УДК 343.982.9
DOI https://doi.org/10.32782/2307-1745.2025.77.16

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

Перлін В. С.,
кандидат юридичних наук,
співробітник Інституту Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого
ORCID: https://orcid.org/0009-0002-7516-2429

ФОРМИ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У ГАЛУЗІ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Анотація. У статті визначено форми використання спеціальних знань у галузі цифрової криміналістики у сфері кримінальної процесуальної діяльності та надано їх коротку характеристику. Наголошено, що значне розширення технічних можливостей виявлення та вилучення цифрових слідів кримінальних правопорушень потребує удосконалення форми використання у кримінальному провадженні спеціальних знань у галузі цифрової криміналістики та розроблення дієвих рекомендацій щодо її практичної реалізації. Наразі процесуальна форма виявляється у залученні відповідних спеціалістів і експертів до участі в кримінальному провадженні, а непроцесуальна – у проведенні цифрової криміналістичної розвідки в рамках кримінального аналізу. Залучення спеціаліста з цифрової криміналістики до проведення слідчих (розшукових) дій, пов'язаних із копіюванням комп'ютерних даних, є обов'язковим, що насамперед зумовлено необхідністю вилучення та збереження цифрових доказів у незмінному стані. Для цього спеціалісти застосовують спеціалізовані інструменти цифрової криміналістики та відповідні методи з урахуванням специфіки об'єктів дослідження. У свою чергу, грамотне вилучення об'єктів під час приведення процесуальних дій є належною умовою для призначення судової комп'ютерно-технічної експертизи, яка досліджує технічний стан комп'ютерних засобів і мереж, а також безпосередньо комп'ютерні дані, вирішуючи завдання, що виникли під час досудового розслідування та судового розгляду. При цьому комп'ютерно-технічна експертиза може проводитись комплексно із іншими, що особливо часто реалізується у зв'язку з дослідженням цифрових аудіо-, відеозаписів. Цифрова криміналістична розвідка є новою формою використання спеціальних знань у кримінальному провадженні, яка не має належного процесуально-правового регулювання і здійснюється переважно на організаційних засадах. Формування єдиної термінології за цим напрямом, а також розроблення нормативно-правових основ здійснення криміналістичної розвідки у кіберпросторі є перспективними напрямами подальших наукових досліджень.

Ключові слова: кримінальне провадження, слідчі (розшукові) дії, експерт, спеціаліст, цифрова криміналістика, цифрові докази, кримінальна розвідка, кримінальний аналіз.

Постановка проблеми. Повсюдне впровадження цифрових технологій у життя людини призвело до значного масштабування завдань правоохоронних органів, пов'язаних із необхідністю виявляти та досліджувати цифрові сліди кримінальних правопорушень. Сьогодні практично кожна особа користується цифровими пристроями. В електронну сферу перейшла значна частка торгівлі та надання різноманітних послуг, активно розвиваються інформаційні системи органів державної влади і місцевого самоврядування, розширюється використання електронних грошей, тощо. В таких умовах все більше злочинців залишають цифрові сліди, а кіберпростір стає одним із ключових сфер застосування криміналістичних інструментів і методів.

Наукову галузь, яка вивчає цифрові сліди злочинів та розробляє засоби їх дослідження, називають цифровою криміналістикою. Затребуваність фахівців з цієї галузі в процесі розкриття та розслідування кримінальних правопорушень постійно зростає. Очевидною видається також і необхідність підвищення рівня обізнаності щодо інструментів і методів цифрової криміналістики у суддів, прокурорів, слідчих та оперативних працівників. Разом з цим у криміналістичній теорії поки що недостатньо вивченими є питання щодо сутності та змісту цифрової криміналістики. Бракує систематизованих методико-криміналістичних рекомендацій, де розглянуто особливості використання різних форм спеціальних знань у цій галузі безпосередньо в процесі досудового розслідування кримінальних правопорушень і судового розгляду кримінальних справ. Наслідком цього є суттєві труднощі, які виникають у практичній діяльності, а також прогалини в науковій теорії та дидактичному забезпеченні навчання працівників правоохоронних органів.

