УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2022-10/155

ЦИФРОВА КРИМІНАЛІСТИКА: СЬОГОДЕННЯ ТА НАПРЯМКИ РОЗВИТКУ

DIGITAL FORENSICS: TODAY AND DIRECTIONS OF DEVELOPMENT

Зленко О.О., студент IV курсу факультету прокуратури
Національний юридичний університет імені Ярослава Мудрого

Котенко Б.В., студент IV курсу факультету прокуратури
Національний юридичний університет імені Ярослава Мудрого

XXI століття ознаменувалося активним розвитком інформаційних та цифрових технологій, що внесло корективи в усі галузі науки, сфери послуг та суспільного життя. Криміналістика не стала винятком у процесі діджиталізації, внаслідок чого у 70-х рр. минулого століття виникла нова галузь криміналістики – цифрова криміналістика. Цифрова криміналістика є відносно новою наукою, що пройшла 4 етапи розвитку, починаючи з 1985 року, для того, щоб у сучасних умовах протидіяти організованій, транснаціональній злочинності та тероризму.

Швидкий розвиток комп'ютерної техніки, інформаційно-телекомунікаційних технологій та інноваційних систем зумовив і стрімкий розвиток цифрової криміналістики протягом останніх 50-ти років. На сьогодні в Україні та європейських країнах широко застосовуються новітні технології для отримання, обробки та використання криміналістичної, оперативної та процесуальної інформації.

У статті досліджено наукові здобутки вітчизняних дослідників цифрової криміналістики, напрацювання міжнародних організацій, що доклали зусиль для розвитку цієї галузі в Європі, та публіцистичні матеріали, пов'язані із сучасними системами збору цифрових доказів в умовах складної воєнно-політичної ситуації на сході Європи (російсько-українська війна).

У статті опрацьовуються нормативно-правові акти, що регулюють процеси цифрової криміналістики в Україні та Європі. Це ДСТУ 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», що набрав чинності з 1 січня 2019 року та протокол Берклі, що широко використовується в Україні останні пів року працівниками кіберполіції, управліннями Національної поліції України, Служби безпеки України та науково-дослідними експертно-криміналістичними центрами МВС України.

Удосконалення біометричних систем розпізнання особи перебуває сьогодні в одному ряду з такими актуальними напрямами, як розвиток реакторів на швидких нейтронах, суперкомп'ютерів і грід-технологій. Унаслідок військової злочинної російської агресії проти України з березня 2022 року українськими правоохоронними органами для перевірки осіб на блокпостах та виявлення окупантів, що перебувають на території України активно застосовується система розпізнавання облич Clearview AI. Наведені переваги та недоліки вказаного додатку з урахуванням двозначного ставлення європейського суспільства до цієї розробки. У статті акцентується увага на таких видах цифрових доказів, як супутникові знімки, та можливості їх застосування у судових процесах, оскільки українське кримінально-процесуальне законодавство не має чіткої регламентації використання такої цифрової інформації під час розслідування злочинів.

Ключові слова: діджиталізація, цифрова криміналістика, цифровий знак, протокол Берклі, принцип обміну Локара, WikiLeaks, Bellingcat, Clearview AI.

The 21st century was marked by the active development of information and digital technologies, which made corrections in all fields of science, services and social life. Forensic science was not an exception in the process of digitalization, as a result of which a new branch of forensics emerged in the 70s of the last century – digital forensics. Digital forensics is a relatively new science that has undergone 4 stages of development since 1985 in order to combat organized, transnational crime and terrorism in today's environment.

The rapid development of computer technology, information and telecommunication technologies, and innovative systems has led to the rapid development of digital forensics over the past 50 years. Today, the latest technologies for obtaining, processing and using forensic, operational and procedural information are widely used in Ukraine and European countries.

The article examines the scientific achievements of domestic digital forensics researchers, the work of international organizations that have made efforts to develop this field in Europe, and journalistic materials related to modern digital evidence collection systems in the conditions of a complex military and political situation in Eastern Europe (Russian- Ukrainian war).

