Organization, discipline, morality. It is noted that the effectiveness of cooperation in countering pre-trial investigation can be evaluated from the standpoint of both prevention and effective overcoming of manifestations of opposition to pre-trial investigation.

Keywords: organization of activity, investigative (search) actions, productive cooperation, competencies, opposition to pre-trial investigation, evaluation of effectiveness of cooperation.

DOI: 10.33766/2524-0323.99.283-294
УДК: 343.98

Степанюк Р. Л., *доктор юридичних наук, професор, професор кафедри криміналістики, судової експертології та домедичної підготовки Харківського національного університету внутрішніх справ (м. Харків, Україна)*
e-mail: stepanuk2@ukr.net
ORCID ID: https://orcid.org/0000-0002-8201-4013
Перлін С. І., *кандидат юридичних наук, доцент, радник Голови Національної поліції України (м. Харків, Україна)*
e-mail: vladlenperlin@gmail.com
ORCID ID: https://orcid.org/0000-0001-9397-2738

ЦИФРОВА КРИМІНАЛІСТИКА Й УДОСКОНАЛЕННЯ СИСТЕМИ КРИМІНАЛІСТИЧНОЇ ТЕХНІКИ В УКРАЇНІ

З кожним роком зростають потреби правоохоронних органів в ефективних інструментах виявлення, вилучення, дослідження та використання в доказуванні цифрових доказів. У криміналістичній науці останніх десятиліть цифрова криміналістика є одним із найбільш актуальних напрямів розвитку. Цифрова криміналістика (digital forensics) є галуззю судових наук, що являє собою систему наукових методів дослідження цифрових доказів з метою сприяння виявленню та розслідуванню кримінальних правопорушень. Водночас у вітчизняній системі криміналістики відповідні засоби та методи належного місця досі не знайшли.

Авторами проаналізовано думки українських науковців щодо місця цифрової криміналістики в системі криміналістичної науки. Обґрунтовано, що в існуючій моделі криміналістики в Україні є нагальна потреба формування окремої галузі криміналістичної техніки, яка включає засоби і методи дослідження цифрових доказів. Це значно спрощує завдання з інтеграції досягнень цифрової криміналістики у вітчизняну систему криміналістики, оскільки, з одного боку, не вимагає перегляду самої системи, а з іншого – дозволяє швидко впровадити більшість відповідних наукових положень і практичних рекомендацій. Зміст розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів, має включати наукові положення цифрової криміналістики як галузі судових наук, адаптованих до реалій вітчизняної правоохоронної практики та криміналістичної теорії. Не варто ототожнювати цифрову криміналістику 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 криміналістики, ніж та, що сформувалась в Україні, тому проблеми їх інтеграції потребують подальших наукових пошуків.

Ключові слова: теорія криміналістики, система криміналістичної техніки, цифрова криміналістика, цифрові докази, криміналістичне дослідження цифрових доказів.

Постановка проблеми. Повсюдне використання цифрових пристроїв і відповідних технологій у різних сферах життя людини зумовлює трансформацію механізмів багатьох кримінальних правопорушень.

Зараз фактично кожна людина використовує кілька цифрових пристроїв та щодобово отримує доступ до різних цифрових послуг. Відповідно, у повсякденному житті виникає величезна кількість цифрових слідів, а отже, вірогідність того, що цифрові сліди залишаться наслідок злочинної діяльності дуже висока [1, с. 25465]. Тому з кожним роком збільшується кількість випадків, коли правоохоронцям необхідно виявляти і досліджувати цифрові сліди, застосовувати інструменти пошуку та фіксації інформації в кіберпросторі, використовувати цифрові дані в процесі доказування у кримінальному провадженні. Відповідно, потреби правоохоронних органів в ефективних інструментах виявлення, вилучення та дослідження цифрових слідів постійно зростають, і в криміналістичній науці останніх десятиліть цей напрямок є одним із найбільш актуальних і тому динамічно розвивається.