Зазначені обставини засвідчують потребу наукового узагальнення та розроблення теоретичних засад і практичних рекомендацій щодо залучення спеціалістів і експертів у галузі цифрової криміналістики до розслідування кримінальних правопорушень та використанні ними найбільш ефективних інструментів і методів дослідження цифрових доказів.

Стан дослідження. Сутність цифрової криміналістики та її місце в системі криміналістичної науки досліджували І.І. Когутич, В.Ю. Шепітько, М.В. Шепітько, І.В, Гора, В.А. Колес-

ник, І.І. Попович, А.С. Колодіна, Т.С. Федорова, Р.Л. Степанюк, С.І. Перлін та інші вітчизняні науковці, які окреслили власне бачення шляхів вирішення зазначеної проблеми. У свою чергу В.М. Шевчук, В.В. Білоус, К.В. Латиш, А.І. Черемнова та ін. зосередили увагу на основних завданнях, які вирішує цифрова криміналістика, зокрема в умовах війни, О.В. Манжай, В.Г. Хахановський, О.П. Метелев, Б.В. Черняховський, О.В. Курман, Є.С. Хижняк, А.В. Коваленко та ін. – на правилах проведення огляду цифрових доказів, а В.П. Харківський, Б.Б. Теплицький, Д.Є. Гавриленко, М.М. Войтович, В.Г. Колесник, М.П. Климчук, Ю.А. Комісарчук та ін. – на проблематиці призначення і проведення судової комп'ютерно-технічної експертизи у кримінальному провадженні. Разом із цим систематизація форм використання спеціальних знань у галузі цифрової криміналістики ще не знайшла належного теоретичного опрацювання, що заважає формуванню дієвих науково-методичних рекомендацій комплексного характеру.

Мета. Метою дослідження є визначення форм використання спеціальних знань у галузі цифрової криміналістики у сфері кримінальної процесуальної діяльності та їх коротка характеристика в контексті сутності, співвідношення між собою, аспектів практичної реалізації та окреслення перспектив подальшого розвитку.

Виклад основного матеріалу. Як відомо, у кримінальному процесі використання спеціальних знань здійснюється у процесуальній та організаційній (непроцесуальній) формах. Перша регламентована безпосередньо у КПК України, а друга визначена у підзаконних актах або вироблена в практичній діяльності. Відповідно процесуальна форма виражається у залученні спеціалістів до проведення слідчих (розшукових) дій та залученні експертів (призначенні судових експертиз), а непроцесуальна передбачає одержання письмових або усних консультацій та довідкової інформації від фахівців з питань, які мають значення для розслідування.

Таким чином, процесуальна форма використання спеціальних знань з цифрової криміналістики виражається в участі спеціаліста з інформаційних технологій у проведенні таких слідчих (розшукових) дій як огляд, обшук, зняття інформації з електронних інформаційних систем, зняття інформації з електронних комунікаційних мереж та ін., а також у проведенні експертом комп'ютерно-технічної експертизи. У свою чергу організаційна форма насамперед виражається в отриманні письмових звітів від аналітичних підрозділів за результатами проведеної цифрової криміналістичної розвідки.

Специфіка *залучення спеціаліста до проведення окремих слідчих (розшукових) дій* насамперед полягає в обов'язковості такого кроку у випадку копіювання комп'ютерних даних, що зазначено у ст. 168 КПК України. Зазначена вимога закону є невипадковою і зумовлена необхідністю збереження цифрових доказів у незмінному стані, що можна зробити лише за умови грамотного використання інструментів цифрової криміналістики, при чому, які вірно наголошено А.В, Коваленком, суто за допомогою сертифікованого та справного службового обладнання, з використанням ліцензійного програмного забезпечення [1, с. 55]. Це виконується шляхом зняття побітової копії (образу) носія цифрової інформації. Подальші дії здійснюють лише з копією, не допускаючи таким чином змін на самому пристрої. Образ комп'ютера спеціалісти знімають із використанням комплексів, які блокують запис, дозволяючи лише читання. Важливо відзначити, що частина цифрових слідів може знаходиться в оперативній пам'яті комп'ютера (RAM). Такі дані зберігаються тимчасово для виконання й обробки програм, поки комп'ютер працює. Вони втрачаються при вимкненні пристрою. Тому вилучення таких слідів можливо лише спеціалістом, який спроможний виконати відповідні завдання, у тому числі забезпечивши правильне підключення пристрою до спеціальних технічних засобів.