The article elaborates legal acts regulating the processes of digital forensics in Ukraine and Europe. This is DSTU 27037:2017 "Information technologies. Protection methods. Guidelines for the identification, collection, acquisition and preservation of digital evidence", which entered into force on January 1, 2019, and the Berkeley protocol, which has been widely used in Ukraine for the past six months by cyber police officers, departments of the National Police of Ukraine, the Security Service of Ukraine and research experts forensic centers of the Ministry of Internal Affairs of Ukraine. The specified national standard was developed by a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and where permanent foreign experience in the identification, collection, acquisition and preservation of potential electronic (digital) evidence is given.

The improvement of biometric systems of personal recognition is today in line with such topical areas as the development of fast neutron reactors, supercomputers and grid technologies. As a result of the military criminal Russian aggression against Ukraine, since March 2022, Ukrainian law enforcement agencies have been actively using the Clearview AI facial recognition system to check people at checkpoints and identify occupiers who are on the territory of Ukraine. The advantages and disadvantages of the specified application are given, taking into account the ambiguous attitude of European society to this development. The article focuses on such types of digital evidence as satellite images and the possibility of their use in court proceedings, since the Ukrainian criminal procedural legislation does not have clear regulations on the use of such digital information during the investigation of crimes.

Key words: digitization, digital forensics, digital sign, Berkeley protocol, Locar exchange principle, WikiLeaks, Bellingcat, Clearview AI.

Виклад основного матеріалу. Розуміння і використання новітніх технологій у контексті протидії злочинності має подвійний характер. З одного боку, сучасні технології використовуються злочинцями для вчинення кримінальних правопорушень. У цьому сенсі новітні технології входять до драйверів злочинності. З іншого боку, технології є інструментом, що дозволяє не тільки успішно боротися з кримінальними злочинами, але і запобігати їм [7].

У вітчизняній криміналістичній доктрині приділено мало уваги дослідженню цифрової криміналістики. Серед авторів, які торкаються окремих проблем цифрової криміналістики є Бутузов В. М., Власова С. В., Іщенко Є. П., Нечаєва Н. Б. тощо. Однією із провідних іноземних дослідниць цифрової криміналістики є Marie-Helen Maras.

Цифрова криміналістика – це досить нова наука, що виокремилася в 70-х рр. минулого століття як окрема галузь криміналістики й фактично стала новим кроком

у розвитку зазначеної науки. До початку XXI століття цифрова криміналістика знаходилася на стадії розвитку й значного поширення набула лише починаючи з 2000 року. Так, А.С. Колодіна та Т.С. Федорова зазначають, що цифрова криміналістика за весь період свого існування пройшла 4 етапи розвитку:

1) 1985-1995 рр. – початковий етап: застосування цифрової криміналістичної експертизи зводилося до зчитування даних внутрішніх операційних систем та апаратних засобів ПК за допомогою програмних кодів;

2) 1995-2005 рр. – поява кіберзлочинності, необхідність боротьби з нею (саме на цьому етапі з'явилася ще один поняття у криміналістиці – «розслідування кіберзлочинів»; на даний момент розслідування кіберзлочинів є одним з основних напрямків діяльності цифрової криміналістики);

3) 2005-2010 рр. – поява складних цифрових моделей розслідування злочинів (одна з найпоширеніших – «загальна модель комп'ютерних криміналістичних розслідувань»);

4) 2010-2022 рр. – активний розвиток цифрових технологій, поява нових напрямків та можливостей цифрової криміналістики у протидії організованій, транснаціональній злочинності та тероризму [5, с. 176 – 179].

