УДК 343.98.067
DOI: 10.31733/2078-3566-2023-6-282-288

Наталія БРАТІШКО©
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

НАПРЯМИ ВИКОРИСТАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В УМОВАХ ВОЄННОГО СТАНУ

У статті досліджено новітню галузь криміналістики – цифрову криміналістику. Проаналізовано погляди провідних вчених щодо поняття та місця цифрової криміналістики в системі криміналістичної науки. Здійснено аналіз техніки та розкрито сучасні методи цифрової криміналістики. Оцінено тенденції розвитку цифрової криміналістики на сучасному етапі та спрогнозовано подальший розвиток цього напряму в Україні. Проведено правовий аналіз стосовно того, що цифрова криміналістика може використовуватися в різних контекстах, включно зі внутрішніми корпоративними розслідуваннями, цивільними судовими процесами тощо. Зазначено, що існуюча модель криміналістики в Україні нагально потребує формування окремої галузі криміналістичної техніки, що включає засоби і методи дослідження цифрових доказів.

Ключові слова*: цифрова криміналістика, криміналістика, методи, розслідування, кримінальні правопорушення, кіберзлочинність, докази.*

Постановка проблеми. Поширення цифрових пристроїв та пов’язаних із ними технологій трансформує механізми вчинення багатьох кримінальних правопорушень у різних сферах людського життя. Сьогодні майже кожна людина щодня користується кількома цифровими пристроями та має доступ до різних цифрових сервісів. Відповідно, повсякденне життя генерує багато цифрових слідів, а отже, ймовірність того, що в результаті кримінального правопорушення залишаються цифрові сліди, є дуже високою. Тому кількість випадків, коли правоохоронцям необхідно виявляти та досліджувати цифрові сліди, застосовувати засоби пошуку та фіксації інформації в кіберпросторі, використовувати цифрові дані під час процесу доказування у кримінальному провадженні, з кожним роком збільшується. З огляду на це попит правоохоронних органів на ефективні інструменти для виявлення, вилучення та дослідження цифрових доказів постійно зростає, тому в криміналістичній науці останніх десятиліть цей напрям є одним із найактуальніших, і він динамічно розвивається.

На думку Т. Матюшкової, цифрова інформація, як невід’ємний атрибут сучасної злочинної й криміналістичної діяльності, визначає перспективи розвитку криміналістики, що пов’язані з оглядом як окремих елементів її системи, так і криміналістики в цілому, і перспективи подальших досліджень у цьому напрямі. Особливо з огляду на поширення теорії «комп’ютерної криміналістки» [1, с. 249]. Однак недостатньо уваги приділяється ролі та місцю цифрової криміналістики у вітчизняній моделі криміналістики. В Україні вчені зосереджуються переважно на проблемах судової експертизи комп’ютерної техніки та програмних продуктів (її об’єктах, завданнях, можливостях та методиках проведення) і на методиці розслідування кіберзлочинів. Вважаємо це неправильним, оскільки цифрова криміналістика є окремим розділом судових наук і має бути повноцінно запроваджена в Україні з урахуванням тієї моделі криміналістичної науки, що склалася.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. В Україні цифровою криміналістикою займається небагато дослідників. Це пов’язане з тим, що вона є новою наукою, що виникла лише у 80-ті роки XX століття. Окремі проблеми цифрової криміналістики розглядали такі автори, як: Г. Авдєєва, В. Бутузов, М. Думчиков, І. Когутич, А. Колодіна, Т. Матюшкова, Н.. Нечаєва, А. Самодін, Т. Федорова, В. Шепітько, М. Шепітько та ін. Варто згадати і М.-Х. Марас – одну з

k_ksmp@dduvs.in.ua

провідних іноземних дослідниць цифрової криміналістики. Однак, незважаючи на наукові дослідження, більшість теоретичних питань, пов'язаних із визначенням конкретних напрямів впровадження положень цифрової криміналістики до системи криміналістичної науки в Україні, й до цього часу залишаються невирішеними.

Метою статті є дослідження нової сфери криміналістики – цифрової криміналістки, а саме її методів, що використовуються при розслідуванні кримінальних правопорушень.

