УДК 343.98:007.77:004.8
DOI: 10.21564/2414-990X.168.324997

Тенденції розвитку цифрової криміналістики: виклики та перспективи для органів кримінальної юстиції

Євгенія Євгеніївна Демидова*
Національний юридичний університет імені Ярослава Мудрого, Харків, Україна
**e-mail: ye.ye.demydova@nlu.edu.ua*

Анотація
Актуальність дослідження зумовлена стрімкою цифровізацією суспільства та необхідністю адаптації криміналістики до нових реалій сьогодення. Традиційні методи збирання, дослідження та використання доказів стають недостатніми для вирішення завдань сучасного кримінального провадження, адже дедалі більше кримінальних правопорушень залишають цифровий слід. Метою статті є аналіз тенденцій розвитку цифрової криміналістики, визначення ключових викликів у сфері виявлення, фіксації, вилучення та дослідження цифрових доказів, використання сучасних цифрових пристроїв та інформаційних технологій для потреб розслідування, а також формулювання перспективних напрямів удосконалення роботи органів кримінальної юстиції. Для досягнення поставленої мети використовувалися нормативно-правовий аналіз, порівняльно-правовий підхід та аналіз практичних кейсів. Дослідження базувалося на вивченні сучасних наукових публікацій, законодавчих актів та судової практики, що дало змогу виокремити як позитивні аспекти застосування сучасних технологій у кримінальному провадженні, так і проблеми, пов'язані з їх упровадженням. Отримані результати свідчать про те, що використання новітніх технологій значно розширює можливості органів кримінальної юстиції, водночас створює виклики та проблеми. Зокрема, встановлено: відсутність єдиного термінологічного апарату як на науковому рівні, так і нормативному, у зазначеному аспекті та необхідність удосконалення чинного законодавства; наявність проблем у виявленні, фіксації та вилученні цифрових слідів; недостатність комплексних науково-практичних розробок щодо використання інструментів цифрової криміналістики; необхідність оновлення та розробки нових методик проведення судових експертиз з урахуванням досягнень науки і техніки; недостатня кваліфікація співробітників органів кримінальної юстиції у роботі з цифровими доказами та важливість постійного підвищення кваліфікації слідчих, прокурорів, детективів, суддів щодо збирання, використання, дослідження та оцінки цифрової інформації, а також включення цих питань до навчальних програм студентів юридичних закладів вищої освіти з метою формування компетентностей у сфері цифрової криміналістики; відсутність єдиних міжнародних стандартів щодо вико-

ристання інструментарію цифрової криміналістики та правових механізмів взаємодії провоохоронних органів та важливість активізації міжнародної співпраці та обміну досвідом як на практичному, так і науковому рівні. Запропоновано напрями вирішення зазначених проблем. Подальші дослідження мають бути спрямовані на розроблення єдиних методичних стандартів та нормативно-правових механізмів, що забезпечать ефективну інтеграцію цифрової криміналістики у систему кримінального судочинства.

Ключові слова: цифрова криміналістика; цифрові сліди; електронні сліди; цифрові докази; доказування; комп'ютерні дані.

Trends in the Development of Digital Forensics: Challenges and Prospects for Criminal Justice Agencies

Yevheniia Ye. Demydova*
Yaroslav Mudryi National Law University,
Kharkiv, Ukraine
**e-mail: ye.ye.demydova@nlu.edu.ua*

Abstract
The relevance of this study is driven by the rapid digitalization of society and the necessity for forensic science to adapt to contemporary realities. Traditional methods of collecting, examining, and utilizing evidence are becoming insufficient for addressing the challenges of modern criminal proceedings, as an increasing number of offenses leave digital traces. This article aims to analyze trends in the development of digital forensics, identify key challenges in detecting, recording, seizing, and examining digital evidence, explore the use of modern digital devices and information technologies for investigative purposes, and propose prospective directions for enhancing the work of criminal justice agencies. To achieve this goal, normative-legal analysis, comparative-legal approaches, and case study analyses were employed. The research was based on a review of contemporary scientific publications, legislative acts, and judicial practices, allowing for the identification of both positive aspects of applying modern technologies in criminal proceedings and issues related to their implementation. The findings indicate that the use of advanced technologies significantly expands the capabilities of criminal justice agencies but simultaneously presents challenges and problems. Specifically, it was established. There is a lack of a unified terminology framework, both at the scientific and normative levels, in this context, necessitating improvements in current legislation. Challenges exist in detecting, recording, and seizing digital traces. There is an insufficiency of comprehensive scientific and practical developments regarding the use of digital forensic tools. There is a need to update and develop new methodologies for conducting forensic examinations, considering scientific and technological advancements. The qualifications of criminal justice personnel in handling digital evidence are inadequate, highlighting the importance of continuous professional development for investigators, prosecutors, detectives, and judges in collecting,

utilizing, examining, and assessing digital information. Additionally, incorporating these topics into the curricula of higher legal educational institutions is essential to develop competencies in digital forensics. There is an absence of unified international standards regarding the use of digital forensic tools and legal mechanisms for cooperation among law enforcement agencies, underscoring the importance of enhancing international collaboration and experience exchange at both practical and scientific levels. The article proposes directions for addressing these issues. Future research should focus on developing unified methodological standards and normative-legal mechanisms to ensure the effective integration of digital forensics into the criminal justice system.

Key words: digital forensics; digital traces; electronic traces; digital evidence; evidence evaluation; computer data.

Вступ

Криміналістика є наукою про формування доказової інформації. До предмета криміналістики традиційно належать закономірності, пов'язані з процесами доказування (збиранням, дослідженням, оцінюванням і використанням доказів) [1, с. 17]. Глобальна диджиталізація людства, впровадження цифрових технологій в усі напрями діяльності людини, перенесення особистої та професійної комунікації до цифрового простору, вчинення кримінальних правопорушень із використанням сучасних інформаційних технологій призвели до суттєвих змін й у розумінні закономірностей злочинної діяльності та особливостях її відображення в різних джерелах інформації, які вивчаються криміналістикою.