Як слушно зазначила Т. П. Матюшкова: «Електронна (цифрова) інформація як невід'ємний атрибут сучасної злочинної й криміналістичної діяльності визначає перспективи розвитку криміналістики, що пов'язані із переглядом як окремих складових її системи, так і криміналістики в цілому, та обумовлює перспективи подальших наукових досліджень у даному напрямку. Особливо, зважаючи на поширення теорії «комп'ютерної криміналістики» [2, с. 249]. Але у вітчизняній моделі криміналістики досі не приділено належної уваги теоретичним питанням щодо ролі та місця в ній цифрової криміналістики (англ. – digital forensics). У нашій державі науковці зосереджуються на проблемах судової експертизи комп'ютерної техніки та програмних продуктів (її об'єктах, завданнях, можливостях та методиках проведення) і на методиці розслідування кіберзлочинів. Такий стан речей вважаємо неприпустимим, оскільки дисципліна «digital forensics» фактично є окремим розділом судових наук (forensic sciences) і в Україні має повноцінно впроваджуватись із врахуванням тієї моделі криміналістичної науки, яка склалась у нас.

Аналіз останніх досліджень і публікацій. Окремі аспекти щодо перспектив розвитку цифрових технологій у криміналістичній діяльності українські науковці розглядають, зосереджуючи увагу на деяких інноваційних напрямах криміналістичної техніки і нових методиках розслідування окремих видів кримінальних правопорушень. Лише нещодавно розпочались пошуки шляхів інтеграції цифрової криміналістики до вітчизняної системи криміналістичної науки. Зокрема, А. С. Колодіна і Т. С. Федорова окреслили авторське бачення щодо поняття та змісту цифрової криміналістики як галузі судових наук [3]. М. О. Думчиков наголосив на важливості інтеграції положень цифрової криміналістики до класичної системи криміналістичної науки [4]. А. В. Самодін дослідив зміст

цифрової криміналістики як навчальної дисципліни та визначив на цій підставі її співвідношення з криміналістикою як юридичною наукою і навчальною дисципліною в Україні [5]. І. І. Когутич окреслив перспективи застосування цифрових технологій як нового напряму розвитку криміналістики [6], а В. Ю. Шепітько та М. В. Шепітько обґрунтували теоретичну концепцію відповідного стратегічного напрямку розвитку криміналістичної науки та практики правозастосування [7]. Водночас більшість теоретичних питань щодо визначення конкретних напрямків впровадження положень цифрової криміналістики до системи криміналістичної науки в Україні до цього часу залишаються не вирішеними.

Формулювання цілей. Мета статті полягає у визначенні напрямків інтеграції положень цифрової криміналістики як галузі судових наук до вітчизняної системи криміналістичної науки, зокрема шляхом формування нової галузі криміналістичної техніки.

Виклад основного матеріалу. Зараз можна констатувати, що у сфері цифрової криміналістики вітчизняна правоохоронна практика випереджає криміналістичну теорію. У практичній площині засоби та методи цифрової криміналістики широко застосовують в оперативно-розшуковій діяльності, під час проведення слідчих (розшукових) і негласних слідчих (розшукових) дій, у ході розслідування кіберзлочинів та в судовій експертизі. Своєю чергою, у криміналістичній теорії немає відповідей навіть на такі питання, як: 1) чи співвідносяться цифрова криміналістика і традиційна криміналістика; 2) чи є перша частиною другої чи це окремі науки? Унаслідок застарілості наукових уявлень про структуру криміналістичної техніки в Україні склалась ситуація, коли такий популярний і надзвичайно практично корисний напрямок судових наук, як цифрова криміналістика, взагалі не представлений у вітчизняних підручниках з криміналістики.

У зарубіжній науковій літературі проблеми цифрової криміналістики досліджуються вже багато років. Виникла ця галузь на початку 1970-х років, коли фахівці відновили копію бази даних, яка була випадково видалена [8]. Вважається, що першою науковою працею з даної галузі була книга Д. Паркера «Crime by Computer», видана у 1976 році, а бурхливий розвиток цифрової криміналістики розпочався з 1985 року, коли значно активізувалось впровадження комп'ютерів у різні сфери суспільного життя. Програмісти почали отримувати доступ до внутрішніх систем та обладнання через програмні коди. Стало зрозуміло, що комп'ютери будуть використовуватись для злочинних цілей [9]. З того часу галузь цифрової криміналістики досягла значних успіхів у протидії викликам суспільству, які виникли у зв'язку з розвитком комп'ютерної злочинності. Було розроблено багато дієвих техніко-криміналістичних інструментів дослідження цифрових доказів, впроваджено ефективні методи виявлення, розкриття та розслідування кримінальних правопорушень, учинених у кіберпросторі.