Виклад основного матеріалу. У сучасному світі інформаційні технології все більше охоплюють різні сфери суспільного життя. Можна сказати, що вони стали невід'ємним компонентом людської діяльності, що визначає перспективи розвитку економіки, політики, національної безпеки та обороноздатності держави. Сьогодні, з розвитком суспільства та процесами цифровізації всіх сфер життя, виникає потреба в удосконаленні роботи судових та правоохоронних органів, особливо в умовах модернізації та переходу до нової цифрової реальності. Адже кіберпростір є сучасним інструментом для створення та поширення різних видів інформації. Він став новим рушієм розвитку економіки, новою платформою соціального адміністрування, новим способом міжнародного співробітництва та новою сферою державного суверенітету. Однак кіберпростір не лише надає ресурси та можливості, але й пов'язаний із загрозами. Стрімкий розвиток цифровізації та видів зв'язку збільшує виклики та ризики кібербезпеки, тим самим перетворюючи суспільство в цілому на більш вразливе до кіберзагроз та продукуючи появу нових форм сучасної злочинності, таких як: інформаційне шахрайство, кібератаки на низку об'єктів критичної інфраструктури, кіберзлочини: порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення, ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів [2, с. 201]. За таких умов цифрова інформація є невід'ємним атрибутом діяльності органів кримінальної юстиції та злочинців, що, у свою чергу, впливає на розвиток суспільства та визначає напрями і завдання розвитку юриспруденції, в тому числі й криміналістики.

Варто зазначити, що запровадження воєнного стану в Україні суттєво вплинуло на розвиток криміналістичної науки, і за таких умов необхідно розробляти нові підходи у боротьбі із сучасними воєнними викликами, створювати та впроваджувати ефективні системи протидії наявним загрозам.

У воєнних реаліях сьогодення все більшої актуальності набуває ефективність розслідування сучасних злочинів, у тому числі кіберзлочинів та воєнних злочинів, за допомогою цифрових технологій. У цьому контексті можна говорити про появу нового напряму – цифрової криміналістики. Для позначення цієї галузі також використовуються інші терміни, такі як: електронна криміналістика, комп'ютерна криміналістика, криміналістика в комп'ютерних системах [3, с. 35–36].

В юридичній літературі науковці мають різні погляди на визначення цифрової криміналістики та її місця в системі криміналістичної науки. Наприклад, А. Колодіна і Т. Федорова зазначають, що цифрова криміналістика є прикладною наукою про розкриття злочинів, пов'язаних із комп'ютерною інформацією, про дослідження цифрових доказів, методів пошуку, отримання та закріплення таких доказів [4, с. 177]. Інші вчені вказують, що цифрова криміналістика – це судова наука практичного спрямування, заснована в 1970-1980-х рр., що вивчає відновлення та дослідження даних, пов'язаних із кіберзлочинністю, котрі містяться на цифрових пристроях [5, с. 290]. Деякі науковці розуміють під цифровою криміналістикою процес збору, отримання, збереження, аналізу та подання електронних доказів із метою отримання оперативно-розшукових відомостей, доказової інформації і здійснення розслідування та кримінального переслідування стосовно різних видів кримінальних правопорушень, у тому числі кіберзлочинів [6, с. 278].

Окремі провідні вчені намагаються визначити місце цифрової криміналістики в тій системі криміналістичної науки, що є загальновизнаною в Україні. Так, М. Думчиков допускає як варіанти або створення нового розділу в класичній криміналістиці, або визнання окремої науки «цифрова криміналістика», або створення окремого вчення в загальній теорії криміналістики, або модернізацію вже існуючих учень (про сліди, організацію розслідування), розділів криміналістики (скажімо, у криміналістичній

техніці з'явиться підрозділ «кібертрасологія») [7, с. 105].

В. Шепітько і М. Шепітько зазначають, що цифрову криміналістику можна вважати стратегічним напрямом розвитку криміналістичної науки та правоохоронної практики. У свою чергу, розвиток самої цифрової криміналістики відбувається за трьома основними напрямами: формування окремої наукової галузі в криміналістиці; застосування спеціальних знань при роботі з цифровими доказами; здійснення судових експертиз (переважно комп'ютерно-технічних) [8, с. 21]. У спеціалізованих джерелах наголошується на необхідності дослідження так званих цифрових доказів (цифрової інформації) – інформації, створеної за допомогою високих інформаційних технологій. У зарубіжних країнах широкого застосування набув термін digital evidences (цифрові докази), під яким розуміють будь-які збережені дані або дані, що передають із використанням комп'ютерної чи іншої техніки. Цифрові докази – це фактичні дані, представлені в цифровій формі та зафіксовані на носії будь-якого типу. Поряд із терміном «цифрові докази» використовуються інші, такі як: «електронні докази», «електронні сліди», «електронні документи», «цифрові джерела інформації» та ін.

Цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні. Заслуговують на увагу розробки українських науковців щодо методик розслідування злочинів, скоєних у кіберпросторі, їхньої криміналістичної характеристики, визначення алгоритму розслідування, а також специфіки використання спеціальних знань та проведення судових експертиз під час розслідування цієї категорії кримінальних правопорушень.

Проаналізувавши наукові визначення поняття «цифрова криміналістика», можна констатувати, що воно потребує подальшого розвитку у напрямі конкретизації, але отримати уявлення про нього можна вже сьогодні. У цілому, цифрова криміналістика базується на загальних принципах. Одним із найважливіших є принцип обміну, розроблений Е. Локаром: коли об'єкти і поверхні вступають в контакт одне з одним, відбувається перехресне перенесення матеріалів.

Цифрова криміналістика вирішує такі завдання: створення методів, апаратних і програмних інструментів для збору та дослідження доказів комп'ютерних злочинів; розробка тактико-оперативно-розшукових заходів та слідчих дій, пов'язаних із комп'ютерною інформацією; встановлення криміналістичних характеристик правопорушень, пов'язаних із комп'ютерною інформацією.

Основою цифрової криміналістики є її технічна складова, інакше кажучи, засоби і методи техніко-криміналістичного дослідження цифрових доказів. Ця галузь характеризується широким інструментарієм, як комерційним, так і з відкритим кодом. Вона має власний міжнародний стандарт, опублікований у 2012 р. Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (МЕК). Згаданий стандарт стосується поводження з цифровими доказами (ISO/IEC 27037 Інформаційні технології – Методи безпеки – Керівництво з ідентифікації, збирання, одержання і збереження свідчень, представлених у цифровій формі) [9]. Він пропонує такі чотири етапи поводження з цифровими доказами:

1. Ідентифікація – передбачає пошук і розпізнання відповідних доказів та їх документування. На цьому етапі пріоритетні завдання збору доказів визначаються на основі цінності й мінливості доказів. Варто звернути увагу, що ідентифікація виступає важливим кроком у процесі цифрової криміналістики, тому що це лише частина більшого, складнішого процесу розслідування;

2. Збирання – передбачає збір усіх необхідних електронних даних із різних джерел, зараховуючи комп'ютери, сервери, мобільні пристрої та інші цифрові носії. Дані збираються за допомогою спеціальних інструментів і методів, що гарантують збереження цілісності та автентичності даних;

3. Отримання. Цифрові докази мають бути отримані без порушення цілісності даних. Для цього робиться копія вмісту цифрового пристрою (процес, відомий як створення неспотвореного образу) з використанням пристрою (блокувальника запису), призначеного для того, щоб гарантувати, що дані не будуть змінені під час процесу копіювання. Для того, щоб визначити, чи є дублікат точною копією оригіналу, значення хеш-функції розраховується з використанням математичних обчислень; у такому випадку для отримання значення хеш-функції використовується криптографічна хеш-функція. Якщо значення хеш-функції для оригіналу та копії збігаються, це означає, що

вміст копії точно відповідає оригіналу;

4. Збереження. Цей етап передбачає захист і збереження електронних доказів, щоб запобігти будь-яким змінам або модифікаціям даних. Процес збереження передбачає створення судово-медичного зображення або копії вихідних даних і збереження копії, щоб забезпечити її незмінність протягом усього розслідування.