Науковий підхід щодо відображення результатів готування, вчинення та приховування кримінальних правопорушень лише в ідеальних або матеріально-фіксованих слідах вже давно не відповідає сучасному рівню розвитку технологій. Якщо раніше для розслідування переважної більшості кримінальних правопорушень характерним було вивчення матеріальної обстановки місця події, то на сьогодні для здійснення кримінальних дій все більше використовуються дистанційні способи (фішинг, створення та розповсюдження deepfake відео, використання шкідливого програмного забезпечення, DDoS-атаки, зламування комп'ютерних мереж і серверів із метою викрадення інформації або грошей, використання криптовалюти зі злочинною метою), інформаційні технології, мережі «Інтернет», шифрування комунікацій тощо. Що, у свою чергу, призводить до появи нових видів слідів – цифрових, які вимагають кардинально інших підходів до їх виявлення, вилучення та дослідження.

Розвиток цифрових технологій також вплинув на провадження слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій, пропонуючи більш досконалі способи та методи збирання доказів. Пере-

сувні криміналістичні лабораторії, 3D-сканери, штучний інтелект, безпілотні літальні апарати відкрили нові можливості для виявлення, вилучення та фіксації слідів вчинення кримінальних правопорушень, водночас ставлячи нові питання перед науковцями та практиками, які потребують вирішення, зокрема, щодо необхідності розроблення тактичних рекомендацій їх використання, забезпечення допустимості їх використання у кримінальному провадженні та ін.

Використання супутникових знімків, технологій аналізу «великих даних», дослідження фотознімків, відео- та аудіозаписів, які знаходяться у відкритому доступі (наприклад, у соціальних мережах) або надані слідству, аналіз електронних пристроїв (GPS-трекерів, смартфонів, смартгодинників тощо) дослідження телефонних розмов [2, с. 32], інтеграція систем відеоспостереження з технологіями штучного інтелекту для ідентифікації особи та номерних знаків транспортних засобів суттєво розширили можливості для органів кримінальної юстиції у встановленні обставин, що підлягають з'ясуванню у будь-якому кримінальному провадженні. Водночас постали нові виклики, пов'язані з необхідністю розроблення нових методів та способів збирання, дослідження та використання цифрових доказів.

Традиційні підходи не здатні задовольнити сучасні потреби для ефективного розслідування кримінального правопорушення. У зв'язку з цим у науковій літературі акцентується увага на необхідності формування окремої галузі, що включає засоби і методи дослідження цифрових доказів [3, с. 282]. Зокрема, В.М. Шевчук зазначає, що сучасна парадигма криміналістики має бути спрямована на подальший розвиток та формування цифрової криміналістики для ефективного вирішення нових завдань в умовах воєнного стану та процесів цифровізації суспільства [4, с. 213]. В. Ю. Шепітько та М. В. Шепітько констатують, що цифрова криміналістика є стратегічним напрямком у розвитку криміналістичної науки [5, с. 21]. Схожий підхід спостерігається не лише в Україні, а й на міжнародному рівні. Так, багато іноземних науковців також акцентують увагу на важливості цифрової криміналістики для сучасних кримінальних проваджень [6], наголошуючи на необхідності створення чітких правових механізмів, які забезпечать ефективність розслідувань та належну допустимість цифрових доказів у суді [7].

Значний вплив на розвиток цифрової криміналістики в Україні здійснила військова агресія рф, спонукавши до активного впровадження цифрових технологій при розслідуванні воєнних злочинів. Документування таких злочинів вимагає інших підходів, у тому числі необхідність забезпечення особистої безпеки осіб, що здійснюють процесуальні дії в таких умовах

(дистанційний огляд ділянок місцевості, які перебувають під окупацією, проведення процесуальних дій за високої імовірності повторних обстрілів), потреба у відтворенні первинної обстановки місця події в конкретний час (зокрема, завдяки використанню супутникових знімків), важливість оперативної фіксації слідів вчинення у зв'язку з ризиком їх швидкої втрати, вагомість урахування міжнародних стандартів у документуванні таких доказів для подальшого використання в міжнародному кримінальному суді.

Отже, тенденції розвитку цифрової криміналістики характеризується активним зростанням її ролі для ефективного розслідування кримінального провадження та необхідністю вирішення багатьох проблем стосовно використання її інструментарія.

Метою цієї робити є проведення аналізу тенденції розвитку цифрової криміналістики, окреслення ключових викликів, які постають перед органами кримінальної юстиції у зв'язку з цим, а також визначення перспективних напрямів удосконалення вітчизняної практики роботи з цифровими доказами. Для досягнення поставленої мети передбачено вирішення таких завдань: дослідити практику застосування цифрових технологій в Україні, проаналізувати сучасний стан нормативного регулювання використання цифрових доказів у кримінальному провадженні, дослідити сучасні прийоми, способи, засоби та методи їх збирання й дослідження, виявити проблеми, які виникають у зазначеній діяльності, порівняти українські підходи їх використання з міжнародними стандартами та досвідом; на основі проведеного аналізу сформулювати висновки і пропозиції щодо вдосконалення роботи з цифровими доказами та розвитку цифрової криміналістики.

Матеріали та методи

Дослідження тенденцій розвитку цифрової криміналістики, зокрема визначення викликів та перспективних напрямів її розвитку, проведено шляхом застосування низки загальнонаукових та спеціальних методів наукового пошуку. Основою методології пропонованого дослідження став діалектичний метод наукового пізнання, який дав можливість усебічно опрацювати проблеми, з якими стикаються органи кримінальної юстиції під час роботи з цифровими слідами кримінального правопорушення, а також використання цифрових пристроїв та сучасних технологій, забезпечивши можливість комплексного аналізу відповідних процесів за умов глобальної цифровізації суспільства та з урахуванням постійної змінності досліджуваних процесів. Під час проведення дослідження авторка виходила також із раніше обґрунтованого нею розуміння цифрових слідів як даних, що залишаються у цифровому просторі в результаті використання цифрових пристроїв, технологій та інформаційних мереж [8, с. 75].

