DOI: 10.34015/2523-4552.2025.3.20
УДК 343.982.9

Степанюк Р. Л.,
доктор юридичних наук, професор, професор кафедри оперативно-розшукової діяльності та розкриття злочинів Харківського національного університету внутрішніх справ
ORCID: 0000-0002-3567-8538

ЦИФРОВА КРИМІНАЛІСТИКА ТА ЇЇ ЗНАЧЕННЯ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У статті визначено основні напрями використання засобів цифрової криміналістики у процесі виявлення та розслідування кримінальних правопорушень. Наголошено, що сутність цифрової криміналістики є науково-технічною. Тому у вітчизняній моделі криміналістичної науки її варто розглядати як самостійний розділ криміналістичної техніки, який вивчає цифрові сліди кримінальних правопорушень і розробляє інструменти та методи їх дослідження. Комплексний підхід до вивчення системи інструментів і методів цифрової криміналістики дає можливість визначити чотири основні напрями її використання під час розкриття та розслідування кримінальних правопорушень. Першим напрямом є цифрова криміналістична розвідка, яка є новітньою сферою діяльності правоохоронних органів і передбачає використання спеціалізованих сервісів для пошуку й аналізу інформації з великої кількості джерел. Цей напрям потребує системного дослідження на рівні криміналістичної теорії та формування якісних правових, організаційних і методичних засад. Другий напрям – це техніко-криміналістичне забезпечення виявлення та вилучення цифрових доказів під час проведення процесуальних дій. Він передбачає обов'язкову участь спеціаліста у галузі цифрової криміналістики та професійне використання її інструментів і методів. Судова комп'ютерно-технічна експертиза, яка є основним напрямом використання засобів цифрової криміналістики в судово-експертній діяльності, потребує подальшого розвитку в контексті удосконалення класифікації об'єктів та розроблення сучасних методів дослідження. Ще одним напрямом є техніко-криміналістичне забезпечення розслідування кіберзлочинів. Він передбачає використання інструментів і методів цифрової криміналістики для виявлення та дослідження цифрових доказів у певних кримінальних провадженнях, а також дотримання наукових рекомендацій щодо процесу розслідування кіберзлочинів. Усі наведені вище напрями пов'язані між собою. Але вони відрізняються за формою використання спеціальних знань, завданнями та способами їх вирішення, а також кінцевими результатами.

Ключові слова: *криміналістична техніка, криміналістична тактика, цифрова криміналістика, розслідування кіберзлочинів, кримінальний аналіз, огляд комп'ютерних даних, судова комп'ютерно-технічна експертиза.*

Постановка проблеми. Все більшого значення у розкритті та розслідуванні кримінальних правопорушень набувають засоби цифрової криміналістики. Повсюдне поширення інформаційних технологій у суспільстві призвело до того, що різні категорії злочинів дедалі частіше залишають цифрові сліди, виявлення та дослідження яких є запорукою успіху в розслідуванні. Зважаючи на гострі потреби правоохоронних органів та постійне збільшення реальних можливостей техніко-криміналістичного дослідження цифрових слідів, галузь цифрової криміналістики бурхливо розвивається в останні десятиліття. Впроваджуються програмні та апаратні засоби, які дозволяють здійснювати пошук і аналіз інформації у великих масивах даних, на різних типах пристроїв та електронних ресурсах. Інструменти цифрової криміналістики стають незамінними засобами виявлення і дослідження комп'ютерних даних як доказів. За їх допомогою розкривають і розслідують не тільки кримінальні правопорушення у сфері використання комп'ютерів та комп'ютерних мереж, а і багато інших протиправних діянь, таких як терористичні акти, вбивства, грабежі та розбої, шахрайства тощо. В умовах масштабного військового конфлікту в Україні ці інструменти демонструють високу ефективність також і у протидії воєнним злочинам та іншим кримінальним правопорушенням, що пов'язані з війною.