Зарубіжні фахівці розглядають цифрову криміналістику як галузь (складову частину) судових наук (Forensic Science) [10]. Її визначають як систему наукових методів зберігання, збирання, перевірки, ідентифікації, аналізу, інтерпре-

тації, документування та представлення цифрових доказів, одержаних із цифрових джерел, з метою сприяння розслідуванню подій, як правило, протиправного характеру [11, с. 14]. У питаннях термінології до цього часу в цифровій криміналістиці серед фахівців згоди дуже мало [12]. Наголошено на її мультидисциплінарній і міждисциплінарній природі [13, с. 275] і водночас досить слабкій інтеграції із судовими науками, зокрема в частині співвідношення технічних аспектів дослідження цифрових доказів та організаційних і правових аспектів здійснення кримінального розслідування [14, с. 649]. Указано на велику прірву між технічними фахівцями та юристами-практиками, які розуміють важливість ознайомлення з методами цифрової криміналістики, але вважають, що зрозуміти та виконувати технічні процедури дуже важко [15, с. 30]. Ці обставини зумовлюють потребу подальшої гармонізації теоретичних уявлень про місце та роль засобів і методів цифрової криміналістики в судових науках і практиці правозастосування. Але, незважаючи на проблеми, за кордоном цифрова криміналістика є визнаною галуззю, яка в останні десятиліття розвивається найбільш активно і демонструє значні досягнення.

Вітчизняні криміналісти тільки нещодавно почали звертались до проблеми визначення сутності цифрової криміналістики та її місця в традиційній системі криміналістики, але єдиного підходу до її вирішення поки що не знайшли.

Так А. С. Колодіна та Т. С. Федорова зауважили, що «цифрова криміналістика (форензіка, комп'ютерна криміналістика, розслідування кіберзлочинів) – прикладна наука про розкриття злочинів, пов'язаних із комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів» [3, с. 177], і не намагались адаптувати це поняття до вітчизняної моделі криміналістики, очевидно, приєднавшись до одного з представлених у криміналістичній спільноті підходу щодо розуміння цифрової криміналістики як окремої галузі судових наук.

Інші автори здійснюють спроби визначити місце цифрової криміналістики в тій системі криміналістичної науки, яка є загальновизнаною в Україні.

Так М. О. Думчиков констатував, що можливими варіантами може бути або поява нового розділу в класичній криміналістиці, або визнання окремої науки «цифрова криміналістика», або формування окремого вчення в загальній теорії криміналістики, або модернізація вже існуючих вчень (про сліди, про організацію розслідування), розділів криміналістики (наприклад, у криміналістичній техніці з'явиться підрозділ «кібертрасологія»; окремою методикою розслідування злочинів з'являться блоки типових комп'ютерних алгоритмів, побудованих на аналізі величезного інформаційного масиву) [4, с. 105]. Такий підхід, безумовно, лише окреслює складність проблеми без конкретики щодо авторського бачення способу її вирішення.

А. В. Самодін проаналізував зміст цифрової криміналістики як навчальної дисципліни, що пропонується до викладання у вітчизняних закладах вищої освіти. На цій підставі науковець дійшов висновку, що, як самостійне формулювання, «цифрова криміналістика» або ж її споріднені інтерпретації доцільно ви-

користовувати та розглядати виключно в контексті окремих навчальних дисциплін як певну сукупність міжпредметних знань. Водночас, з огляду на предмет науки криміналістики й зокрема самостійної прикладної юридичної навчальної дисципліни, яка викладається на її основі, знання про цифрові технології мають знаходити свій вияв у контексті її традиційних складових частин – криміналістичної техніки, криміналістичної тактики та криміналістичної методики [5, с. 278]. Видається, що варто особливо виокремити важливість виділеного автором міжпредметного змісту галузі знань, яку називають цифровою криміналістикою, охоплення нею не тільки тих аспектів, які, за вітчизняними уявленнями, входять до предмету науки криміналістики, а й деяких інших питань, що дещо ускладнює завдання з повної інтеграції цифрової криміналістики до традиційної для нас системи криміналістичної науки.