Якщо об'єктом огляду є мобільні пристрої (телефони, планшети), невідкладні заходи щодо збереження цифрових слідів полягають у застосуванні алгоритму, який полягає у підтриманні ввімкненого режиму пристрою при одночасному блокуванні можливості внесення змін шляхом віддаленого доступу. Деталізація невідкладних дій під час огляду насамперед залежить від стану блокування пристрою. Беззаперечним пріоритетом є забезпечення його розблокування. Надалі пристрій переводиться у «режим польоту», після чого у його налаштуваннях дисплею та меню налаштувань безпеки встановлюються параметри: «Вимикання екрану» – «ніколи», «Блокування екрану/режим очікування» – «ніколи», яскравість екрану виставляється в мінімум з метою збільшення строку збереження заряду батареї, телефон під'єднується до зовнішнього носія живлення (power bank) та упаковується у пакет, блокуючий радіохвилі. Таким чином, екран не буде гаснути, пристрій буде знаходитись постійно у розблокованому стані та може вільно оглядатись до розряджання всіх джерел живлення [2, с. 296]. При вилученні заблокованого пристрою також потрібно дотримуватись вищенаведеного алгоритму щодо підтримання його у ввімкненому стані та недопущення віддаленого доступу.

Важливі цифрові докази можуть міститись не тільки безпосередньо у пристрої, але й у віддалених сховищах. Виявлення таких даних під час огляду вимагає використання спеціальних знань та інструментів цифрової криміналістики і фактично здійснюється шляхом виявлення й аналізу кешу мобільних застосунків, резервних копій, вебдоступу із захопленням активної сесії.

Вилучення цифрових доказів з відкритих джерел інтернету варто здійснювати із дотриманням вимог Протоколу Берклі – практичного посібника, який містить положення щодо методології та процедури збору, аналізу та збереження цифрової інформації у професійному (юридичному) та етичному аспектах [3, с. 94]. Незважаючи на те, що протокол Берклі не має обов'язкової юридичної сили, викладені в ньому стандарти та рекомендації є орієнтиром для представників правоохоронних органів держав світу в процесі здійснення розслідування з використанням відкритих цифрових даних, їх дотримання сприятиме точності та надійності зібраних доказів, зменшує вірогідність визнання доказів неприйнятними [4, с. 172]. Методичні рекомендації з проведення огляду цифрових матеріалів з відкритих джерел з урахуванням протоколу Берклі передбачають дотримання певного алгоритму, який наведений науковцями [5, с. 246–247].

Ще однією процесуальною формою використання спеціальних знань у галузі цифрової криміналістики у кримінальному провадженні є *залучення експерта у галузі судової комп'ютерно-технічної експертизи*. Основні завдання цієї експертизи пов'язані з встановленням технічного стану (працездатності) комп'ютерної техніки, виявленням цифрової інформації, у тому числі видаленої, пошуком цифрових доказів мережевої актив-

ності користувача та аналізом його дій, аналізом програмного забезпечення тощо [2, с. 294]. До виду комп'ютерно-технічної експертизи відносять декілька підвидів, зокрема дослідження комп'ютерної техніки, дослідження програмних продуктів, інформаційно-комп'ютерну експертизу [6, с. 32] та комп'ютерно-мережеву експертизу [7, с. 37-38], хоча систему комп'ютерно-технічних досліджень остаточно не сформовано [8, с. 98]. Тому варто відзначити, що експертні дослідження цифрової інформації в окремих випадках здійснюють не тільки судові експерти у галузі комп'ютерно-технічної експертизи, а і деякі інші. Широке використання цифрової техніки майже в усіх сферах життя людини, в тому числі й у механізмах злочинної діяльності, призвело до потреби застосовувати засоби і методи цифрової криміналістики під час проведення різних видів судових експертиз. Зокрема, з комп'ютерно-технічною експертизою можуть бути пов'язані дослідження, які аналізують електронні дані [9].