У вітчизняній моделі системи науки криміналістики поки що не сформовано єдиного уявлення про місце в ній цифрової криміналістики та про сутність і структуру цього розділу. Систематизація напрямів зазначеної галузі судових наук є надзвичайно проблемною, а слабке теоретичне опрацювання цих питань у традиціях «криміналістики Ганса Гроса» додає невизначеності ключовим аспектам їх вирішення. В таких умовах актуальним науковим завданням видається відображення сутності та створення логічно побудованої системи цифрової криміналістики в контексті класичної моделі криміналістичної науки та сучасних потреб правозастосовної практики.

Аналіз останніх досліджень і публікацій. У вітчизняних наукових публікаціях досліджувалась сутність цифрової криміналістики як новітнього напряму розвитку криміналістичної науки (І. І. Когутич, В. Ю. Шепітько, В. М. Шевчук, М. В. Шепітько, І. В. Гора, В. А. Колесник, І. І. Попович та ін.) та як галузі криміналістичної техніки (Р. Л. Степанюк, С. І. Перлін, А. В. Коваленко, А. І. Черемнова та ін.). Також науковцями було систематизовано основні інструменти цифрової криміналістики, які використовують у практиці правоохоронних органів та судово-експертних установ (В. А. Поліщук, О. В. Неня, С. М. Корнійко, А. В. Гуляєв, Н. М. Березненко, О. С. Омельян, Р. Л. Степанюк, В. Г. Колесник, та ін.) і розкрито особливості використання спеціальних знань у галузі комп'ютерних технологій у розслідуванні кримінальних правопорушень (О. А. Самойленко, В. Г. Хахановський, О. В. Одерій, О. А. Кожевніков, М. В. Гуцалюк, В. Д. Гавловський, С. В. Самойлов та ін.). Разом із цим систематизація основних напрямів використання інструментів і методів цифрової криміналістики у правоохоронній діяль-

ності потребує подальшого наукового аналізу.

Постановка завдання. Метою статті є визначення основних напрямів використання засобів цифрової криміналістики як новітньої галузі дослідження цифрових слідів (доказів) із метою виявлення та розслідування кримінальних правопорушень.

Виклад основного матеріалу. Цифрова криміналістика як галузь судових наук виникла в середині 1970-х років і з того часу пройшла шлях активного розвитку від розроблення методів відновлення видалених даних до впровадження потужних інструментів виявлення, збереження та дослідження цифрових слідів (доказів) кримінальних правопорушень.

За широко представленою точкою зору вітчизняних науковців, цифрова криміналістика є новітнім напрямом розвитку криміналістичної науки і практики [1, с. 21; 2, с. 81-82]. При цьому, як підкреслили І. В. Гора, В. А. Колесник та І. І. Попович, її слід розглядати як сучасний і важливий для розвитку як загальних положень криміналістичної науки, так і для її усталених розділів – криміналістичної техніки, тактики й методики напрям, а не як окрему науку кримінально-правового циклу або ж окремий і самостійний розділ традиційної криміналістики [3, с. 91]. Проте, як видається, такий підхід не визначає конкретного місця цифрової криміналістики в системі криміналістичної науки. Більше того, він призводить до певної плутанини у розумінні співвідношення сфери реалізації новітніх її досягнень, зокрема в системі криміналістики в цілому та як її окремих теорій або напрямів розвитку. Погоджуючись із тим, що на статус окремої науки, а тим більше кримінально-правового циклу, зазначена галузь не претендує, зауважимо, що її характеристика виключно як напряму в розвитку криміналістики майже не враховує, а отже дещо нівелює, її технікокриміналістичну сутність.

Вважаємо, що в традиційній для нас системі криміналістичної науки цифрова криміналістика як раз є науково-технічним розділом, а використання її рекомендацій у тактиці проведення процесуальних дій чи методиці розслідування окремих видів злочинів не повинно призводити до втрати основного змісту. У криміналістичній теорії варто розрізняти цифровізацію криміналістики, тобто впровадження цифрових технологій у різні її галузі (напрям розвитку науки), окремі криміналістичні вчення, зокрема про використання цифрових технологій у розслідуванні злочинів, про судову комп'ютерно-технічну експертизу тощо (окремі криміналістичні теорії) та цифрову криміналістику як галузь криміналістичної техніки (елемент структури науки криміналістики).

