***Стратонов Василь Миколайович***
професор кафедри національного, міжнародного права та правоохоронної діяльності Херсонського державного університету; доктор юридичних наук, професор, заслужений юрист України
***Дзюрбель Андрій Дарійович***
старший викладач кафедри кримінального права та процесу Західноукраїнського національного університету, кандидат юридичних наук

# ЦИФРОВА ТА МОБІЛЬНА КРИМІНАЛІСТИКА: РОЗГОРНУТИЙ ОГЛЯД

У роботі представлено узагальнений огляд двох споріднених, але різнорівневих напрямів криміналістики: цифрової криміналістики (Digital Forensics) та мобільної криміналістики (Mobile Forensics), визначено їхні особливості, методологію, інструментарій, юридичні та етичні аспекти. Наведено виклики, практичні рекомендації як для сторони обвинувачення так для сторони захисту, окреслено тенденції подальшого розвитку галузі. Також наведено узагальнену інформацію на основі власних наукових напрацювань.

У добу глобальної цифровізації цифрові сліди стають одним із ключових джерел доказів у розслідуваннях. Нами було проведено аналіз інформації та визначено її як об'єкт [1], надано окремі особливості та характеристики «комп'ютерних злочинів» [2], охарактеризовано деякі види комп'ютерної злочинності та кіберзлочинності в Україні [3]. Доведено, що накопичені в системі криміналістичних обліків різноманітні види біометричних персональних даних можуть успішно використовуватися в процесі розслідування кримінальних правопорушень, а в окремих випадках й приватними особами в межах їх статутних повноважень. Ми також звернули увагу, що поряд з позитивними результатами такої діяльності є певні ризики, а саме наявність загрози витоку та отримання доступу до біометричних даних сторонніми особами, про що свідчить негативна судова практика окремих країн щодо незадовільного збирання, обробки, зберігання та використання біометричних персональних даних. З огляду на зазначене, констатовано, що збирання, обробка та використання біометричних персональних даних з метою їх використання в процесі розслідування кримінальних правопорушень, мають відповідати певним вимогам, а саме: володільцем бази біометричних персональних даних має бути тільки держава в особі спеціального державного органу. Відповідно держава має забезпечувати зберігання й захист біометричних персональних даних [4]. Зберігання даних повинно забезпечувати їх безпеку, прикладом нашої правоти були унеможливлення доступу військових рф до персональних даних відділу кадрів Херсонського державного університету. Створення та зберігання інформації в хмарному середовищі дозволило її відновити після релокації університету на підконтрольну територію. Таким чином поєднання цифровізації з управлінськими процесами убезпечило та зберегло життя багатьом співробітникам.

Вже в 2022 році ми прийшли до висновку щодо необхідності нормативно-правового визначення штучного інтелекту, як інструменту в кримінальному судочинстві [5]. Зважаючи на постійний розвиток та можливості інформаційних систем та мобільних пристроїв ми прийшли до висновку, а саме доцільності створення окремого напряму в криміналістиці який вивчатиме «комп'ютерні злочини», враховуючи потреби практики розроблення окремих методик розслідування даних видів злочинів. Ми вбачаємо доцільність розгляду в цій систем цифрової та мобільної криміналістики. Цифрова криміналістика охоплює аналіз комп'ютерів, серверів, хмарних середовищ, мережевих журналів, пристроїв Інтернету речей (IoT) тощо. Мобільна криміналістика фокусується на дослідженні смартфонів і планшетах, що містять персональні дані, геолокацію та комунікації користувачів [6, с. 5].

Обидва напрями вже швидко розвиваються під впливом технологічних змін, зокрема шифрування та впровадження нових ОС. Визначаючи межі даних напрямів можемо зауважити, що цифрова криміналістика – це процес виявлення, збереження, аналізу та представлення цифрових доказів із дотриманням їхньої достовірності [7, с. 15].