Цифрова криміналістика на даний момент слугує суттєвим доповненням до традиційних методів розслідування, оскільки майже кожен суб'єкт у сучасному світі під час використання інформаційно-комунікаційних технологій залишає цифрові сліди. Механізм виникнення цифрових слідів базується на одному з основних принципів класичної криміналістики – принципі обміну Едмона Локара. Суть твердження Локара полягає в тому, що при контакті об'єктів з поверхнями відбувається перехресне перенесення матеріалів. Так і суб'єкти при контакті з всесвітньою мережею залишають в неї певний комплекс інформації: гігабайти вкладених файлів, систему пошукових запитів, IP-адреси пристроїв, історії переглядів у браузерах тощо.

Такі цифрові сліди вчені-криміналісти називають «цифровими відбитками» та поділяють їх на активні та пасивні. Так, А.С. Колодіна та Т.С. Федорова зазначають, що активний цифровий відбиток створюється даними, наданими користувачем, такими як персональні дані, відео, зображення і коментарі, що розміщуються в додатках, на вебсайтах, електронних дошках оголошень, в соціальних мережах та інших онлайн-форумах. Пасивний цифровий відбиток – це дані, які ненавмисно залишають люди, які користуються Інтернетом і цифровими технологіями (наприклад, історія переглядів в браузері, IP-адреси пристроїв, мета-дані тощо). Дані, які є частиною активних і пасивних цифрових відбитків, можуть використовуватися як доказ скоєння злочину, враховуючи кіберзлочини (тобто як цифрові докази). Такі дані можуть використовуватися для доведення або спростування твердження про факт; підтвердження або спростування показань потерпілого, свідка і підозрюваного; визначення причетності або непричетності підозрюваного до скоєного злочину [5, с. 176 – 179].

На нашу думку, у більшості випадків конкретна фізична особа може бути ідентифікована лише в тому випадку, якщо залишить активний цифровий відбиток – самостійно опублікує особисту інформацію на сайті чи в соціальних мережах.

Основним завданням цифрової криміналістики є збір, дослідження, оцінка та використання цифрових доказів під час розслідування злочинів. Термін «цифрові докази» вживається паралельно з терміном «електронні докази», оскільки розмежування цих понять не окреслено на законодавчому рівні. Електронними доказами називаються докази у кримінальних провадженнях, отримані за допомогою електронних пристроїв, комп'ютерних мереж та комп'ютерних носіїв інформації [4, с. 5].

У криміналістичній літературі цифрові докази діляться на 2 категорії. Перша – це контент (інформація, отримана безпосередньо з тексту електронних листів, повідомлень, фото, аудіо, відео з соціальних мереж), друга – мета-дані (інформація про користувачів інформаційно-комунікаційних технологій, їх геолокацію тощо).

Робота слідчих з цифровими доказами безпосередньо в досудовому розслідуванні передбачає два етапи – отримання цифрових даних та їх збереження. Кожен із етапів регламентується цілою низкою правил, що загалом зводиться до одного базового – забезпечення цілісності цифрових даних як при їх отриманні, так і протягом усього періоду слідства. Отримання цифрових даних має здійснюватися шляхом створення копії вмісту пристрою з обов'язковим використанням блокувальника запису – з метою запобігання зміні даних пристрою під час утворення дубліката. Ідентичність дубліката з оригіналом визначається за допомогою математичних обчислень. При отриманні цифрових доказів обов'язковою є детальна документація (інформація «хто, де, коли і за яких обставин отримав докази» вноситься до журналу реєстрації), що забезпечує допустимість доказів у судді та їх збереження протягом усього процесу слідства.

Цифрові докази повинні бути автентифіковані, щоб забезпечити їх допустимість в суді. У порівнянні з традиційними доказами (наприклад, паперовими документами, зброєю, контрольованими речовинами і т. д.), цифрові докази створюють унікальні складності при автентифікації через обсяг доступних даних, їх швидкості (тобто швидкості, з якою вони створюються і передаються), нестійкості (тобто вони можуть швидко зникнути при перезапису або видаленні) і вразливості (тобто їх легко можна обробити, змінити або пошкодити) [5, с. 180]. Для того, щоб уніфікувати роботу з цифровими доказами, у 2012 році Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (МЕК) опублікували міжнародні стандарти, що стосуються поводження з цифровими доказами (ISO / IEC 27037 Керівництво по ідентифікації, збирання, одержання і збереження свідчень, представлених в цифровій формі [10].