Сьогодні все більшого наукового та практичного інтересу набувають цифрові криміналістичні інструменти, що допомагають розкривати та розслідувати воєнні злочини, а також сприяють забезпеченню невідворотності покарання воєнних злочинців. Із-поміж них основну увагу приділяють таким: пошук за ключовими словами та хештегами, списки яких заздалегідь підготовлено, аналіз супутникових знімків, використання технології аналізу «великих даних» (Big Data); аналіз геолокаційних міток, дослідження фото- та відеоматеріалів у відкритому доступі та наданих слідству, використання програмного забезпечення для аналізу та обробки цифрових зображень, дослідження телефонних розмов, аналіз електронних пристроїв, ігрових систем, систем розпізнавання осіб, пошук у відповідних базах даних (в Україні використовують додаток із розпізнавання облич Clearview Af для ідентифікації потенційних злочинців і загиблих) [10, с. 32].

Інші джерела виділяють такі напрями сучасної цифрової криміналістики: 1) дослідження застосунків (месенджерів та інших застосунків для смартфонів, що використовуються для обміну інформацією); 2) дослідження хмарних сховищ; 3) дослідження мобільних пристроїв (телефонів); 4) дослідження інтернет-речей (IoT); 5) дослідження новітніх пристроїв та застосунків (Alexa від Amazon, Google Assistant, Siri від Appel); 6) дослідження мереж; 7) цифровий аналіз поведінки окремих осіб, груп людей та їхніх стосунків і взаємовідносин; 8) дослідження застосунків, що не призначені для використання іншими особами; 9) мережеві дослідження; 10) цифровий аналіз поведінки окремих осіб, груп людей та їхніх стосунків і зв'язків; 11) дослідження застосунків не для телефону (дослідження баз даних, Spotlight, America online instant messaging, засобів антикриміналістики, видалених і фрагментованих файлів, зображень, флеш-пам'яті, криптовалют); 12) цифрова криміналістична розвідка та розвідка на основі відкритих джерел.

Залежно від об'єкта інструменти та методи цифрової криміналістики поділяються на певні категорії, зокрема, дослідження файлової системи, операційної системи, оперативної пам'яті, електронної пошти, вебдослідження, мережеві дослідження, мультимедійні дослідження тощо (дослідження месенджерів, знімних носіїв) [11, с. 29].

Незважаючи на те що цифрова криміналістика стрімко розвивається та протидіє поширенню кіберзлочинності, вона має певні недоліки, зокрема: слідчі та дізнавачі повинні мати широкі комп'ютерні навички; навіть якщо цифрові докази прийнято до суду, необхідно довести, що не було жодного втручання; необхідно надавати достовірні та переконливі докази; виготовлення і зберігання електронних записів потребують значних витрат; відсутність технічних знань у слідчого, дізнавача може призвести до недосягнення бажаного результату; якщо інструмент, що використовується для цифрової судової експертизи, не відповідає зазначеним стандартам, докази можуть бути відхилені судом.

Також не важко помітити, що ця галузь є насамперед техніко-криміналістичною. Але, на відміну від багатьох інших галузей криміналістичної техніки, вона не обмежується лише технічними аспектами. Останніми роками було докладено значних зусиль для інтеграції технічних аспектів дослідження цифрових доказів до всього процесу виявлення та розслідування кіберзлочинів. Це було зроблено з метою розробки цілісних підходів до розслідування, оскільки специфіка процесу доказування кіберзлочинів вимагає участі спеціаліста на всіх етапах розслідування, а не лише під час проведення однієї чи кількох слідчих (розшукових) дій або судової експертизи.

У контексті розслідування кримінальних правопорушень вищенаведене означає, що засоби та методи цифрової криміналістики широко застосовуються в оперативно-розшуковій діяльності для виявлення ознак кримінального правопорушення, на стадії досудового розслідування – при підготовці та проведенні гласних і негласних слідчих (розшукових) дій, пов'язаних зі збором цифрових доказів, у судовій експертизі комп'ютерної техніки й програмних продуктів та інших експертизах, що досліджують цифрові докази.