Пропоноване дослідження є структурованим та послідовним. На першому етапі було застосовано загальнонауковий метод системного аналізу, що дозволило дослідити загальні закономірності становлення й розвитку цифрової криміналістики як напряму криміналістичного знання. Зокрема, проаналізовано наукові праці провідних українських та зарубіжних вчених, серед яких роботи В. М. Шевчука, В. Ю. Шепітька, К. В. Латиш та інших, що дало можливість сформулювати теоретико-методологічну основу цього дослідження. З метою з'ясування сучасного стану нормативно-правового регулювання цифрових доказів в Україні було застосовано формально-юридичний метод, за допомогою якого здійснено вивчення чинного законодавства України, зокрема положень Кримінального процесуального кодексу України, законів України «Про електронні документи та електронний документообіг», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», а також міжнародних нормативних актів, таких як Конвенція про кіберзлочинність, Керівні принципи Ради Європи щодо електронних доказів. Це дозволило встановити основні прогалини і суперечності у регулюванні роботи з цифровими доказами. Емпіричну базу дослідження становлять матеріали слідчої та судової практики, зокрема рішення судів щодо допустимості цифрових доказів у кримінальному провадженні, а також приклади вітчизняного та міжнародного використання цифрових доказів та сучасних технологій у кримінальному провадженні, в тому числі з метою документування воєнних злочинів, вчинених унаслідок військової агресії рф проти України.

Для отримання нових наукових результатів, що стосуються практичного застосування сучасних цифрових технологій, таких як штучний інтелект, лазерне 3D-сканування, OSINT-технологій та використання безпілотних літальних апаратів, був застосований метод аналізу практичних кейсів. Аналізувалися конкретні ситуації, в яких зазначені технології продемонстрували свою ефективність для виявлення, фіксації, аналізу і оцінки доказової інформації. Також важливу роль у дослідженні відіграв метод систематизації інформації, що дало змогу виокремити основні тенденції розвитку цифрової криміналістики, сформулювати ключові проблеми та перспективні напрями розвитку. Для забезпечення наукової новизни і обґрунтованості результатів використано синтез та узагальнення отриманих теоретичних і практичних даних.

Теоретичну базу дослідження становили положення загальної теорії криміналістики, вчення про сліди вчинення кримінального правопорушення, а також процес слідоутворення, вчення про виявлення, фіксацію, вилучення, дослідження та використання доказів при розслідуванні кримінальних правопорушень.

Отже, комплексне застосування наведених методів дало змогу отримати об'єктивні й науково обґрунтовані результати, які мають як теоретичну, так і практичну цінність для криміналістичної науки та діяльності органів кримінальної юстиції. Використані у дослідженні підходи сприяють формуванню рекомендацій щодо ефективного застосування цифрових технологій у кримінальному провадженні, забезпечуючи високу якість процесу розслідування і судового розгляду відповідно до сучасних викликів та потреб цифрової епохи.

Результати та обговорення

Цифрові докази в кримінальному провадженні та їх вплив на формування цифрової криміналістики

Надзвичайно важливою частиною розвитку будь-якої науки, навчальної дисципліни та практичної діяльності є удосконалення їх термінологічного апарату з метою забезпечення чіткості, ясності та однозначності у процесі застосування. Особливої актуальності це питання набуває сьогодні, коли використання сучасних технологій істотно змінює характер слідів кримінальних правопорушень та створює нові виклики перед наукою і практикою.

Необхідно звернути увагу, що появу цифрової криміналістики вчені пов'язують ще з періодом 1970–1980-х рр., тобто часом, коли виникли персональні комп'ютери та з'явилися перші відомості про злочини в цифровій сфері. Проте у той час основна увага була сфокусована на кібератаках та витоку даних [9, с. 142]. У зв'язку з цим у науковій літературі також зустрічається такий термін, як «комп'ютерна криміналістика».

Активне поширення інформаційних технологій та користування цифровими пристроями та ресурсами привело до виникнення особливого виду слідів, які виникають унаслідок такої діяльності, – цифрових, значно розширивши сферу застосування цифрової криміналістики, охопивши не лише розслідування кіберзлочинів, а й аналіз будь-якої цифрової інформації, що може бути використана як доказ у кримінальному провадженні. На цьому етапі розвитку криміналістики вчені та практики почали звертати увагу на цифрові сліди, тобто ті, які виникають у результаті діяльності людей у цифровому просторі, зокрема: дані IP-адреси; історію пошуку веббраузера; кеш та файли cookies; повідомлення, аудіо- та відеозаписи у соціальних мережах, месенджерах, хмарних сховищах, цифрових носіях; електронні файли; вебсторінки; метадані тощо. На сьогодні вони є вихідними даними при розслідуванні кримінальних правопорушень та після відповідного процесу виявлення, фіксації, вилучення під час здійснення процесуальних дій набувають статусу доказів. Однак потрібно зауважити, що навколо такого виду

доказів відбувається багато дискусій, зумовлених відсутністю їх чіткого нормативно-правового регулювання, зокрема, щодо їх поняття, сутності, місця у структурі доказової інформації, алгоритму роботи з ними під час слідчих (розшукових), негласних слідчих (розшуковий) дій, заходів забезпечення кримінального провадження, обрання оптимальних методів та способів їх виявлення, фіксації та вилучення.