Варто визнати, що цифрова криміналістика вже склалась як окрема галузь знань. Вона розвивається насамперед як одна з судових наук, тобто як частина криміналістики в тій її моделі, що представлена в країнах класичного права. У вітчизняній моделі криміналістики як юридичної науки положення цифрової криміналістики знаходять своє місце лише частково, насамперед ті складові, які відносяться до криміналістичної тактики та методики і застосовуються до проведення окремих слідчих (розшукових) дій та розслідування кіберзлочинів. Технічні питання, які є основними в цифровій криміналістиці, вочевидь, мали б сформувати окрему галузь криміналістичної техніки, чого досі зроблено не було, за винятком окремого виду судової експертизи комп'ютерної техніки та програмних продуктів і вдосконалення методик проведення деяких інших експертиз, які використовують методи цифрової криміналістики (фототехнічної, експертизи відео- звукозапису та ін.). На нашу думку, проблема пов'язана із застарілістю вітчизняних уявлень про систему криміналістики, що і викликало труднощі в інтеграції до цієї системи цифрової криміналістики.

Авторитетні українські вчені висловлюють думку про цифрову криміналістику як новий напрям у криміналістичній науці.

Так В. Шепітько та М. Шепітько вказують, що цифрова криміналістика може розглядатись як стратегічний напрям у розвитку криміналістичної науки та правозастосовної практики. Своєю чергою, розвиток самої цифрової криміналістики відбувається у трьох основних напрямах: 1) формування окремої наукової галузі в криміналістиці; 2) застосування спеціальних знань під час роботи з цифровими доказами; 3) проведення судових експертиз (зокрема, комп'ютерно-технічної експертизи) [7, с. 21].

І. І. Когутич теж розглядає «цифрову» («електронну») криміналістику як новітній напрям у межах науки криміналістики. Але, на його думку, підгалузями цифрової криміналістики є: 1) криміналістичне вчення про комп'ютерну інформацію; 2) теоретичні положення й рекомендації щодо криміналістичного дослідження комп'ютерних засобів, інформаційних систем та інформаційно-телекомунікаційних мереж; 3) теоретичні положення й рекомендації стосовно шляхів і можливостей криміналістичного застосування комп'ютерної інформації, засобів її обробки та захисту [6, с. 81-82].

Вищенаведені підходи спрямовані на зближення позицій із розуміння місця цифрової криміналістики в різних моделях криміналістичної науки. Нам видається, що вони потребують подальшого розвитку з метою більшої конкретизації.

Дійсно, не можна заперечити важливість подальшого розвитку криміналістики в Україні шляхом широкого впровадження засобів і методів цифрової криміналістики. Але вважаємо, що ототожнювати цифрову криміналістику із застосуванням цифрових технологій у криміналістичній діяльності не варто. Цифрові технології впроваджуються повсюдно, у тому числі й у слідчу та експертну практику. Тому зараз фактично всі галузі криміналістичної техніки та судової експертизи розвиваються насамперед в аспекті автоматизації процесів дослідження. Це має відношення і до криміналістичних обліків, і до окремих розділів криміналістичної техніки, і щодо процедур досудового розслідування. Але цифрова криміналістика не охоплює всю методологію та інструментарій криміналістичної діяльності, яка здійснюється за допомогою інформаційних технологій. Насамперед це технічне дослідження цифрової інформації (цифрових доказів) у криміналістичних цілях, аналіз цієї інформації з метою сприяння розкриттю та розслідуванню злочинів та її захист від злочинних посягань (фактично – криміналістична профілактика).

Основою цифрової криміналістики є її технічна складова, тобто засоби і методи техніко-криміналістичного дослідження цифрових доказів. Ця галузь характеризується широким інструментарієм, як комерційним, так і з відкритим кодом. Вона має свій міжнародний стандарт, який був імплементований і в Україні – ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) [16]. Відповідно, засоби і методи цифрової криміналістики орієнтовані на забезпечення технічних процедур пошуку, вилучення, зберігання й аналізу інформації, яка міститься в комп'ютерних засобах, електронних мережах, мобільних телефонах та інших цифрових пристроях, хмарних сховищах тощо.