Цифрову криміналістику нерідко використовують для розслідування

кіберзлочинів, таких як хакерство, крадіжка особистих даних, шахрайство. Щоб ідентифікувати злочинця і побудувати справу проти нього, можна проаналізувати цифрові докази, наприклад, електронні листи, журнали чатів і мережеві журнали. Варто зазначити, що цифрова криміналістика все частіше використовується в різних контекстах, зокрема у: 1) корпоративних розслідуваннях: компанії можуть використовувати цифрову криміналістику для розслідування порушень внутрішньої безпеки або неправомірної поведінки співробітників. Це може передбачати, наприклад, аналіз комп'ютерних журналів або електронної пошти, щоб визначити, чи порушив працівник політику компанії або викрав конфіденційну інформацію; 2) цивільних судових процесах: у цивільних справах цифрову криміналістику можна використовувати для збору доказів на підтримку або спростування претензій. Наприклад, у справах про крадіжку інтелектуальної власності судово-медичні експерти можуть проаналізувати комп'ютерні системи, щоб визначити, чи був отриманий доступ до комерційної таємниці або іншої конфіденційної інформації; 3) реагуванні на інцидент: коли відбувається порушення безпеки або кібератака, цифрова криміналістика може бути використана для розслідування інциденту та визначення джерела атаки. Потім цю інформацію можна використовувати для вдосконалення заходів безпеки та запобігання подібним інцидентам у майбутньому; 4) встановленні відповідності нормативним вимогам. Багато галузей, таких як охорона здоров'я та фінанси, підпадають під дію нормативних вимог. Цифрова криміналістика може бути використана, щоб переконатися, що ці правила дотримуються та електронні записи зберігаються й захищаються належною мірою [12, с. 478].

Загалом цифрова криміналістика є універсальним інструментом, котрий можна використовувати в різних контекстах для виявлення цінної інформації та підтримки розслідувань, судових процесів і зусиль щодо відповідності. Для розслідування цифрових інцидентів і виявлення осіб, відповідальних за кіберзлочини або витік даних, процес цифрової криміналістики має вирішальне значення.

На сучасному етапі основним напрямом розвитку криміналістики є формування та вдосконалення галузі техніко-криміналістичного дослідження цифрових даних. Як виявляється, відповідні засоби та методи ще не знайшли свого місця у вітчизняній системі криміналістики. Тому існує нагальна потреба у створенні окремого розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів, зміст якого включатиме наукові положення цифрової криміналістики як галузі судових наук, адаптованої до реалій вітчизняної правоохоронної практики та криміналістичної теорії.

Слід зазначити, що цифрову криміналістику не слід ототожнювати із застосуванням цифрових технологій у криміналістиці, з методиками розслідування кримінальних правопорушень, пов'язаних із комп'ютерною інформацією, або визначати її окремою частиною вітчизняної моделі криміналістики як прикладної юридичної науки та навчальної дисципліни. Цифрова криміналістика є галуззю іншої моделі, відмінною від тієї, що склалася в Україні, тому проблема їх інтеграції потребує подальших наукових досліджень.

Висновки. Підсумовуючи вищезазначене, можна констатувати, що цифрова криміналістика – це новітня галузь криміналістики, прикладна наука про розкриття кримінальних правопорушень, пов'язаних із комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання та закріплення таких доказів. Процес цифрової криміналістики має фундаментальне значення для розслідування цифрових інцидентів та виявлення осіб, відповідальних за кіберзлочини або витоки даних. Наразі необхідно актуалізувати розвиток цифрової криміналістики в сучасних умовах. Особливу увагу слід приділити посиленню ролі криміналістичної дидактики, зокрема підготовці слідчих, дізнавачів, прокурорів, судів, детективів, слідчих криміналістів та судових експертів у сфері цифрових технологій. Доволі актуальним нині є започаткування нової професії та здійснення підготовки цифрового криміналіста. У такому контексті сучасна парадигма криміналістики має бути спрямована на подальший розвиток і формування цифрової криміналістики для ефективного вирішення нових завдань в умовах воєнного стану та процесів цифровізації суспільства.

Список використаних джерел

1. Матюшкова Т. П. Електронна (цифрова) інформація: сучасний стан і перспективи розвитку криміналістики. *Актуальні проблеми кримінального процесу та криміналістики : тези доп. Міжнар. наук.-практ. конф.* (м. Харків, 29 жовт. 2021 р.). Харків : ХНУВС, 2021. С. 248–250.

2. Тютченко С. М., Братішко Н. А. Правове забезпечення кіберзахисту в Україні. *Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VI Міжнар. наук.-практ. конф.* (м. Дніпро, 11 бер. 2022 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. С. 201–202.