У науковій літературі є різні підходи до визначення терміна, яким необхідно визначати докази у цифровій формі, зокрема, використовуються такі, як «цифрові докази», «комп'ютерні дані», «електронні (цифрові) докази», «електронні докази». Наприклад, Г. К. Авдєєва [10, с. 135], Е. Живуцька-Козловська [11, с. 141], О. І. Гарасимів, С. І. Марко та О. В. Ряшко [12, с. 161–162] аргументують необхідність використання поняття «цифрові докази». А.-М. Ю. Ангеленюк [13], А. В. Матвійчук [14] вживають поняття «електронні докази», а О. В. Калінніков [15, с. 123] у своїх роботах акцентує увагу на електронних (цифрових) доказах. Це відбувається, з одного боку, у зв'язку з тим, що Кримінальний процесуальний кодекс України не містить окремого поняття такого доказу, а з іншого – наявністю відмінностей у використанні термінологічного апарату в різних нормативно-правових актах. Наприклад, Господарський процесуальний кодекс України, Цивільний процесуальний кодекс та Кодекс адміністративного судочинства України оперують терміном «електронний доказ», визначаючи його як окремий вид доказів. Так, наприклад, ст. 100 Цивільного процесуального кодексу України (а також ст. 96 Господарського процесуального кодексу України, ст. 99 Кодексу адміністративного судочинства України) визначає, що електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі «Інтернет») [16]. Конвенція про кіберзлочинність, яка була ратифікована 7 вересня 2005 р., також відома як Будапештська конвенція (Budapest Convention, ETS No. 185), вживає термін «комп'ютерні дані», позначаючи ним будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою (п. b ст. 1) [17]. Відсутність єдиного тер-

мінологічного апарату як у науці, так і в законодавстві призводить до утворення колізій у нормативному регулюванні, ускладнює правозастосування та створює можливості для зловживань як зі сторони обвинувачення, так і сторони захисту. Крім того, суди кримінальної юрисдикції України також іноді ухвалюють протилежні рішення щодо визнання цифрової інформації допустимим доказом за тих самих умов. Причинами невизнання судом допустимими доказами цифрової інформації є надання суду копії цифрової інформації, а не оригіналу; проведення негласних слідчих (розшукових) дій та отримання цифрової інформації без доручення на те слідчого, прокурора й без ухвали слідчого судді; невідкриття стороні захисту доручення на проведення негласних слідчих (розшукових) дій; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення негласних слідчих (розшукових) дій «іншої особи» та ін. [11, с. 141]. Тому актуальним питанням сьогодення є необхідність удосконалення чинного законодавства України щодо використання цифрової інформації шляхом впровадження єдиного термінологічного апарату. На наш погляд, термін «цифровий доказ» є більш адаптованим до розвитку інформаційних технологій, що дає змогу включати нові формати та джерела доказів, які можуть стати важливими в майбутньому. Крім того, в зарубіжних наукових роботах для визначення цифрового доказу також використовується термін «digital evidence», що фактично і можна перекласти як «цифровий доказ» [18, с. 312]. Уніфікація відповідного термінологічного апарату є важливою передумовою ефективності здійснення досудового розслідування та судового розгляду в цілому та стане базою для пошуку рішень щодо особливостей виявлення, вилучення та дослідження таких доказів.

Важливим елементом предмета криміналістики, зокрема цифрової, є процеси збирання, дослідження, оцінки та використання доказів [19, с. 6]. Цифрові докази стороною обвинувачення можуть бути отримані в результаті проведення обшуку, огляду, зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, зняття інформації з електронних інформаційних систем, зняття інформації з електронних комунікаційних мереж, установлення місцезнаходження радіоелектронного засобу, а також тимчасового доступу до речей та документів. Проте традиційні підходи до виявлення, фіксації та вилучення слідів кримінальних правопорушень (трасологічних слідів, слідів застосування вогнепальної зброї, слідів ДНК, слідів підроблення текстових документів тощо) не можуть бути застосовані до цифрових слідів. Такі сліди потребують особливих способів та методів роботи з ними, зумовлених особливостями механізму утворення, специфікою зберігання,

можливістю зміни змісту та знищення (в тому числі дистанційно) тощо. Зокрема, на відміну від традиційних доказів (паперових документів, матеріальних об'єктів, наприклад, зброї, транспортних засобів, певних речовин), характеристики та просторові межі яких ми звикли бачити, цифрові докази мають іншу природу і вирізняються такими характеристиками: електронний документ не може існувати без носія інформації (при цьому набувають значення ідентифікаційні ознаки носія інформації (зокрема найменування типу, марки моделі, індивідуального машинного носія, на якому записаний документ)); вони можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників (високий рівень вологості, висока температура, електромагнітні випромінювання тощо) [20, с. 6–7]. Такі докази можуть бути отримані за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу «Інтернет». Вони стають доступними для сприйняття людиною після оброблення засобами комп'ютерної техніки [15, с. 125]. Для цифрових доказів також характерна така властивість, як можливість копіювання без втрати інформаційної цінності, що суттєво відрізняє їх від традиційних доказів. Проте це створює як переваги, так і ризики, оскільки цей процес їх копіювання може супроводжуватися змінами, які ускладнюють встановлення автентичності. У зв'язку з цим, наприклад, при копіюванні інформації з комп'ютеру підозрюваної особи важливим є використання спеціалізованого обладнання, яке забезпечує автентичність отриманих даних, а не USB-флешнакопишувача чи інших подібних засобів.

У наукових джерелах акцентується увага на інших проблемах роботи з цифровими доказами: необхідності постійного підвищення кваліфікації слідчих і прокурорів щодо технічних аспектів цифрових доказів; наданні рекомендацій щодо перевірки справжності електронних листів; перевірці достовірності роздруківок інформації з комп'ютера, поясненні понять «оригінал», «копія» і «дублікат» цифрової інформації; формуванні алгоритму встановлення автентичності цифрових фотознімків та ін. [10, с. 40–41]. Тому актуальним питанням на сьогодні є необхідність розроблення наукових рекомендацій щодо роботи з окремими видами цифрових доказів, процесуального оформлення виявлених цифрових слідів кримінального правопорушення; необхідності забезпечення цілісності та автентичності цифрових доказів шляхом застосування сучасних методів захисту інформації.

Сучасні науково-технічні засоби та технології в цифровій криміналістиці

Значну допомогу в збиранні, дослідженні та оцінці доказів у кримінальному провадженні надають сучасні науково-технічні засоби та техноло-

гії. Особливу увагу останнім часом привертає штучний інтелект. Його застосування при розслідуванні кримінальних правопорушень може бути корисним у багатьох аспектах, зокрема: аналіз супутникових знімків, відео-, фото- та аудіоматеріалів, соціальних мереж, даних з медичних закладів, текстової інформації, розпізнавання обличчя [21, с. 511–512]. Наприклад, використання технології Clearview AI дає можливість здійснювати пошук та ідентифікацію осіб за обличчям. Зокрема, за її допомогою здійснюється ідентифікація зниклих безвісті людей, військових злочинців, ідентифікація громадян на блокпостах тощо, шляхом порівняння відповідних зображень з базою, яка сформована на основі зібраних загальнодоступних зображень з вебресурсів. Також штучний інтелект використовується з метою попередження кримінальних правопорушень з використанням інтелектуальних систем безпеки з різними пристроями (датчиками) збору інформації [22, с. 176].