Загалом для цифрової криміналістики характерна відсутність не тільки єдиної термінології, але і чітко визначеної системи. Проте одержати явлення про таку систему можна, аналізуючи відповідні наукові огляди.

Наприклад, в одному з оглядів засоби і методи цифрової криміналістики пропонується поділяти за компонентами на апаратні засоби, програмне забезпечення та послуги, а за типом – на «комп'ютерну криміналістику», «мережеву криміналістику», «криміналістику мобільних приладів» і «хмарну криміналістику» [17]. Деталізовано такі сучасні напрями цифрової криміналістики: 1) дослідження хмарних сховищ; 2) дослідження мобільних пристроїв (телефонів); 3) дослідження програм (месенджерів та інших застосунків для смартфонів, що використовуються для обміну інформацією); 4) дослідження інтернет-речей (IoT); 5) мережеві дослідження; 6) дослідження новітніх приладів і додатків (Alexa від Amazon, Google Assistant, Siri від Apple та ін.); 7) дослідження додатків не для те-

лефону (дослідження баз даних, Spotlight, America online instant messaging, дронів, волатильної пам'яті, Даркнету, засобів антикриміналістики, видалених і фрагментованих файлів, зображень, флеш-пам'яті, криповалют); 8) цифровий аналіз поведінки; 9) цифрова криміналістична розвідка та розвідка на основі відкритих джерел тощо [17]. В іншому науковому огляді інструменти і методи цифрової криміналістики розподілено залежно від об'єкту на: 1) дослідження операційної системи; 2) дослідження файлової системи; 3) дослідження оперативної пам'яті; 4) web-дослідження (дослідження web-браузерів); 5) дослідження електронної пошти; 6) мережеві дослідження; 7) мультимедійні дослідження; 8) інші (дослідження месенджерів, зйомних носіїв інформації тощо) [18].

Попри різні підходи до систематизації засобів і методів цифрової криміналістики, не складно побачити, що ця галузь насамперед є техніко-криміналістичною. Але, на відміну від багатьох інших галузей криміналістичної техніки (судових наук), вона не обмежується тільки технічними аспектами. В останні десятиліття здійснюються значні зусилля з інтеграції технічних аспектів дослідження цифрових доказів до всього процесу виявлення та розслідування кіберзлочинів. Це робиться з метою вироблення шляхів побудови цілісних підходів до розслідування, адже специфіка процесу доказування кіберзлочину вимагає участі фахівця на всіх етапах розслідування, а не тільки в ході однієї чи кількох слідчих (розшукових) дій або судової експертизи.

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

Викладені вище обставини зумовлюють значні труднощі у визначенні місця цифрової криміналістики в системі криміналістики в Україні. Ми вважаємо, що в нинішніх умовах, коли систему криміналістики в Україні не переглянуто, визначення цифрової криміналістики як окремого напрямку всієї криміналістичної науки є теоретично корисним, але практично малоперспективним шляхом. Спочатку необхідно вдосконалити систему криміналістики, знайшовши в ній місце для різних стратегічних напрямів. Водночас в нинішніх умовах вважаємо, що треба чітко розрізняти цифровізацію криміналістики як закономірний сучасний етап її розвитку, тобто впровадження цифрових технологій у різні галузі криміналістичної техніки та судової експертизи, до самого процесу досудового розслідування, та цифрову криміналістику як окрему галузь, спрямовану на дослідження цифрових пристроїв, мереж та інформації.

Вважаємо, що в існуючій моделі криміналістичної науки в Україні є нагальна потреба формування окремої галузі криміналістичної техніки, яка включає засоби і методи дослідження цифрових доказів. Це значно спрощує завдання з інтеграції досягнень цифрової криміналістики у вітчизняну систему криміналістики, оскільки, з одного боку, не вимагає перегляду самої системи, а з іншого –

дозволяє швидко впровадити більшість відповідних наукових положень і практичних рекомендацій. Деяка частина положень цифрової криміналістики може бути віднесена і до криміналістичної тактики (щодо тактики зняття інформації з електронних комунікаційних мереж, електронних інформаційних систем і т. ін.), і методики (щодо окремих методик розслідування злочинів), але основа цієї галузі знань все одно є техніко-криміналістичною.