Зважаючи на вищевказане, нам видається оптимальним інший підхід до визначення цифрової криміналістики. А саме, її варто розглядати як «галузь криміналістичної техніки, яка досліджує закономірності й механізм утворення цифрових (електронних) слідів і розробляє методи, прийоми й науково-технічні засоби їх виявлення, вилучення і дослідження під час розкриття та розслідування кримінальних правопорушень» [4, с. 112] або в іншій інтерпретації як галузь, «яка займаєть-

ся вивченням закономірностей виникнення і використання цифрових слідів та розроблення на знанні цих закономірностей технічних засобів, прийомів та методів щодо виявлення, фіксації, вилучення та дослідження цифрової інформації (доказів) й засобів її оброблення з метою розкриття, розслідування та профілактики кримінальних правопорушень» [5, с. 36]. Такий спосіб інтеграції досягнень цифрової криміналістики враховує усталені в нашій країні уявлення про сутність, завдання і систему криміналістичної науки і при цьому відображає сутність та основне завдання цифрової криміналістики, яким є забезпечення достовірності цифрових доказів завдяки використанню науково-обґрунтованих методів їх виявлення, вилучення та дослідження.

Варто зауважити, що науковцями представлені й інші підходи до цієї проблеми. Наприклад, І. В. Лущик та А. С. Тяпкін вважають, що цифрова криміналістика не є окремою галуззю криміналістики. «Коректніше говорити про криміналістику злочинів у цифровому просторі. Цифрова криміналістика займається відновленням та дослідженням матеріалів, виявлених у цифрових пристроях, пов’язаних з кіберзлочинністю. Цифрова криміналістика – це процес виявлення, збереження, аналізу та документування цифрових доказів» [6, с. 152]. Як видається, такий підхід, який фактично полягає у розгляді цифрової криміналістики як сукупності процедур (процесу) практичної діяльності, не повинен призводити до заперечення її ж як складової частини науки. Адже фактично всі галузі криміналістики та її окремих розділів знаходять своє вираження у відповідних практичних діях (процедурах), тому багато криміналістичних наукових категорій визначають і як процес практичної діяльності, і як сукупність відповідних наукових положень.

Як і будь-який інший розділ криміналістичної техніки, цифрова криміналістика повинна вміщувати теоретичні знання та практичні рекомендації щодо об’єктів, які вона вивчає (в даному випадку цифрові сліди в інфраструктурі кіберпростору), технологій їх аналізу (виявлення, фіксації, дослідження) з метою вирішення завдань з розкриття, розслідування та попередження кримінальних правопорушень.

Практична реалізація досягнень цифрової криміналістики напряму залежить від інструментарію, оскільки часто потребує аналізу величезних масивів інформації. У практиці правоохоронних органів та судово-експертних установ використовують низку апаратних і програмних технічних засобів, що дозволяє вирішувати широкий спектр слідчих і експертних завдань. Є різні підходи до систематизації таких засобів. При цьому як класифікаційні підстави прийнято використовувати характеристики самих засобів (програмні, апаратні, програмно-апаратні, послуги, універсальні, спеціалізовані тощо), об’єкти та цілі дослідження (персональні комп’ютери, мережі, мобільні пристрої, хмарні сховища, інтернет-речі, криптовалюти тощо) [7, 8, с. 288-289]. Але варто зауважити, що слідчі, спеціалісти й експерти у певних ситуаціях застосовують засоби з різних класифікаційних груп для комплексного вирішення типових тактичних завдань розслідування. Тобто крім класифікації інструментів

і методів цифрової криміналістики важливо систематизувати типові напрями їх використання в інтересах кримінального провадження.