Досвід використання штучного інтелекту також притаманний судовій експертизі. Наприклад, у зв'язку з тим, що для проведення портретної експертизи іноді надають не достатньо чіткі, не якісні фотозображення або фотозображення з різних ракурсів (зображення обличчя підозрюваного, яке зафіксовано за допомогою відеоспостереження), набуває актуальності використання штучного інтелекту під час відповідних досліджень. В Україні вперше до процесу такого дослідження долучили штучний інтелект під час проведення портретної експертизи в Київському науково-дослідному інституті судових експертиз з визначення особи загиблого Героя України Олександра Мацієвського у справі за фактом розстрілу росіянами українського військовослужбовця. На вирішення експертів виносилося питання ідентифікації особи загиблого українського військового, який був на відеозаписі. Фахівцям КНДІСЕ було надано відеозапис події з мережі «Інтернет», а також порівняльні зразки – фото осіб, які, на думку правоохоронців, могли бути на відео. Складність полягала в низькій якості досліджуваного відеозапису та нечіткому зображенні стоп-кадрів, які виділяли експерти. У результаті проведеного дослідження експерти КНДІСЕ підтвердили, що українським військовим на відео був Мацієвський Олександр. Потрібно звернути увагу, що штучний інтелект під час дослідження використовувався як допоміжний засіб та не підміняв роботу судового експерта.

Сучасні технології, які засновані на штучному інтелекті, дійсно, здатні перевіряти значний обсяг інформації за короткі проміжки часу, ефективно обробляти інформацію з різних джерел з урахуванням конкретних запитів, прогнозувати ризики та загрози, що значно полегшує здійснення професійної діяльності органів кримінальної юстиції. Водночас це може створити проблеми з конфіденційністю, безпекою та надійністю отриманих

даних та ін., що потребує відповідного правового регулювання на міжнародному рівні та впровадження ефективних механізмів контролю за його використанням.

Значно розширило можливості для фіксації обстановки місця події використання безпілотних авіаційних комплексів. Особливої актуальності ці технології набули у сучасних умовах воєнних дій. Так, в Україні БПЛА успішно вже використовуються для фіксації таких порушень. За допомогою БПЛА було на високому рівні й детально зафіксовано численні руйнування і факти порушень законів та звичаїв війни в м. Харкові. Отримані фото та відео дають змогу детально відтворити обстановку місця подій, виявити масштаби руйнувань та сліди вчинення кримінальних правопорушень. Ці матеріали також є важливою частиною доказової бази.

Використання лазерного 3D-сканеру, як додаткового способу фіксації, дозволяє за кілька годин роботи отримати результат у вигляді 3D-моделі відповідного об'єкта (будинку, транспортного засобу тощо). Це дає змогу з усіх боків оглянути місце кримінального правопорушення і зробити всі необхідні для розслідування заміри з великою точністю. На сьогодні це вкрай важливо при розслідуванні сотень військових правопорушень рф [23, с. 660]. Перевагами цієї технології є висока точність, повнота інформації, забезпечення високої якості проведення фіксації процесуальної дії, забезпечення її наочності та документальності, можливість подальшого роздрукування окремих предметів для використання під час інших слідчих (розшукових) дій [24, с. 282–283]. Крім того, під час перегляду отриманої 3D-моделі є можливість для зміни масштабу, ракурсу та деталізації окремих деталей, що дозволяє виявити навіть найдрібніші елементи місця кримінального правопорушення, які можуть залишитися непоміченими при традиційних методах фіксації.

Використання OSINT-технологій у кримінальному провадженні: можливості, проблеми та перспективи

Особливе місце серед інформаційних технологій, що використовуються при розслідуванні, також займає OSINT (Open Source Intelligence), що дозволяє оперативно отримувати інформацію про обставини кримінального правопорушення, осіб, які причетні до його вчинення, а також ефективно розслідувати злочини міжнародного характеру. По суті, OSINT – це збір інформації з джерел, які є загальнодоступними, зокрема до них належать веб-ресурси, соціальні мережі, відкриті реєстри та інші публічно доступні джерела. До OSINT-методів належать: збирання інформації (у тому числі за фотографіями) з відкритих пошукових систем; аналіз активності користувача в соціальних мережах і блогах, на форумах, інших віртуальних

платформах; пошук відкритих персональних даних користувачів у соціальних мережах, месенджерах; отримання геолокаційних даних за допомогою загальнодоступних ресурсів, таких як Google Maps та ін. [25, с. 164–165]. Прикладом ефективного застосування OSINT-методів є справа про дезертирство військовослужбовця з Криму, де ключовими доказами стали матеріали, зібрані з відкритих джерел, включно із даними із соціальних мереж та електронними документами. Верховний Суд визнав такі докази допустимими та відхилив спроби сторони захисту оскаржити їх достовірність [26].

Однак, незважаючи на переваги застосування OSINT-технологій при розслідуванні кримінальних правопорушень, зокрема: можливість оперативного отримання інформації, відсутність необхідності отримання дозволів уповноважених осіб (оскільки інформація є загальнодоступною), економічність у застосуванні (не потребує використання спеціалізованого технічного обладнання), водночас супроводжується низкою проблем. Так, серед науковців та практиків продовжуються дискусії щодо самого поняття інформації з відкритих джерел, гарантій законності її отримання з деяких із них, різних видів програмного забезпечення та способів його використання, а також роботи з отриманою інформацією. При цьому вчені акцентують увагу, що важливою складовою використання даних, отриманих за допомогою OSINT, є перспектива їх подальшого використання в судах, зокрема в Міжнародному кримінальному суді, і хоча вже розроблено низку стандартів для цього, виходячи з міжнародного досвіду та вже набутого досвіду вітчизняних спеціалістів, перспективним напрямом дослідження такої інформації залишаються питання процесуалізації: збір, перевірка та оцінка отриманих фактичних даних [27, с. 108]. Водночас OSINT-технології на сьогодні є одним із найперспективніших напрямів розвитку цифрової криміналістики та потребують подальших досліджень і розроблення оптимальних алгоритмів роботи з відкритими базами даних, зокрема з одночасним використанням можливостей штучного інтелекту.