Віднесення до цифрової криміналістики технічних питань розслідування кримінальних правопорушень, які вчиняються у кіберпросторі, методів цифрової розвідки з метою розкриття злочинів тощо, на нашу думку, не заважає завданню з формування відповідної частини криміналістичної техніки. За аналогією можна звернутись до будь-якої іншої галузі криміналістичної техніки, яка завжди впливає і на криміналістичну тактику, і на методику розслідування окремих видів кримінальних правопорушень. Наприклад, положення судової балістики широко застосовуються в методиці розслідування злочинів, вчинених із використанням вогнепальної зброї, а положення судового документознавства в методиці розслідування фальшивомонетництва. Проте це не зумовлює розширення предметної області відповідних галузей за межі криміналістичної техніки. Так само і криміналістичне дослідження цифрових доказів (електронних носіїв інформації, комп'ютерної інформації, комп'ютерних даних), що, безумовно, набуває все більшого поширення відносно різних видів слідчих (розшукових) дій і розслідування все більшого кола різноманітних кримінальних правопорушень, не потребує його розгляду більш широко, ніж окремої галузі криміналістичної техніки.

Висновки. У нинішніх умовах одним із найбільш важливих напрямків розвитку криміналістики є становлення та вдосконалення галузі техніко-криміналістичного дослідження цифрових даних (доказів).

У судових науках (forensic sciences) сформовано окрему галузь – цифрову криміналістику (digital forensics), яка являє собою систему наукових методів дослідження цифрових доказів з метою сприяння виявленню та розслідуванню кримінальних правопорушень. Водночас у вітчизняній системі криміналістики відповідні засоби та методи належного місця досі не знайшли. Тому в Україні існує нагальна потреба у становленні окремого розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів, зміст якого включатиме наукові положення цифрової криміналістики як галузі судових наук, адаптованих до реалій вітчизняної правоохоронної практики та криміналістичної теорії.

Не варто ототожнювати цифрову криміналістику із застосуванням цифрових технологій у криміналістиці, з методиками розслідування кримінальних правопорушень, пов'язаних із комп'ютерною інформацією, або визначати її як окрему частину вітчизняної моделі криміналістики як прикладної юридичної науки та навчальної дисципліни. Цифрова криміналістика є галуззю іншої моделі криміналістики, ніж та, що сформувалась в Україні, тому проблеми їх інтеграції потребують подальших наукових пошуків.

Використані джерела:

1. Casino F., Dasaklis T. K., Spathoulas G., Anagnostopoulos M., Ghosal A., Borocz I., ... & Patsakis C. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*. 2022. Vol. 10. P. 25464 – 25493. DOI: 10.1109/ACCESS.2022.3154059.

2. 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.

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

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

5. Самодін А. В. Сучасне розуміння феномену «цифрова криміналістика». *Інновації в криміналістиці та судовій експертизі : матеріали міжвідом. наук.-практ. конф. (Київ, 25 листоп. 2021 р.) / [редкол.: В. В. Чернєй, С. С. Чернявський, А. А. Саковський та ін.].* Київ : Нац. акад. внутр. справ, 2021. С. 275-279.

6. 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.

7. 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.

8. Caviglione L., Wendzel S., Mazurczyk W. The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security & Privacy*. 2017. Vol. 15, № 6. P. 12-17. DOI: 10.1109/MSP.2017.4251117.

9. Pollitt M. A History of Digital Forensics In: Chow KP., Shenoi S. (eds) Advanc-es in Digital Forensics VI. Digital Forensics 2010. IFIP Advances in Information and Communication Technology. 2010. Vol. 337. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-15506-2_1.

10. Guarino A. Digital Forensics as a Big Data Challenge. In: Reimer, H., Pohlmann, N., Schneider, W. (eds) ISSE 2013 Securing Electronic Business Processes. Springer Vieweg, Wiesba den. DOI : 10.1007/978-3-658-03371-2_17.

11. Delp E., Memo N., Wu M. Digital forensics. *IEEE Signal Processing Magazine*. 2009. Iss. 26(2). P. 14–15.

12. Vincze Eva A. Challenges in digital forensics. *Police Practice and Research*. 2016. Iss. 17:2. P. 183–194. DOI: 10.1080/15614263.2015.1128163.