3. Шевчук В. М. Цифрова криміналістика: воєнні виклики сьогодення та нові завдання в сучасних умовах. *Правові виклики сучасності : матеріали всеукр. круглого столу* (м. Харків, 20 груд. 2022 р.). Харків : Державний біотехнологічний університет, 2022. С. 35–39.

4. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права.* 2022. Вип. 1. С. 176–180.

5. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2022. № 3(99). С. 283–294.

6. Самодін А. В. Сучасне розуміння феномену «цифрова криміналістика». *Інновації в криміналістиці та судовій експертизі : матеріали міжвідом. наук.-практ. конф.* (м. Київ, 25 листоп. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 275–279.

7. Думчиков М. О. Процеси діджиталізації і криміналістика: ректроспективний аналіз. *Криміналістика і судова експертиза.* 2020. Вип. 65. С. 100–108.

8. Шепітько В. Ю., Шепітько М. В. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 2021. № 8. С. 12–27.

9. 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.

10. Латиш К. В. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika.* 2022. Т. 18. С. 31–37.

11. Полотай О. І. Комп'ютерна криміналістика: основні завдання та проблеми. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : Міжнар. наук. інтернет-конф.* (м. Тернопіль, 7-8 черв. 2022 р.). Тернопіль, 2022. Вип. 68. С. 29–30.

12. Кашуба Н. М. Використання цифрової криміналістики в різних контекстах. *Scientific paradigm in the context of technologies and society development : proceedings of the 5th International scientific and practical conference* (Geneva, Switzerland, May 16-18, 2023). Geneva, Switzerland. 2023. № 154. С. 476–479.

Надійшла до редакції 04.12.2023

References

1. Matiushkova, T. P. (2021) Elektronna (tsyfrova) informatsiia: suchasnyi stan i perspektyvy rozvytku kryminalistyky [Electronic (digital) information: current state and prospects of development of criminalistic]. *Aktualni problemy kryminalnoho protsesu ta krymi nalistyky : tezy dop. Mizhnar. nauk.-prakt. konf.* (m. Kharkiv, 29 zhovt. 2021 r.). Kharkiv : KhNUVS, pp. 248–250. [in Ukr.].

2. Tiutchenko, S., Bratishko, N. (2022) Pravove zabezpechennia kiberzakhystu v Ukraini [Legal provision of cyber protection in Ukraine]. *Mizhnarodna ta natsionalna bezpeka: teoretychni i prykladni aspekty : materialy VI Mizhnar. nauk.-prakt. konf.* (m. Dnipro, 11 ber. 2022 r.). Dnipro : Dniprop. derzh. un-t vnutr. sprav, pp. 201–202. [in Ukr.].

3. Shevchuk, V. M. (2022) Tsyfrova kryminalistyka: voienni vyklyky sohodennia ta novi zavdannia v suchasnykh umovakh [Digital forensics: military challenges of today and new tasks in modern conditions]. *Pravovi vyklyky suchasnosti : materialy vseukrainskoho kruhloho stolu* (m. Kharkiv, 20 hrud. 2022 r.). Kharkiv : Derzhavnyi biotekhnolohichnyi universytet, pp. 35–39. [in Ukr.].

4. Kolodina, A. S., Fedorova, T. S. (2022) Tsyfrova kryminalistyka: problemy teorii i praktyky [Digital forensics: problems of theory and practice]. *Kyivskyi chasopys prava.* Issue 1, pp. 176–180. [in Ukr.].

5. Stepaniuk, R. L., Perlin, S. I. (2022) Tsyfrova kryminalistyka y udoskonalennia systemy kryminalistychnoi tekhniky v Ukraini [Digital forensics and improvement of the forensic technology system in Ukraine]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka*. № 3(99), pp. 283–294. [in Ukr.].

6. Samodin, A. V. (2021) Suchasne rozuminnia fenomenu «tsyfrova kryminalistyka» [Modern understanding of the phenomenon of «digital forensics»]. *Innovatsii v kryminalistytsi ta sudovii ekspertyzi : materialy mizhvidom. nauk.-prakt. konf.* (m. Kyiv, 25 lyst. 2021 r.). Kyiv : Nats. akad. vnutr. sprav, pp. 275–279. [in Ukr.].