Оцінка цифрових доказів у суді: проблеми та шляхи вирішення

Судова практика України поступово виробляє підходи до оцінки цифрових доказів. Так, суддя Верховного Суду у Касаційному кримінальному суді Надія Стефанів акцентує увагу на тому, що суди повинні перевіряти цілісність і автентичність цифрових доказів, зокрема враховувати джерело їх походження. Важливу роль у цьому процесі відіграють міжнародні рекомендації. Так, Рада Європи розробила «Керівні принципи щодо електронних доказів», яких мають дотримуватися як представники органів досудового розслідування, так і судді. Вони дають змогу визначити, чи отримано доказ

у законний спосіб, а також встановити його відповідність критеріям допустимості. Не менш значущим є розуміння суддями природи таких доказів. Для цього необхідні базові знання у сфері електронного документообігу, комп'ютерних мереж та цифрових технологій. Крім того, судді, як зазначає Надія Стефанів, мають розрізняти джерело доказу та сам доказ [26].

Дійсно, аналіз матеріалів практики свідчить про те, що суди в Україні поступово стандартизують використання цифрових доказів у кримінальному провадженні, акцентуючи увагу на важливості встановлення технічних даних (хеш-значення, наявності висновків експертів щодо відсутності внесених змін), виявляючи гнучкість у врахуванні нових видів доказів (OSINT) та орієнтуючись на сутність, а не форму (наприклад, відеозапис може стати визначальним доказом, навіть якщо на протоколі обшуку немає підписів понятих). Проте, це тільки підкреслює наявність проблем у використанні цифрових доказів у кримінальному провадженні та важливість вироблення єдиних стандартів щодо їх збирання й оцінювання.

Висновки

Аналіз наукової літератури та матеріалів практики розслідування кримінальних правопорушень в аспекті сучасних тенденцій розвитку цифрової криміналістики дає підстави зробити висновок, що вона є важливим напрямом розвитку науки та практичної діяльності в умовах глобальної цифровізації суспільства.

Використання новітніх технологій значно розширює можливості органів кримінальної юстиції у виявленні, фіксації, дослідженні та використанні цифрових доказів у кримінальному провадженні. Однак існує низка викликів, які потребують вирішення. Зокрема: 1) відсутність єдиного термінологічного апарату, як на науковому рівні, так і нормативному; 2) необхідність удосконалення чинного законодавства – потрібно законодавчо закріпити поняття цифрових доказів, їх місце серед джерел доказів; 3) наявність складнощів у виявленні, фіксації та вилученні цифрових слідів – важливим є розроблення практичних рекомендацій та стандартів роботи з відповідними слідами; 4) відсутність ґрунтовних науково-практичних розробок щодо використання інструментів цифрової криміналістики – важливість забезпечення органів кримінальної юстиції новітніми знаннями та засобами, розробка яких має ґрунтуватися на положеннях цифрової криміналістики, узагальненні та аналізі передової судово-слідчої практики, досягненнях науково-технічного прогресу; 5) оснащеність органів кримінальної юстиції та впровадження цифрових технологій у їх діяльність – необхідність розроблення новітніх підходів використання

сучасних технологій під час розслідування та судового розгляду; 6) проблеми щодо встановлення цілісності та автентичності цифрових даних тощо – важливість оновлення та розроблення нових методик проведення судових експертиз з урахуванням досягнень науки і техніки; 7) недостатня обізнаність співробітників органів кримінальної юстиції у роботі з цифровими доказами – важливість постійного підвищення кваліфікації слідчих, прокурорів, детективів, суддів щодо збирання, зберігання, використання, дослідження та оцінки цифрової інформації, а також включення цих питань до навчальних програм студентів юридичних закладів вищої освіти з метою формування компетентностей у сфері цифрової криміналістики; 8) відсутність єдиних міжнародних стандартів щодо використання інструментарію цифрової криміналістики та правових механізмів взаємодії правоохоронних органів – активізація міжнародної співпраці та обміну досвідом як на практичному, так і науковому рівні.

Отже, цифрова криміналістика на сьогодні стоїть на межі стрімкого розвитку, який супроводжується не лише новими можливостями, а й викликами. Для забезпечення ефективного функціонування органів кримінальної юстиції необхідно продовжити розроблення та впровадження інноваційних технологій, вдосконалювати законодавче регулювання використання цифрових доказів та розвивати міжнародне співробітництво у цій сфері. Тільки комплексний підхід дасть змогу забезпечити ефективну боротьбу зі злочинністю в умовах цифрової епохи.

Список використаних джерел

[1] Шепітько В. Теоретико-методологічна модель криміналістики та її нові напрями. *Теорія та практика судової експертизи і криміналістики*. 2021. № 3(25). С. 9–20. https://doi.org/10.32353/khrife.3.2021.02.

[2] Латиш К. В. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika*. 2022. Т. 18. С. 31–37. URL: https://cris.mruni.eu/cris/entities/publication/547c5ae6-e838-4712-ab88-69c59b88f096 (дата звернення: 09.03.2025).

[3] Братішко Н. Напрями використання цифрової криміналістики в умовах воєнного стану. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2024. № 2. С. 282–288. https://doi.org/10.31733/2078-3566-2023-6-282-288.

[4] Shevchuk V. Development trends in criminalistics in the era of digitalization. *Scientific Collection «InterConf+»*. 2023. Vol. 33(155). P. 198–218. https://doi.org/10.51582/interconf.19-20.05.2023.019.

[5] Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України*. 2021. № 8. С. 12–27. http://dx.doi.org/10.33498/louu-2021-08-012.