13. Sadiku M. N., Tembely M., Musa S. M. Digital Forensics. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2017. Iss. 7(4). P. 274–276.

14. Casey E. The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences*. 2019. Iss. 51 (6). P. 649–664. DOI: 10.1080/00450618.2018.1554090.

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

16. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037: 2012, IDT). URL : http://online.budstandart.com/ua/catalog/doc-page?id_doc =74978.

17. Reedy P. Interpol review of digital evidence 2016-2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520.

18. Javed A. R., Ahmed W., Alazab M., Jalil Z., Kifayat K., Gadekallu T. R. A compre hensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*. 2022. Vol. 10. P. 110650–11089. DOI: 10.1109/ACCESS.2022. 3142508.

References:

1. Casino, F., Dasaklis, T. K., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz I., ... & Patsakis, C. (2022) Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access. Vol. 10, 25464 – 25493*. DOI: 10.1109/ACCESS.2022.3154059. [in English].

2. Matiushkova, T. P. (2021) Elektronna (tsyfrova) informatsiia: suchasnyi stan i perspektyvy rozvytku kryminalistyky. *Aktualni problemy kryminalnoho protsesu ta krymi nalistyky: tezy dop. Mizhnar. nauk.-prakt. konf.(m. Kharkiv, 29 zhovt. 2021 r.) - Actual problems of the criminal process and criminology: theses add. International science and practice conference (Kharkov, October 29, 2021).* Kharkiv: KhNUVS, *248-250*. [in Ukrainian].

3. Kolodina, A. S., Fedorova, T. S. (2022) Tsyfrova kryminalistyka: problemy teorii i praktyky. *Kyivskyi chasopys prava – Kyiv Journal of Law, issue 1, 176-180.* [in Ukrainian].

4. Dumchykov, M. O. (2020) Protsesy didzhytalizatsii i kryminalistyka: rektrospektyvnyi analiz. *Kryminalistyka i sudova ekspertyza - Forensics and forensic examination, issue 65, 100-108*. [in Ukrainian].

5. Samodin, A. V. (2021) Suchasne rozuminnia fenomenu «tsyfrova kryminalistyka». *Innovatsii v kryminalistytsi ta sudovii ekspertyzi : materialy mizhvidom. nauk.-prakt. konf. (Kyiv, 25 lystop. 2021 r.) / [redkol.: V. V. Cherniei, S. S. Cherniavskyi, A. A. Sakovskyi ta in.] - Innovations in criminology and forensic examination: interdisciplinary materials. science and practice conf. (Kyiv, November 25, 2021) / [editors: V. V. Chernei, S. S. Chernyavskyi, A. A. Sakovskyi, etc.].* Kyiv : Nats. akad. vnutr. sprav, *275-279*. [in Ukrainian].

6. Kohutych, I. I. (2021) Zastosuvannia tsyfrovykh tekhnolohii – novyi napriam kryminalistyky. *Naukovi chytannia pamiati Hansa Hrossa: zbirnyk tez mizhnarodnoi naukovo-praktychnoi konferentsii (m. Chernivtsi, 09 hrudnia 2021 r.) - Scientific readings in memory of Hans Gross: collection of theses of the international scientific and practical conference (Chernivtsi, December 9, 2021).* Chernivetskyi natsionalnyi universytet imeni Yuriia Fedkovycha. Chernivtsi : Tekhno-druk, *79-84*. [in Ukrainian].

7. Shepitko, V., Shepitko, M. (2021) Doktryna kryminalistyky ta sudovoi ekspertyzy: formuvannia, suchasnyi stan i rozvytok v Ukraini. *Pravo Ukrainy – Law of Ukraine, 8, 12-27*. DOI: 10.33498/louu-2021-08-012. [in Ukrainian].

8. Caviglione, L., Wendzel, S., Mazurczyk, W. (2017) The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security & Privacy. Vol. 15, 6, 12-17.* DOI: 10.1109/MSP. 2017.4251117. [in English].

9. Pollitt, M. (2010) A History of Digital Forensics In: Chow KP., Shenoi S. (eds) Advances in Digital Forensics VI. Digital Forensics 2010. IFIP Advances in Information and Communication Technology. Vol. 337. Springer, Berlin, Heidelberg. DOI : 10.1007/978-3-642-15506-2_1. [in English].

