,* 2016. С. 166–180.
6. Nance K., Armstrong H., Armstrong C. «Digital forensics: Definingan education agenda» in Proc. 43rd Hawaii Int. Conf. Syst. Sci., 2010, DOI: 10.1109/HICSS.2010.151. Pp. 1–10.
7. The European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape. 2021. ISBN: 978-92-9204-536-4. DOI: 10.2824/324797. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
8. Research Trends, Challenges and Emerging Topics in Digital Forensics: A Review of Reviews. Received January 22, 2022, accepted February 16, 2022, date of publication February 24, 2022, date of current version March 10, 2022. URL: https://www.researchgate.net/ publication/358837101_Research_Trends_Challenges_and_Emerging_Topics_in_Digital_Forensics_A_Review_of_Reviews.
9. ACPO Good Practice Guide for Digital Evidence, March, 2012. 43 p.
10. Electronic evidence – a basic guide for First Responders. Good practice material for CERT first responders. European Union Agency for Network and Information Security (ENISA). Vassilika Vouton, 700 13, Heraklion, Greece, 2014. 21 p. ISBN 978-92-9204-111-3, doi: 10.2824/068545.