Так, закордонна практика свідчить, що в США станом на 2005 рік кількість доказів у електронному форматі вже становила 70% від загальної. А в Китаї на даний момент усі вуличні камери приєднано до застосунку, що ідентифікує обличчя й здійснює його пошук у базах [2].

Значну роль у розвитку цифрової криміналістики відіграли деякі організації. До таких організацій можна віднести WikiLeaks (засновану у 2006 році австралійцем Джуліаном Ассанжем, яка спеціалізується на публікації секретної інформації, отриманої в результаті витоків інформації, – при цьому джерела інформації не розголошуються) та Bellingcat (завдяки засновнику якої Еліота Хіггінса було підтверджено застосування забороненої зброї під час війни в Сирії) [9].

У криміналістичній практиці України за останні роки також брала участь одна з названих організацій – саме дослідники Bellingcat, проаналізувавши доступні відео та телефонні розмови, встановили причетність збройних сил Російської Федерації до авіакатастрофи Boeing-777 MH17 у Донецькій області 2014 року.

На сьогодні в Україні значного поширення набув додаток Clearview Al американської розробки (система розпізнавання облич), що в умовах повномасштабного вторгнення Російської Федерації в Україну виконує 3 основні функції: ідентифікація військових РФ, ідентифікація загиблих, перевірка осіб на контрольно-пропускних пунктах та боротьба з дезінформацією [11]. Деякі експерти (зокрема, експерт із технологій спостереження Альберт Факс Кан) стверджують, що використання Clearview Al може суперечити окремим положенням Женевської конвенції стосовно стандартів ведення війни (насамперед

ідеться про неточність ідентифікації й можливі помилки при скануванні, внаслідок чого як військові злочинці будуть ідентифіковані невинні люди). Однак розробники програми заперечують можливість таких порушень. По-перше, має застосовуватися певна процедура ідентифікації – перед ідентифікацією військові повинні вводити номер справи та причину пошуку. По-друге, при перевірках Clearview AI показала точність розпізнавання до 99,6%. Але найбільшу кількість суперечок викликає спосіб збору інформації – програма збирає дані із соціальних мереж, на що, за словами європейських регуляторів, не має правової підстави. Питання є спірним саме тому, що Clearview AI опрацьовує інформацію із соціальних мереж, тобто активний цифровий відбиток [2].

Системи збору цифрових доказів в Україні намагалися запровадити й раніше: у 2014 році подібну ініціативу намагалася запровадити прокуратура АР Криму, що зараз дислокується в Києві. Однак безпосереднього доступу до території півострова не було, тому збором цифрових доказів займалися журналісти. Цифрові докази (знімки із супутників) послугували підтвердженням збройної агресії РФ і у 2022 році. Після звільнення Бучі на вулицях було виявлено багато людських тіл. У той же час інформаційні центри РФ почали поширювати інформацію, що тіла загиблих з'явилися там уже після звільнення, щоб скомпрометувати російські війська. Однак саме завдяки супутниковим знімкам було виявлено, що люди загинули під час окупації. Таким самим способом було виявлено й масове поховання біля церкви Святого Андрія в Бучі (зафіксоване за допомогою супутникових знімків Maxar) [6].