А. І. Черемнова пропонує виокремити два таких напрями: 1) збирання та фіксація цифрової інформації з різноманітних носіїв (зі стаціонарних пристроїв та переносних носіїв); 2) дослідження цифрової інформації (на комп'ютерних пристроях, на носіях цифрової інформації та у хмарних сховищах, у т.ч. соціальних мережах) [9, с. 60-61]. Такий розподіл, що здійснений на основі діяльнісного підходу, є цілком логічним, тому що робота з цифровими слідами включає два основні етапи – збір та аналіз. При цьому на етапі збирання найважливішим завданням є забезпечення цілісності комп'ютерних даних задля забезпечення подальшої судової перспективи їх використання як доказів. У свою чергу аналіз масиву даних дозволяє отримати саме ту інформацію, яка має значення для розслідування. Проте необхідність пошуку та збереження цифрових слідів у великих масивах даних і захищених пристроях, що найчастіше має місце у практиці, потребує комплексного підходу як щодо їх збирання та фіксації, так і щодо аналізу. Тому, як видається, до підстав систематизації напрямів використання засобів цифрової криміналістики потрібно додати сферу їх реалізації, тобто ту сукупність умов, середовище, де здійснюється відповідна діяльність.

Сфера реалізації засобів цифрової криміналістики в діяльності правоохоронних органів насамперед залежать від суб'єктів та відповідно мети, правових та організаційних засад їхньої діяльності. Наразі в практичній діяльності прокурорів, слідчих, працівників оперативних підрозділів, спеціалістів та експертів найбільш актуальними видаються чотири основні напрями, де активно застосовують засоби цифрової криміналістики: цифрова криміналістична розвідка, техніко-криміналістичне забезпечення виявлення та вилучення цифрових доказів під час проведення процесуальних дій, судова комп'ютерно-технічна експертиза і техніко-криміналістичне забезпечення розслідування кіберзлочинів. Ці напрями тісно пов'язані між собою, тому що у практиці кожного з них можуть бути присутніми елементи іншого. Наприклад, окремі заходи в межах цифрової криміналістичної розвідки можуть включати проведення огляду, методика розслідування кіберзлочинів вміщує рекомендації з проведення пошуково-аналітичних заходів, процесуальних дій, призначення судових експертиз тощо. Але вони відрізняються насамперед за формою використання спеціальних знань, способами виконання завдань і підсумковими результатами. Тому диференціація кожного напряму та їх характеристика є вагомими для системного розуміння ролі цифрової криміналістики в криміналістичній теорії та формування якісних рекомендацій для практики.

Цифрова криміналістична розвідка в практичній площині зараз переважно реалізується у межах проведення кримінального аналізу за конкретними кримінальними провадженнями профільними підрозділами правоохоронних органів, а щодо аналізу відкритих джерел (OSINT) також і громадськими організаціями, спільнотами журналістів,

окремими ентузіастами тощо, які спеціалізуються на цій діяльності. Водночас системного бачення зазначеного напряму на рівні криміналістичної теорії ще не вироблено. Бракує також і правової бази, внаслідок чого пошук цифрових слідів правоохоронними органами із використанням інструментів і методів тактичного кримінального аналізу здійснюється в організаційній (непроцесуальній) формі. Ця діяльність не регламентована КПК України, а науковцями цифрова криміналістична розвідка розглядається як категорія оперативно-розшукової діяльності [10] або криміналістичної тактики [11].

Цифрова криміналістична розвідка демонструє надзвичайно високу ефективність у виявленні, попередженні, розкритті та розслідуванні кримінальних правопорушень. Зокрема правоохоронці активно використовують спеціалізовані сервіси аналізу відкритих джерел (OSINT), пошуку за державними і міжнародними базами даних, блокчейн-аналізу, географічного профілювання тощо. Можливості цього напряму постійно зростають разом зі діджиталізацією суспільного життя й активним розвитком різноманітних інформаційних мереж та баз даних. Аналітична розвідка у кіберсередовищі дає можливість відшукувати цінну для кримінального провадження інформацію у величезному її обсязі та будувати зв'язки між різними подіями, особами та речами. Тому відповідна проблематика потребує більшої уваги з боку криміналістів.