[6] Miller C. M. A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Sci Int Synerg*. 2023. Vol 6. https://doi.org/10.1016/j.fsisyn.2022.100296.

[7] Allah Rakha N. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*. 2024. Vol. 16(2). P. 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892.

[8] Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2024. Вип. 85, ч. 4. С. 71–75. https://doi.org/10.24144/2307-3322.2024.85.4.10.

[9] Лущик І. В., Тяпкін А. С. Проблемні питання визначення цифрової криміналістики. *Теорія і практика правознавства*. 2023. № 23. С. 135–160. https://doi.org/10.21564/2225-6555.2023.23.281734.

[10] Авдєєва Г. К. Проблеми визначення достовірності цифрових доказів у кримінальному провадженні. *Вісник Луганського навчально-наукового інституту імені Е. О. Дідоренка*. 2024. № 1. С. 33–48. https://doi.org/10.33766/2786-9156.105.33-48.

[11] Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 1. С. 126–143. URL: https://dspace.nlu.edu.ua//jspui/handle/123456789/20008 (дата звернення: 09.03.2025).

[12] Гарасимів О., Марко С., Ряшко О. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. № 2(75). С. 158–162. https://doi.org/10.24144/2307-3322.2022.75.2.25.

[13] Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Т. 2. Вип. 79. С. 214–218. https://doi.org/10.24144/2307-3322.2023.79.2.32.

[14] Матвійчук А. В. Електронні докази у корупційних правопорушеннях. *DICTUM FACTUM*. 2024. № 2(16). С. 239–245. URL: https://df.duit.in.ua/index.php/dictum/article/view/360 (дата звернення: 09.03.2025).

[15] Калінніков О. В. Електронні (цифрові) докази у кримінальному провадженні: поняття та особливості. *World problems and ways of solving modern problems* : The 26th International scientific and practical conference (July 2–5, 2024). Oslo, Norway. International Science Group. 2024. 269 p. URL: https://isg-konf.com/wp-content/uploads/2024/07/WORLD-PROBLEMS-AND-WAYS-OF-SOLVING-MODERN-PROBLEMS.pdf (дата звернення: 09.03.2025).

[16] Цивільний процесуальний кодекс України. *Відомості Верховної Ради України*. 2004. № 40-41, 42. Ст. 492.

[17] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 09.03.2025).

[18] Demidova Y., Latysh K., Kapustina M. Digital evidence in criminal justice: challenges of utilization. *Organizational and legal fundamentals for the formation of a security environment in Ukraine*. Riga, Latvia : Baltija Publishing, 2023. P. 305–318. http://dx.doi.org/10.30525/978-9934-26-363-7-14.

[19] Криміналістика : підручник : у 2-х т. Т. 1 / за ред. В. Ю. Шепітька. Харків : Право, 2019. 456 с.

[20] Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

[21] Шевчук В. М. Роль новітніх цифрових технологій в документуванні та розслідуванні воєнних злочинів в Україні. *Сучасні напрямки розвитку судової експертизи та криміналістики* : матеріали Всеукр. наук.-практ. конф. з нагоди 110-річчя діяльності Одес. наук.-дослідн. Ін-ту суд. експертиз М-ва юстиції України (м. Одеса, 5 вересня 2024 р.). Одеса : Юридика, 2024. С. 510–513.

[22] Шевчук В. М. Використання технологій штучного інтелекту та процес цифровізації криміналістики в умовах війни. *Актуальні проблеми протидії злочинності та корупції* : зб. тез Всеукр. наук.-практ. конф. Харків : Юрайт, 2023. С. 171–176.

[23] Яремчук В. О. Новітні криміналістичні науково-технічні засоби. *Юридичний науковий електронний журнал*. 2024. № 4. С. 659–660. https://doi.org/10.32782/2524-0374/2024-4/157

[24] Баранчук В. В. 3D сканування як спосіб фіксації на місці злочину: переваги й недоліки. *Юридичний бюлетень*. 2020. Вип. 16. С. 280–286. https://doi.org/10.32850/LB2414-4207.2020.16.01.

[25] Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с.

[26] Суддя Верховного Суду проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1751385/ (дата звернення: 09.03.2025).

[27] Ліхтанська А. П., Михайлов В. О. Використання OSINT в кримінальному праві України. *DICTUM FACTUM*. 2024. № 1(15). С. 105–111. URL: https://df.duit.in.ua/index.php/dictum/article/view/319/286 (дата звернення: 09.03.2025).

References

[1] Shepitko, V. (2021). Theoretical and methodological model of criminalistics and its new directions. *Theory and Practice of Forensic Science and Criminalistics, 3*(25), 9-20. https://doi.org/10.32353/khrife.3.2021.02

[2] Latysh, K.V. (2022). Digital forensics during the war in Ukraine: Opportunities for the use of specialized knowledge in the field of information technology. *Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika, 18*, 31–37. Retrieved from https://cris.mruni.eu/cris/entities/publication/547c5ae6-e838-4712-ab88-69c59b88f096.

[3] Bratishko, N. (2024). Directions of using digital forensics under martial law. *Scientific Bulletin of the Dnipro State University of Internal Affairs, 2*, 282-288. https://doi.org/10.31733/2078-3566-2023-6-282-288.

[4] Shevchuk, V. (2023). Development trends in criminalistics in the era of digitalization. *Scientific Collection "InterConf+", 33*(155), 198-218. https://doi.org/10.51582/interconf.19-20.05.2023.019.

[5] Shepitko, V., & Shepitko, M. (2021). The doctrine of forensic science and forensic expertise: Formation, current state, and development in Ukraine. *Law of Ukraine, 8*, 12-27. http://dx.doi.org/10.33498/louu-2021-08-012.

[6] Miller, C.M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy, 6*. https://doi.org/10.1016/j.fsisyn.2022.100296.

[7] Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review, 16*(2), 23-54. https://doi.org/10.22201/iij.24485306e.2024.2.18892.

[8] Demidova, Y.Y. (2024). Digital traces of a criminal offense: Concept and features. *Scientific Bulletin of Uzhhorod National University. Law Series, 85*(4), 71-75. https://doi.org/10.24144/2307-3322.2024.85.4.10.