Мобільна криміналістика є підполем цифрової, орієнтованим на мобільні пристрої, що мають різноманітні ОС (Android, iOS), власницькі файлові системи й засоби шифрування [8, с. 48].

Методологія розслідувань даних видів кримінальних правопорушень повинні засновуватись на чотирьох типових етапів, які включатимуть:

1) планування та правове обґрунтування;
2) збереження та вилучення (forensic imaging, клонування);
3) аналіз (таймлайни, відновлення файлів);
4) представлення результатів [6, с. 29].

У мобільній криміналістиці застосовують логічні, файлові, фізичні та хмарні методи вилучення даних. Постійні оновлення ОС і шифрування потребують спеціалізованих інструментів і валідації процедур [8, с. 51].

Технічні аспекти та інструменти які дозволять приймати рішення цифрової криміналістики є Autopsy, EnCase, FTK, X-Ways. Мобільна криміналістика використовує Cellebrite UFED, MSAB XRY, Oxygen Forensic Detective, Magnet AXIOM. Значна роль належить open-source-інструментам, які забезпечують прозорість і доступність аналітики [9, с. 76].

Ми працюємо в умовах принципів законності тож важливо дотримуватись юридичних та етичних вимог. Дії слідчих мають ґрунтуватися на правових підставах обшуку й вилучення. Важливим є ведення ланцюга збереження доказів (chain of custody). Водночас необхідно дотримуватись принципу захисту приватності при роботі з персональними даними [4; 10, с. 34].

Кріста Міллер вказує «Цифрові докази є важливими для кримінальних розслідувань та судового переслідування, але їх використання пов'язане з певними труднощами: швидкими змінами в технологіях, необхідністю повідомляти про ці зміни зацікавленим сторонам та соціально-політичним ландшафтом, який залишає мало місця для помилок, особливо щодо конфіденційності електронних даних. У системі кримінального правосуддя ці проблеми можуть впливати на допустимість доказів та їх належне подання в суді, а також на те, як висуваються звинувачення та вирішуються справи» [10, с. 76].

Один огляд 145 справ, оскаржених у федеральних окружних судах США між 2010 і 2015 роками, показав, що лише 22 «ґрунтувалися на науці комп’ютерної криміналістики, включаючи доказову силу, автентичність, чутки, релевантність та наукову цінність» [11]. Мартін Новак зазначає, що «хоча використання комп’ютерної криміналістики в кримінальних розслідуваннях розширилося в останні роки, існує мало емпіричних доказів щодо поширеності використання цифрових доказів у судовій системі та його впливу на результати судового переслідування» [11].

Таким чином ми спостерігаємо, що технічні труднощі пов’язані з шифруванням, закритими форматами та швидким оновленням ОС. А також мають організаційні обмеження, а саме дефіцит кадрів і відсутність єдиних протоколів [12, с. 81]. Перспективними напрямами є використання штучного інтелекту в профілюванні особи злочинця [13], окремого дослідження потребує використання електронних систем [14], особливо в процесі формування доказів для розгляду в міжнародних судах [15].

Тож узагальнюючи можемо констатувати, що цифрова та мобільна криміналістика є взаємодоповнюючими сферами. Цифрова криміналістика та мобільна криміналістика тісно пов'язані: перша надає загальні підходи та принципи, друга — деталізує методи роботи зі смартфонами й планшетами та іншою криміналістично значимою інформацією. Сучасні виклики вимагають поєднання технічної, правової та етичної компетенцій. Через швидкі технологічні зміни практикам потрібні постійні оновлення знань, валідовані інструменти та міжнародна співпраця. Рекомендовано поєднувати технічні навички з розумінням юридичного контексту та реалізації напрацювань науковців. Підвищення кваліфікації, розробка відкритих стандартів і міжнародна співпраця є запорукою ефективного розвитку криміналістичних знань.