Техніко-криміналістичне забезпечення виявлення та вилучення цифрових доказів під час проведення процесуальних дій, на відміну від цифрової криміналістичної розвідки, здійснюється у процесуальній формі та повною мірою передбачає використання засобів цифрової криміналістики насамперед задля забезпечення допустимості отриманих фактичних даних як доказів у кримінальному провадженні. Серед слідчих дій у першу чергу це огляд, обшук, зняття інформації з електронних інформаційних систем, зняття інформації з електронних комунікаційних мереж та інші, де здійснюються фактичні дії, спрямовані безпосередньо на пошук і фіксацію цифрових слідів.

Складність проведення огляду цифрового середовища та окремих пристроїв завжди потребує специфічних навичок у особи, яка його проводить. Ця обставина активізувала дискусію в криміналістиці щодо ролі та значення участі спеціаліста у процесуальних діях. За класичного підходу, прийнятого в теорії кримінального процесу і криміналістики та закріпленого в кримінальному процесуальному законодавстві, процесуальні дії проводить слідчій. Спеціаліст може бути залучений для надання технічної допомоги. Його участь не є обов'язковою, а залежить від рішення слідчого. Проте науковці, які досліджують проблематику цифрової криміналістики та розслідування комп'ютерних злочинів, досить давно звернули увагу на складність поєднання у однієї особи знань правових і технічних процедур роботи з цифровими доказами. При цьому юристи-практики розуміють важливість ознайомлення з методами цифрової криміналістики, але вважають, що зрозуміти та виконувати технічні процедури дуже важко

[12, с. 30]. Тому гостро постало питання об'єднання зусиль правознавців і фахівців у галузі інформаційних технологій у розслідуванні.

Зазначений аспект зумовив формування цілком слушної думки про те, що під час проведення слідчого огляду для виявлення, фіксації та збереження доказів в електронній (цифровій) формі участь спеціаліста у галузі цифрової криміналістики є обов'язковою [13, с. 63]. Його участь і неухильне дотримання рекомендацій щодо роботи цифровими доказами є умовою забезпечення їх достовірності [14, с. 235-236].

Новацією КПК України стало закріплення окремого різновиду слідчого огляду, а саме огляду комп'ютерних даних. Як наслідок, наразі збирання електронних (цифрових) доказів у кримінальних провадженнях найчастіше здійснюється шляхом проведення огляду комп'ютерних даних в порядку ст. 237 КПК України, який може виконуватись як самостійна слідча (розшукова) дія, а може поєднуватись з оглядом комп'ютерної техніки, мобільних телефонів [15, с. 351]. При цьому у ст. 168 КПК України передбачено, що копіювання інформації з інформаційних (автоматизованих) систем, електронних комунікаційних систем, інформаційно-комунікаційних систем, комп'ютерних систем здійснюється із залученням спеціаліста [16].

Обрання технічних засобів огляду залежить від об'єкта дослідження. Наразі виробниками спеціалізованого обладнання цифрової криміналістики запропоновано низку інструментів, які дозоляють здійснювати пошук і аналіз цифрових доказів (FTK imager, Magnet AXIOM, Oxygen Forensic KeyScout, Celebrate Digital Collector, Magnet RAM Capture, Volatility 3, Celebrate UFED, Oxigen Forensic Detective, Passware Kit Mobile тощо). Використання таких засобів спеціалістами сприяє швидкому та якісному виконанню завдань, що виникають в ході проведення процесуальної дії.

Специфіка вилучення інформації з соціальних мереж, відеохостингів та інших онлайн-платформ полягає в урахуванні вимог «Протоколу Берклі» – набору міжнародних керівних принципів збору й аналізу даних з відкритих джерел інтернету для розслідування кримінальних правопорушень у сфері прав людини та гуманітарного права. Ця настанова було розроблена фахівцями школи права Університету Каліфорнії в Берклі у співпраці з представниками ООН та іншими експертами. Дотримання зазначеного протоколу на стадії огляду забезпечується виконанням алгоритму дій щодо виявлення, збирання та збереження цифрової інформації з відкритих джерел.

Таким чином під час проведення процесуальних дій, пов'язаних із оглядом (виявленням, вилученням і позаекспертним дослідженням) цифрових слідів, обов'язковою є участь спеціаліста у галузі цифрової криміналістики та професійне використання її інструментів і методів.