[9] Lushchyk, I.V., & Tyapkin, A.S. (2023). Problematic issues in defining digital forensics. *Theory and Practice of Jurisprudence, 23*, 135-160. https://doi.org/10.21564/2225-6555.2023.23.281734.

[10] Avdeeva, G.K. (2024). Problems of determining the reliability of digital evidence in criminal proceedings. *Bulletin of the Luhansk Educational and Scientific Institute named after E. O. Didorenko, 1*, 33-48. https://doi.org/10.33766/2786-9156.105.33-48.

[11] Avdeeva, G., & Zhivutska-Kozlovska, E. (2023). Problems of using digital evidence in criminal proceedings in Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics, 1*, 126-143. Retrieved from https://dspace.nlu.edu.ua//jspui/handle/123456789/20008.

[12] Harasymiv, O., Marko, S., & Ryashko, O. (2023). Digital evidence: Some problematic issues regarding their concept and use in criminal proceedings. *Scientific Bulletin of Uzhhorod National University. Law Series, 2*(75), 158-162. https://doi.org/10.24144/2307-3322.2022.75.2.25.

[13] Angelenyuk, A.-M.Y. (2023). The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues). *Scientific Bulletin of Uzhhorod National University. Law Series, 2*(79), 214-218. https://doi.org/10.24144/2307-3322.2023.79.2.32.

[14] Matviichuk, A.V. (2024). Electronic evidence in corruption offenses. *DICTUM FACTUM, 2*(16), 239-245. Retrieved from https://df.duit.in.ua/index.php/dictum/article/view/360.

[15] Kalinnikov, O.V. (2024). Electronic (digital) evidence in criminal proceedings: Concept and features. *The 26th International Scientific and Practical Conference "World Problems and Ways of Solving Modern Problems" (July 2-5, 2024, Oslo, Norway)*. International Science Group. Retrieved from https://isg-konf.com/wp-content/uploads/2024/07/WORLD-PROBLEMS-AND-WAYS-OF-SOLVING-MODERN-PROBLEMS.pdf.

[16] Civil Procedure Code of Ukraine. (2004). *Official Bulletin of the Verkhovna Rada of Ukraine, 40-41, 42,* art. 492.

[17] Council of Europe Convention "Convention on Cybercrime". (November 23, 2001). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575.

[18] Demidova, Y., Latysh, K., & Kapustina, M. (2023). Digital evidence in criminal justice: Challenges of utilization. In *Organizational and Legal Fundamentals for the Formation of a Security Environment in Ukraine: Scientific Monograph* (pp. 305–318). Riga, Latvia: Baltija Publishing. http://dx.doi.org/10.30525/978-9934-26-363-7-14

[19] Shepitko, V.Yu. (Ed.). (2019). Criminalistics. (Vols. 1-2), *Vol. 1.* Kharkiv: Pravo.

[20] Gutsalyuk, M.V., Havlovskyi, V.D., & Khakhanovskyi, V.G. (2020). The use of electronic (digital) evidence in criminal proceedings: Methodological recommendations. O.V. Korneiko (Ed.). Kyiv: Publishing House of the National Academy of Internal Affairs.

[21] Shevchuk, V.M. (2024). The role of modern digital technologies in documenting and investigating war crimes in Ukraine. *Modern Directions of Forensic Science and Criminalistics: Materials of the All-Ukrainian Scientific and Practical Conference Dedicated to the 110th Anniversary of the Odesa Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine. (September 5, 2024).* Odesa: Yuridika, 510-513.

[22] Shevchuk, V.M. (2023). The use of artificial intelligence technologies and the process of digitalization of criminalistics in wartime. *Current Problems of Combating Crime and Corruption: Collection of Abstracts of the All-Ukrainian Scientific and Practical Conference*. Kharkiv: Yurayt, 171-176.
[23] Yaremchuk, V.O. (2024). Modern forensic scientific and technical tools. *Legal Scientific Electronic Journal, 4*, 659–660. https://doi.org/10.32782/2524-0374/2024-4/157.
[24] Baranchuk, V.V. (2020). 3D scanning as a way of recording crime scenes: Advantages and disadvantages. *Legal Bulletin, 16*, 280-286. https://doi.org/10.32850/LB2414-4207.2020.16.01.
[25] Torbas, O.O. (2024). *OSINT in criminal investigations*. Odesa: Yurydyka.
[26] Supreme Court Judge analyzed the criteria for the admissibility and reliability of electronic evidence in criminal proceedings. (n.d.). Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/1751385/.
[27] Likhtanska, A.P., & Mykhailov, V.O. (2024). The use of OSINT in the criminal law of Ukraine. *DICTUM FACTUM, 1*(15), 105-111.

Євгенія Євгеніївна Демидова
кандидатка юридичних наук, доцентка
доцентка кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, Харків, Україна
e-mail: ye.ye.demydova@nlu.edu.ua
ORCID 0000-0002-5049-7946

Yevheniia Ye. Demydova
Ph.D. in Law, Associate Professor
Associate Professor of the Criminalistics Department
Yaroslav Mudryi National Law University
61024, 77, Hryhoriia Skovorody Str., Kharkiv, Ukraine
e-mail: ye.ye.demydova@nlu.edu.ua
ORCID 0000-0002-5049-7946

Рекомендоване цитування: Демидова Є. Є. Тенденції розвитку цифрової криміналістики: виклики та перспективи для органів кримінальної юстиції. *Проблеми законності*. 2025. Вип. 168. С. 164–182. https://doi.org/10.21564/2414-990X.168.324997.

Suggested Citation: Demydova, Ye.Ye. (2025). Trends in the Development of Digital Forensics: Challenges and Prospects for Criminal Justice Agencies. *Problems of Legality, 168*, 164-182. https://doi.org/10.21564/2414-990X.168.324997.

Статтю подано / Submitted: 30.01.2025
Доопрацьовано / Revised: 26.02.2025
Схвалено до друку / Accepted: 25.03.2025
Опубліковано / Published: 31.03.2025