7. Dumchykov, M. O. (2020) Protsesy didzhytalizatsii i kryminalistyka: rektrospektyvnyi analiz [Processes of digitization and forensics: a retrospective analysis]. *Kryminalistyka i sudova ekspertyza*. Issue 65, pp. 100–108. [in Ukr.].

8. Shepitko, V., Shepitko, M. (2021) Doktryna kryminalistyky ta sudovoi ekspertyzy: formuvannia, suchasnyi stan i rozvytok v Ukraini [Doctrine of criminology and forensic examination: formation, current state and development in Ukraine]. *Pravo Ukrainy.* № 8, pp. 12–27. [in Ukr.].

9. 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.

10. Latysh, K. (2022) Tsyfrova kryminalistyka u period viiny v Ukraini: mozhlyvosti vykorystannia spetsialnykh znan u sferi informatsiinykh tekhnolohii [Digital forensics during the war in Ukraine: possibilities of using special knowledge in the field of information technologies]. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika.* T. 18, pp. 31–37. [in Ukr.].

11. Polotai, O. I. (2022) Kompiuterna kryminalistyka: osnovni zavdannia ta problemy [Computer forensics: main tasks and problems]. *Informatsiine suspilstvo: tekhnolohichni, ekonomichni ta tekhnichni aspekty stanovlennia : mizhnar. nauk. konf.* (m. Ternopil, 7-8 cherv. 2022 r.). Ternopil. Vyp. 68, pp. 29–30. [in Ukr.].

12. Kashuba, N. M. (2023) Vykorystannia tsyfrovoi kryminalistyky v riznykh kontekstakh [Use of digital forensics in different contexts]. *Scientific paradigm in the context of technologies and society development : proceedings of the 5th International scientific and practical conference* (Geneva, Switzerland, May 16-18, 2023). Geneva, Switzerland. № 154, pp. 476–479. [in Ukr.].

ABSTRACT

Natalia Bratishko. Directions of use of digital forensics under martial law. The article examines the newest branch of forensic science – digital forensics, which is an applied science of solving crimes related to computer information, the study of digital evidence, methods of searching, obtaining and securing such evidence.

The views of leading scholars on the concept and place of digital forensics in the system of forensic science are analyzed. The author analyzes the technique and modern methods of digital forensics in the investigation of criminal offenses. The author assesses the current trends in the development of digital forensics and predicts its further development in Ukraine.

The author provides a legal analysis of the fact that digital forensics can be used in various contexts, including internal corporate investigations, civil litigation, etc. This involves the use of specialized tools and methods to obtain information from a wide range of digital devices, such as computers, mobile phones and storage media.

It is noted that in the existing model of forensic science in Ukraine, there is an urgent need to form a separate branch of forensic technology, which includes means and methods of digital evidence examination. This greatly simplifies the task of integrating the achievements of digital forensics into the national forensic system, since, on the one hand, it does not require revision of the system itself, and on the other hand, it allows for the rapid implementation of most of the relevant scientific provisions and practical recommendations. The content of the section of forensic technique devoted to the forensic examination of digital evidence should include scientific provisions of digital forensics as a branch of forensic science adapted to the realities of domestic law enforcement practice and forensic theory.

Keywords: *digital forensics, criminalistics, methods, investigation, criminal offenses, cybercrime, evidence.*

УДК 343.98
DOI: 10.31733/2078-3566-2023-6-288-296

Діана ГАРАЩУК©
ад'юнкт
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

ОСОБЛИВОСТІ ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПРИ РОЗСЛІДУВАННІ НЕЗАКОННОГО ЗАЙНЯТТЯ РИБНИМ ДОБУВНИМ ПРОМИСЛОМ У ВОЄННИЙ ЧАС

Досліджено особливості проведення слідчих (розшукових) дій при розслідуванні незаконного зайняття рибним добувним промислом у воєнний час. Розглядаються теоретичні засади і тактичні особливості проведення огляду місця події, обшуку, допиту свідка та підозрюваного під час розслідування вказаних кримінальних правопорушень.

Акцентовано увагу, що в умовах воєнного стану проведення деяких слідчих (розшукових) дій набуло певних особливостей, зокрема у частині складання протоколу, а також щодо спрощення процедури залучення понятих при проведені обшуку житла чи іншого володіння особи.

© Д. Гаращук, 2023
k_ksmp@dduvs.in.ua