Судова комп'ютерно-технічна експертиза як напрям використання засобів цифрової криміналістики також є процесуальною формою використання спеціальних знань, сутність якої полягає у проведенні експертом самостійного дослідження та формуванні висновку експерта як окремого джерела доказів.

Комп'ютерно-технічна експертиза є основною з числа судових експертиз, які передбачають використання засобів цифрової криміналістики. Вона відноситься до класу інженерно-технічних експертиз. Свого часу з неї як самостійний вид експертизи було виокремлено експертизу електронних комунікацій (телекомунікаційних систем і засобів) [17, с. 76]. Крім того, вона нерідко проводиться комплексно з експертизою звуко-, відеозапису, фототехнічною, судово-мистецтвознавчою та іншими експертизами, де теж виникають питання, пов'язані із необхідністю дослідження цифрових доказів [18, с. 293]. Систему комп'ютерно-технічних досліджень в Україні досі остаточно не сформовано, оскільки швидкий розвиток цифрових технологій випереджає теоретично обґрунтовані та закріплені в нормативно-правових актах з питань судово-експертної діяльності підходи до класифікації об'єктів дослідження.

Під час проведення комп'ютерно-технічної експертизи вирішують питання, що стосуються працездатності комп'ютерної техніки, наявності та змісту певних файлів, програмного забезпечення та його функціонального призначення, облікових даних користувача, його активності, змісту спілкування в месенджерах тощо. При цьому експерти в основному використовують ті ж інструменти цифрової криміналістики, що і спеціалісти під час огляду. Це універсальні програмні та апаратно-програмні засоби (X-Ways Forensics, AccessData Forensic Toolkit, Magnet AXIOM, UFED 4PC та ін.), пристрої апаратного блокування запису (Tableau Forensic Bridge, Digital Intelligence UltraBlock) та виготовлення побітових копій (Tableau Forensic Duplicator TD3, IM Solo-4), засоби для дослідження мобільних пристроїв (Cellebrite UFED, Oxygen Forensic Detective), програми для відновлення видалених даних (UFS Explorer Professional Recovery, R-Studio та ін.) [18, с. 297]. Арсенал об'єктів комп'ютерно-технічної експертизи та інструментів цифрової криміналістики постійно розширюється разом зі сферою застосування цифрових технологій. Наприклад, зараз в Україні в умовах широкомасштабних бойових дій значно збільшилась кількість надходження на експертизу електронних компонентів безпілотних літальних апаратів. Як і в усьому світі все більш актуальними стають дослідження Інтернет-речей, новітніх цифрових пристроїв і додатків тощо. Таким чином можна прогнозувати подальший активний розвиток галузі цифрової криміналістики в цілому та сфер її використання в судовій експертизі зокрема.

Техніко-криміналістичне забезпечення розслідування кіберзлочинів як напрям використання засобів цифрової криміналістики стосується галузі криміналістичної методики. Тому тут важливим є поєднання досягнень усіх розділів криміналістики щодо їх застосування під час розслідування окремої групи кримінальних правопорушень, які відносяться до категорії кіберзлочинів.

У науках кримінально-правового циклу поняття кіберзлочинів є доволі дискусійним і передбачає принаймні широкий та вузький підходи, де до першого відносять протиправні посягання, у яких комп'ютер є об'єктом або засобом посягання, а до другої, де об'єктом посягання є комп'ютерна інформа-

ція, а засобом вчинення комп'ютер. Але в цілому, до таких злочинів відносять ті, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж [19, с. 44]. Не вдаючись до детального аналізу цієї проблеми, відзначимо думку О.А. Самойленко, що вітчизняні криміналісти тривалий час розробляли методики розслідування та засоби протидії окремих видів кіберзлочинів у розумінні Конвенції про кіберзлочинність (Будапештської конвенції), окремі положення якої вже не відповідають умовам часу. Проте зараз концептуальним у криміналістичній науці стає визнання кіберпростору середовищем злочинної діяльності й одночасно об'єктом криміналістичних досліджень [20, с. 134]. А отже, криміналістичні методики розслідування кіберзлочинів стосуються різних за кримінально-правовою ознакою кримінальних правопорушень, які вчиняються у специфічному середовищі – кіберпросторі. Виявлення та дослідження слідів таких кримінальних правопорушень передбачає широке використання інструментів і методів цифрової криміналістики, а також дотримання рекомендацій технічного, тактичного і методичного характеру щодо розслідування кіберінцидентів.