Зв'язок інших досліджень із комп'ютерно-технічними може проявлятись у різній мірі. Це роздільне дослідження тих самих об'єктів, коли у кримінальному провадженні слідчий послідовно призначає комплекс експертиз, визначивши черговість їх проведення, або комплексна експертиза, коли дослідження проводяться експертами з різних спеціальностей спільно. Прикладами окремого вирішення завдань, є проведення технічної експертизи документів щодо матеріальних документів, виготовлених за допомогою комп'ютерних засобів, та ідентифікації самих засобів, експертизи електронних комунікацій щодо визначення типу і стану мереж і засобів електронних комунікацій і т.п. У свою чергу, комплексна експертиза призначається у випадках, коли проведення дослідження різними експертами не є можливим, оскільки поставлені завдання заходяться на стику різних галузей спеціальних знань і можуть бути вирішеними тільки спільними зусиллями. У судовій експертизі експертні дослідження комплексного характеру набувають все більшого значення, адже надійність висновків щодо об'єкта, вивченого взаємопов'язано з позицій різних наук, якісно зростає [10, с. 4]. Це повною мірою стосується експертних досліджень комп'ютерної техніки і комп'ютерних даних й особливо часто проявляється у практиці досліджень матеріалів цифрового відео-, звукозапису.

У призначенні комп'ютерно-технічної експертизи важливою є якісна підготовка її об'єктів та грамотне формулювання завдань експерту.

Підготовка об'єктів насамперед здійснюється шляхом проведення процесуальних дій, спрямованих на вилучення та попередній аналіз цифрових слідів та їх носіїв. Як слушно відзначено, особливості вилучення об'єктів комп'ютерно-технічного дослідження полягають у тому, що зловмисники, нерідко намагаються застосувати заходи «контркриміналістики» [11, с. 64]. Якщо додати до цього таку загальну властивість цифрових слідів, як простота видозмінення з одного боку та можливість повного відтворення шляхом копіювання з іншого, стає очевидним, що правильне вилучення та збереження об'єктів дослідження є запорукою успішного проведення комп'ютерно-технічної експертизи. Такими об'єктами переважно є комп'ютерні дані (цифрові докази) та їх носії, а основні проблеми пов'язані із постійним розвитком систем апаратного та програмного захисту інформації та збільшенням розміру даних.

Щодо формулювання питань експерту вирішальне значення мають обставини події, що розслідується, та потреби кримінального провадження в їх з'ясуванні. Орієнтовні переліки таких питань містяться у профільних науково-методичних рекомендаціях, які, тим не менш, не можуть охопити всі можливі ситуації практичної діяльності. Тому важливо підкреслити, що запропоновані у різних джерелах переліки запитань є орієнтовними. Вони можуть бути уточнені як стосовно певних різновидів злочинів, так і у конкретному кримінальному провадженні. Тому у зв'язку з широким спектром завдань, які можуть виникнути під час розслідування, та варіативністю ситуацій практичної діяльності сформувати повний перелік рекомендованих питань експерту не уявляється можливим. У складних випадках слідчому варто звернутись до співробітників установ судової експертизи для отримання консультацій з приводу їх оптимального формулювання.

У постанові про призначення комп'ютерно-технічної експертизи потрібно вказувати інформацію про наявність або відсутність даних про паролі доступу до об'єктів дослідження. Якщо паролі невідомі, то доцільно надати дозвіл експерту на застосування руйнуючих методів, необхідних для подолання системи логічного захисту.

Під час проведення досліджень експерти застосовують спеціалізовані апаратні засоби та програмне забезпечення, асортимент яких на ринку є солідним. Науковцями відзначено критичну залежність судової експертизи від відповідних інструментів, без яких неможливий аналіз цифрових пристроїв [12]. Тому кожна експертна лабораторія повинна мати відповідне обладнання, програмне забезпечення, підтримувати його у дієвому стані та періодично оновлювати.

В аспекті методичного забезпечення комп'ютерно-технічної експертизи з одного боку спостерігається суттєва кількість офіційно затверджених експертних методик, але з іншого існують і деякі проблемні питання. Зважаючи на постійний розвиток комп'ютерної індустрії слушно зауважено, що рівень науково-методичного забезпечення комп'ютерно-технічної експертизи потребує постійного вдосконалення [13, с. 9], а отже, експертні методики динамічно розвиваються.