10. Guarino, A. (N. d.) Digital Forensics as a Big Data Challenge. In: Reimer, H., Pohlmann, N., Schneider, W. (eds). ISSE 2013 Securing Electronic Business Processes. Springer Vieweg, Wiesba den. DOI: 10.1007/978-3-658-03371-2_17. [in English].

11. Delp, E., Memo, N., Wu, M. (2009) Digital forensics. *IEEE Signal Processing Magazine, issue 26(2), 14–15*. [in English].

12. Vincze, Eva A. (2016) Challenges in digital forensics. *Police Practice and Research, issue 17:2, 183–194.* DOI : 10.1080/15614263.2015.1128163. [in English].

13. Sadiku, M. N., Tembely, M., Musa, S. M. (2017) Digital Forensics. *International Journal of Advanced Research in Computer Science and Software Engineering, issue 7(4), 274–276*. [in English].

14. Casey, E. (2019) The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences, issue 51 (6), 649–664*. DOI : 10.1080/00450618.2018.1554090. [in English].

15. Ricci, S. C. (2006) Ieong. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation, vol. 3, 29–36.* Supplement, URL : https://doi.org/10.1016/j.diin.2006.06.004. [in English].

16. DSTU ISO/IEC 27037:2017 Informatsiini tekhnolohii. Metody zakhystu. Nastanovy dlia identyfikatsii, zbyrannia, zdobuttia ta zberezhennia tsyfrovykh dokaziv (ISO/IEC27037: 2012, IDT). N. d. N. p. URL : http://online.budstandart.com/ua/catalog/doc-page?id_doc= 74978. [in Ukrainian].

17. Reedy P. Interpol review of digital evidence 2016-2019. (2020) *Forensic Science International: Synergy. Vol. 2, 489–520.* [in English].

18. Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., Gadekallu, T. R. (2022) A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access. Vol. 10, 110650–11089.* DOI: 10.1109/ACCESS.2022.314 2508. [in English].

Стаття надійшла до редколегії 02.08.2022

Stepaniuk R., *Doctor of Law, Professor, Professor of the Department Criminalistics, Forensic Science and Pre-Medical Training of Kharkiv National University of Internal Affairs (Kharkiv, Ukraine)*

Perlin S., *Candidate of Law, Associate Professor, Adviser to the Head of the National Police of Ukraine (Kharkiv, Ukraine)*

DIGITAL FORENSICS AND IMPROVEMENT OF THE FORENSIC TECHNOLOGY SYSTEM IN UKRAINE

Every year, the needs of law enforcement agencies for effective tools for detection, extraction, research and use in proving digital evidence are growing. In the forensic sciences of recent decades, digital forensics is one of the most relevant areas of development. Digital forensics is a branch of forensic sciences, which is a system of scientific methods of researching digital evidence with the aim of facilitating the detection and investigation of criminal offenses. At the same time, the appropriate means and methods have not yet found their proper place in the domestic criminalistics system.

The authors analyzed the opinions of Ukrainian scientists regarding the place of digital forensics in the system criminalistics. It is substantiated that in the existing model of criminalistics in Ukraine, there is an urgent need for the formation of a separate field of forensic technology, which includes the means and methods of digital evidence research. This greatly simplifies the task of integrating the achievements of digital forensics into the domestic system of criminalistics, since, on the one hand, it does not require a review of the system itself, and on the other, it allows for the rapid implementation of most of the relevant

scientific provisions and practical recommendations. The content of the forensic technology section dedicated to the forensic investigation of digital evidence should include the scientific provisions of digital forensics as a field of forensic science adapted to the realities of domestic law enforcement practice and forensic theory. Digital forensics should not be equated with the use of digital technologies in criminalistics, with the methods of investigating criminal offenses related to computer information, or define it as a separate part of the domestic model of criminalistics as an applied legal science and educational discipline. Digital forensics is a branch of a different model of forensic sciences than the one developed in Ukraine, so the problems of their integration require further scientific research.

Keywords: theory of forensics, system of forensic technology, digital forensics, digital evidence, forensic investigation of digital evidence.