Висновки. Сутність цифрової криміналістики є науково-технічною, а отже у вітчизняній моделі криміналістичної науки повинна знайти чітке відображення, зокрема в умовах широкого використання інформаційних технологій в усіх її галузях. У зв'язку з цим цифрову криміналістику варто розглядати як самостійний розділ криміналістичної техніки, який вивчає цифрові сліди кримінальних правопорушень і розробляє інструменти та методи їх дослідження.

Комплексний підхід щодо дослідження сутності цифрової криміналістики та системи її інструментів і методів, що використовуються під час розкриття та розслідування кримінальних правопорушень, дає можливість визначити, що на цей час основними є чотири напрями.

1. Цифрова криміналістична розвідка, яка є новітньою сферою діяльності правоохоронних органів і передбачає використання спеціалізованих інструментів для пошуку й аналізу інформації з великої кількості джерел. Цей напрям потребує системного дослідження на рівні криміналістичної теорії та формування якісних правових, організаційних і методичних засад.

2. Техніко-криміналістичне забезпечення виявлення та вилучення цифрових доказів під час проведення процесуальних дій, що передбачає обов'язкову участь спеціаліста у галузі цифрової криміналістики та професійне використання її інструментів і методів.

3. Судова комп'ютерно-технічна експертиза, яка є основним напрямом використання засобів цифрової криміналістики в судово-експертній діяльності та потребує подальшого розвитку в контексті удосконалення класифікації об'єктів та розроблення сучасних методів дослідження.

4. Техніко-криміналістичне забезпечення розслідування кіберзлочинів, що передбачає використання інструментів і методів цифрової криміналістики для виявлення та дослідження цифрових доказів у певних кримінальних провадженнях, а

також дотримання рекомендацій технічного, тактичного і методичного характеру щодо процесу розслідування кіберінциндентів, які мають кримінально-протиправний характер.

Вищенаведені елементи пов'язані між собою, але відрізняються за формою використання спеціальних знань, завданнями та способами їх вирішення, а також кінцевими результатами. Формування теоретичних засад напрямів розвитку цифрової криміналістики та вдосконалення практичних рекомендацій з використання її досягнень у правозастосовній діяльності є перспективами подальших наукових досліджень.

Список використаних джерел

1. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України*. 2021. № 8. С. 12–27. DOI: 10.33498/louu-2021-08-012.
2. Когутич І. І. Застосування цифрових технологій – новий напрям криміналістики. *Наукові читання пам'яті Ганса Гросса*: *збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.).* Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79–84.
3. 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. https://doi.org/10.32782/2307-1745.2024.68.18
4. Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. 388 с.
5. Шевчук В. М. Цифрова криміналістика: воєнні виклики та нові завдання у сучасних умовах. *Правові виклики сучасності: Матеріали круглого столу (20 грудня 2022 р.)*. Харків : Державний біотехнологічний університет, 2022. С. 35–39.
6. Tiapkin A., Lushchyk I. Problematic Issues of Definition of Digital Forensics. *Theory and Practice of Jurisprudence.* 2024. Vol. 1 (23). P. 135–161. DOI: https://doi.org/10.21564/2225-6555.2023.23.281734.
7. Reedy P. Interpol review of digital evidence 2016-2019. *Forensic Science International: Synergy*. 2020. № 2. P. 489–520. DOI: https://doi.org/10.1016/j.fsisyn.2020.01.015
8. 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. 283–284. DOI: 10.33766/2524-0323.99.283-294
9. Черемнова А. І. Цифрова криміналістика як складова криміналістичної техніки: сучасний стан та перспективи розвитку. *Вісник ОНДІСЕ*. 2024. Вип. 16. С. 56–63. DOI: https://doi.org/10.32782/2522-9656/2024-16-6
10. Козицька О. Г. Кіберрозвідка як новітній напрям оперативно-розшукової діяльності. *Науковий процес та наукові підходи: методика та реалізація досліджень: матеріали Міжнар. наук. конф. (Одеса, 23 жовт. 2020 р.).* Одеса : МЦНД, 2020. С. 107–109.
11. Степанюк Р. Л. Розвідка у криміналістиці й оперативно-розшуковій діяльності. *Вісник Луганського навчально-наукового інституту ім. Е. О. Дідоренка*. 2024. Вип. 2 (106) Ч.1. С. 191–203. DOI:10.33766/2786-9156.106.1.191-203.