У більшості країн, де активно використовуються засоби цифрової криміналістики, верифікація даних затверджена в нормативно-правових актах. Окрім цього, для всіх країн, що працюють у цьому напрямку, існує єдиний документ, у якому закріплено вимоги до збору та використання інформації, отриманої з відкритих джерел. Ідеться про протокол Берклі, що розроблявся Центром прав людини університету Берклі та Офісом Верховного комісара ООН з прав людини. Протокол Берклі регламентує використання цифрової інформації при розслідуванні порушень у таких галузях: право людини, гуманітарне право, міжнародне кримінальне право. При цьому варто зауважити, що протокол застосовується не тільки слідчими, він може бути використаний адвокатами та журналістами. До даних, використання яких є регламентовано за протоколом, належать: активний цифровий слід (інформація, опублікована особою на сайтах чи в соціальних мережах) та дані супутникових знімків.

На території України нормативно-правовим актом, що регулює використання цифрової інформації як з відкритих джерел, так і тієї, що міститься на цифрових носіях, є Національний стандарт України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів». У стандарті зазначено перелік джерел та носіїв інформації, щодо яких здійснюється регулювання, однак тут же вказано, що зазначений перелік наведено для прикладу й він не є вичерпним [1]. Водночас питання залучення цифрових доказів під час судового провадження в українському кримінальному законодавстві залишається відкритим, хоча у європейських судах уже досить тривалий час існує практика долучення цифрових доказів до справи. Таким чином необхідною умовою розвитку української цифрової криміналістики є наближення вітчизняних правозахисних структур до європейського рівня на законодавчому та методичному рівнях.

Отже, з огляду на зазначене, можна підкреслити важливе значення широкого застосування комп'ютерних, інформаційних, комунікаційних, цифрових, судово-експертних та інших інноваційних технологій у практиці розслідування злочинів [3, с. 46].

Висновки. У роботі опрацьовано поняття цифрової криміналістики, причини відокремлення та основні етапи її розвитку, функції (на момент виникнення та сьогодення). Також розглянуто поняття «цифрового сліду» та «цифрових доказів» (їх види та правила роботи з ними). У статті зосереджено увагу на двох міжнародних організаціях, що суттєво вплинули на розвиток цифрової криміналістики у світі: WikiLeaks та Bellingcat. Указано на роль останньої у висвітленні обставин авіакатастрофи пасажирського літака у Донецькій області 2014 року. З метою детального аналізу переваг та недоліків додатку Clearview AI опрацьовано публіцистичні джерела, де висвітлюється думка представників правничої галузі у Європі щодо додатку. Акцентовано увагу на ролі супутникових знімків як цифрових доказів та прогалинах в українському кримінально-процесуальному законодавстві (відсутність чіткої регламентації долучення таких доказів до судових справ, незважаючи на наявну європейську практику).

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. [Чинний від 2019-01-01]. Київ, 2017. 31 с.
2. Антонюк Д. Технологію розпізнавання облич Clearview AI вважають нелегальною. Навіщо вона українським військовим. *Forbes*. URL: https://forbes.ua/innovations/tekhnologiyu-rozpiznavannya-oblich-clearview-ai-vvazhayut-nelegalnoyu-i-nebezpechnoyu-ii-budut-vikoristovuvati-ukrainski-viyskovi-16032022-4696
3. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
4. Гуцалюк М., Гавловський В., Хахановський В. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / за заг. Ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.
5. Колодіна А., Федорова Т. Цифрова криміналістка: проблеми теорії і практики. *Київський часопис права.* 2022. № 4. С. 176–180.
6. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? *Погляди.* 2022. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978
7. Овчинский В. Технологии будущего против криминала. URL: http://www.books.google.com.ua/
8. Царьов Р. Онлайн-тренінг «Цифровий слід в Інтернеті». URL: https://osvita-omr.gov.ua/wp-content/uploads/2022/02/lektsyia_tsyfrovyj-slid.-ok.pdf
9. Bellingcat. LB.ua. URL: https://lb.ua/tag/16466_bellingcat
10. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html
11. Paresh D., Jeffrey D. Exclusive: Ukraine started using Clearview AI facial recognition during the war. URL: https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/
12. WikiLeaks. URL: https://wikileaks.org/