Цифрова криміналістична розвідка, на відміну від залучення спеціалістів і експертів, наразі здійснюється переважно як напрям оперативного кримінального аналізу, а отже, може розглядатись лише як непроцесуальна форма використання спеціальних знань у галузі цифрової криміналістики. При цьому варто наголосити на відсутності загальновизнаної термінології в цій сфері та належного теоретичного обґрунтування сутності таких понять, як кримінальний аналіз, цифрова кримінальна/криміналістична розвідка тощо та їх співвідношення із цифровою криміналістикою. Ми не претендуємо на остаточне вирішення цих питань, а лише наголошуємо, що сучасні технології пошуку цифрових доказів у кіберсередовищі демонструють високу практичну ефективність і безумовно потребують ґрунтовних наукових досліджень.

Можливості цифрової розвідки постійно зростають разом зі діджиталізацією суспільного життя та 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. Проте ця діяльність до цього часу в КПК України не

регламентована. Науковцями кіберрозвідка розглядається як категорія оперативно-розшукової діяльності [14] або як засіб криміналістичної тактики [15]. У практичній площині вона реалізується переважно на організаційних засадах. Як видається, таке становище не можна визнати задовільним. Потрібно визначити єдину термінологію в теорії кримінального процесу та криміналістики, вдосконалити правове регулювання процедури застосування засобів цифрової розвідки та процесуального оформлення її результатів.

Висновки. Значне розширення технічних можливостей виявлення та вилучення цифрових слідів кримінальних правопорушень потребує удосконалення форми використання у кримінальному провадженні спеціальних знань у галузі цифрової криміналістики та розроблення дієвих рекомендацій щодо її практичної реалізації. Наразі процесуальна форма виявляється у залученні відповідних спеціалістів і експертів до участі в кримінальному провадженні, а непроцесуальна – у проведенні цифрової криміналістичної розвідки в рамках кримінального аналізу.

Залучення спеціаліста з цифрової криміналістики до проведення слідчих (розшукових) дій, пов'язаних із копіюванням комп'ютерних даних, є обов'язковим, що насамперед зумовлено необхідністю вилучення та збереження цифрових доказів у незмінному стані. Для цього спеціалісти застосовують спеціалізовані інструменти цифрової криміналістики та відповідні методи з урахуванням специфіки об'єктів дослідження. У свою чергу, грамотне вилучення об'єктів під час приведення процесуальних дій є належною умовою для призначення судової комп'ютерно-технічної експертизи, яка досліджує технічний стан комп'ютерних засобів і мереж, а також безпосередньо комп'ютерні дані, вирішуючи завдання, що виникли під час досудового розслідування та судового розгляду. При цьому комп'ютерно-технічна експертиза може проводитись комплексно із іншими, що особливо часто реалізується у зв'язку з дослідженням цифрових аудіо-, відеозаписів.

Цифрова криміналістична розвідка є новою формою використання спеціальних знань у кримінальному провадженні, яка не має належного процесуально-правового регулювання і здійснюється переважно на організаційних засадах. Формування єдиної термінології за цим напрямом, а також розроблення нормативно-правових основ здійснення криміналістичної розвідки у кіберпросторі є перспективними напрямами подальших наукових досліджень.

Література:

1. Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2023. Вип. 4. С. 53–58.
2. Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2023. № 2(102). С. 289–305. https://doi.org/10.33766/2524-0323.102.289-305.
3. Подкопаєв С. Протокол Берклі як методологічна основа проведення розслідувань з використанням відкритих цифрових даних. Collection of Scientific Papers «SCIENTIA», (May 6, 2022; Vilnius, Lithuania). Vilnius, 2022. P. 94–95. URL: https://previous.scientia.report/index.php/archive/article/view/172
4. Бабаєва О. В., Авербах Д. В. Щодо питання про використання доказів, отриманих з відкритих джерел, у кримінальному провадженні. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 3(83). С. 169–174.
5. Гаврилюк Л., Бурлака В., Пелехатий В. Особливості огляду цифрових матеріалів з відкритих джерел мережі «інтернет» за протоколом Берклі. *Наука і правоохорона*. 2024. Вип. 2(64). С. 238–250.
6. Теплицький Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2021). Вип. 120 (3). С. 28–34.
7. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навчальний посібник / Климчук М. П., Комиссарчук Ю. А., Марко С. І., Стецик Б. В. Львів : Львівський державний університет внутрішніх справ, 2022.112 с.
8. Харківський П. П. Комп'ютерно-технічна експертиза: проблемні питання. *Криміналістичний вісник*. 2014. Вип. 2 (22). С. 97–100.
9. Гавриленко Д. Є., Войтович М. М. Комплексний характер судової комп'ютерно-технічної експертизи та її зв'язок з іншими родами та видами судових експертиз. Судово-експертна діяльність: сучасний стан та перспективи розвитку: збірник матеріалів круглого столу. / редкол.: Кобилянський О.Л., Антонюк П.Є., Свобода Є.Ю.; Київ. ННІПФЕКП НАВС. К. : Навчально-науковий інститут підготовки фахівців для експертно-криміналістичних підрозділів Національної академії внутрішніх справ, 2015. С. 94–97.
10. Гончаренко В. Г. Організаційні та правові проблеми судової експертизи в Україні. *Часопис Академії адвокатури України*. 2011. Вип. 4 (10) Ч. 1. С. 1–4.
11. Нізовцев Ю., Омельян О. Щодо підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень пов'язаних із кібератаками. *Криміналістичний вісник*. 2021. Вип. 36 (2). С. 59–68. https://doi.org/10.37025/1992-4437/2021-36-2-59.
12. Horsman G. «I couldn't find it your honour, it mustn't be there!» –Tool errors, tool limitations and user error in digital forensics. *Science & Justice*. 2018. V. 58(6). P. 433–440. https://doi.org/10.1016/j.scijus.2018.04.001.
13. Білоус В., Латиш К. Судові експертизи радіоелектронних засобів як форма використання спеціальних знань під час розслідування корупційних кримінальних правопорушень. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2022. Вип. 1 (61). С. 5–11. https://doi.org/10.32689/2522-4603.2022.1.1
14. 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.
15. 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. https://doi.org/10.33766/2786-9156.106.1.191-203.

Stepaniuk R., Perlin V. Forms of use of special knowledge in the field of digital forensics in criminal proceedings

Summary. In the article, the authors identified forms of using special knowledge in the field of digital forensics in criminal proceedings and provided a brief description of them. The authors emphasise that the significant expansion of technical capabilities for detecting and extracting digital traces of criminal offences requires improving the use of specialised knowledge in the field of digital forensics in criminal proceedings and developing effective recommendations for its practical implementation. Currently,

the procedural form manifests itself in the involvement of relevant specialists and experts in criminal proceedings, while the non-procedural form manifests itself in the conduct of digital forensic investigations as part of criminal analysis. The involvement of a digital forensics specialist in investigative (search) activities related to the copying of computer data is mandatory, primarily due to the need to seize and preserve digital evidence in an unaltered state. To this end, specialists use specialised digital forensics tools and appropriate methods, taking into account the specifics of the objects under investigation. In turn, the competent seizure of objects during procedural actions is a prerequisite for the appointment of a forensic computer-technical examination, which investigates the technical condition of computer equipment and networks, as well as computer data itself, solving problems that arose during the pre-trial investigation and court proceedings. Computer-technical expertise can be conducted in conjunction with other types of expertise, which is particularly common in connection with the examination of digital audio and video recordings. Digital forensic investigation is a new form of applying specialised knowledge in criminal proceedings, which lacks adequate procedural and legal regulation and is carried out mainly on an organisational basis. The development of uniform terminology in this area, as well as the development of a regulatory and legal framework for forensic intelligence in cyberspace, are promising areas for further scientific research.

Key words: criminal proceedings, investigative (search) actions, expert, specialist, digital forensics, digital evidence, criminal intelligence, criminal analysis.

Стаття надійшла 16.10.2025
Статтю прийнято 03.11.2025
Стаття опублікована 10.12.2025