12. Ricci S. C. Ieong. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. 2006. Vol. 3. P. 29–36. DOI:10.1016/j.diin.2006.06.004.

13. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ.* 2020. Вип. 2. С. 58–68. doi: https://doi.org/10.33270/01201152.58

14. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства.* 2019. Вип. 3. С. 224-238. DOI:10.17721/2413-5372.2019.3/224-238

15. Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. *Вісник кримінологічної асоціації України*. 2024. № 2 (32). С. 344–353. DOI: 10.32631/vca.2024.2.25

16. Кримінальний процесуальний кодекс України : Закон України від13.04.2012 No 4651-VI. *Вебпортал Верховна Рада України. Законодавство України*. URL: http://zakon.rada.gov.ua/laws/show/ 4651-17

17. Лапта С. П. Щодо предмета експертизи телекомунікаційних систем і засобів. *Вісник Харківського національного університету внутрішніх справ*. 2011. № 3 (54). С. 75–79.

18. Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Луганського державного університету внутрішніх справ імені ЕО Дідоренка.* 2023. № 2 (102). С. 289–305. DOI: 10.33766/2524-0323.102.289-305

19. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора, О. М. Литвака (м. Харків, 23 квіт. 2020 р.)* / МВС України, Харків. нац. ун-т внутр. справ; Кримінол. асоц. України. Харків : ХНУВС, 2020. С. 44–45.

20. Самойленко О. А. Протидія кримінальним правопорушенням, учиненим у кіберпросторі, як новий напрям криміналістики. *Право України*. 2021. № 8. С. 131–141. DOI: 10.33498/louu-2021-08-131

***Stepaniuk Ruslan**, Doctor of Law, Professor, Professor of the Department of Operational and Investigative Activity and Crime Solution of Kharkiv National University of Internal Affairs*

ORCID: 0000-0002-3567-8538

Digital Forensics and its Importance in Investigating Criminal Offences

The article defines the main areas of application of digital forensics in the process of detecting and investigating criminal offences. It is emphasised that the essence of digital forensics is scientific and technical. Therefore, in the domestic model of forensic science, it should be considered as an independent branch of criminalistic technique that studies digital traces of criminal offences and develops tools and methods for their investigation. A comprehensive approach to studying the system of tools and methods of digital forensics makes it possible to identify four main areas of its use in the detection and investigation of criminal

offences. The first area is digital forensic intelligence, which is a new field of activity for law enforcement agencies and involves the use of specialised tools to search for and analyse information from a large number of sources. This area requires systematic research at the level of forensic theory and the formation of high-quality legal, organisational and methodological foundations. The second area is scientific and technical support for the identification and seizure of digital evidence during procedural actions. It requires the mandatory participation of a specialist in the field of digital forensics and the professional use of its tools and methods. Forensic computer-technical expertise, which is the main area of application of digital forensics in forensic activities, requires further development in the context of improving the classification of objects and developing modern research methods. Another area is technical and forensic support for cybercrime investigations. It involves the use of digital forensics tools and methods to identify and examine digital evidence in specific criminal proceedings, as well as compliance with scientific recommendations on the cybercrime investigation process. All of the above areas are interrelated. However, they differ in terms of the form of application of specialised knowledge, the tasks and methods used to solve them, and the final results.

Keywords: *criminalistic technique, criminalistic tactics, digital forensics, cybercrime investigation, criminal analysis, computer data examination, forensic computer technical expertise.*