**Список використаних джерел**


1. Стратонов В.М. Інформація та інформаційні відносини як новий криміналістичний об’єкт. Південноукраїнський правничий часопис №4, 2019. 84–89 с.
2. Стратонов В.М. «Комп’ютерні злочини» окремі особливості та характеристики. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. №2. С.134-141. URL: https://visnik.dduvs.in.ua/?page_id=48
3. Стратонов В., Слінько Д., Слінько С. «Деякі види комп’ютерної злочинності та кіберзлочинності в Україні» *Доступ до правосуддя у Східній Європі* 2021, *Т4,* 3(11) С. *191–197* URL: https://ajee-journal.com/some-types-of-computer-crime-and-cybercrime-in-ukraine https://doi.org/10.33327/AJEE-18-4.3-n000078
4. Violetta E. Konovalova, Vasyl M. Stratonov, & Iryna V. Savelieva (2021). Biometric personal data and their use in the investigation of criminal offences. *Journal of the National Academy of Legal Sciences of Ukraine*, (4), P. 289-300 URL: https://visnyk.kh.ua/uk/journals/visnik-naprnu-4-2021-r/biometrichni-personalni-dani-ta-yikh-vikoristannya-v-rozsliduvanni-kriminalnikh-pravoporushen
5. Стратонов В.М., Проценко М.В. Штучний інтелект у судочинстві України: нормативно-правове визначення. Криміналістика і судова експертиза: міжвідом. наук.-метод. зб. / Київський НДІ судових експертиз; редкол.: Д. В. Журавльов (голов. ред.), О. Г. Рувін (заст. голов. ред.) та ін., Київ : Видавництво Ліра-К, 2022. Вип. 67. 704 с.

6. Rick Ayers, Sam Brothers, Wayne Jansen Guidelines on Mobile Device Forensics NIST (Special Publication 800-101 Revision Gaithersburg: National Institute of Standards and Technology, 2014 URL: https://nvlpubs.nist.gov/nistpubs/ specialpublications/nist.sp.800-101r1.pdf

7. Frank Breitinger, Jan-Niclas Hilgert, Christopher Hargreaves, John Sheppard, Rebekah Overdorf, Mark Scanl DFRWS EU 10-year review and future directions in Digital Forensic Research. Forensic Science International, 2024. URL: https://dfrws.org/wp-content/ uploads/2024/03/DFRWS-EU-10-year-review-and-future-direct_2024_Forensic-Science -Internationa.pdf

8. Гуммерт, Крістіан, Pawlaszczyk, Dirk Mobile Forensics – The File Format Handbook. OAPEN, 2023. URL: https://library.oapen.org/handle/20.500.12657/ 54441

9. Nishchal Soni Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements and Future Challenges. Herald Open Access, 2023. URL: https://www.heraldopenaccess.us/article_pdf/34/digital-forensicsconfronting-modern-cyber-crimes-technological-advancements-and-future-challenges.pdf

10. Christa M. Miller A survey of prosecutors and investigators using digital evidence. PubMed Central (PMC), 2023. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC10311201/

11. Новак Мартін. Цифрові докази у кримінальних справах, що розглядаються апеляційними судами США: тенденції та питання для розгляду. Журнал цифрової криміналістики, безпеки та права. 2020; 14(4). URL: https://scholar.google.com/scholar_lookup?journal=Journal%20of%20Digital%20Forensics,%20Security%20and%20Law&title=Digital%20evidence%20in%20criminal%20cases%20before%20the%20U.S.%20Courts%20of%20appeal:%20trends%20and%20issues%20for%20consideration&author=Martin%20Novak&volume=14&issue=4&publication_year=2020&

12. Абір Д. Салман, Екрам Х. Хасан Оглядове дослідження цифрової криміналістики: проблеми, застосування та інструменти. 6-та Міжнародна конференція з розвитку інженерії електронних систем (DeSE) 2023 року URL: https://www.researchgate.net/publication/379174338_Survey_Study_of_Digital_Forensics_Challenges_Applications_and_Tools

13. Стратонов В., Дзюрбель А. Використання штучного інтелекту та інформаційних можливостей у створенні профіля злочинця. Науковий вісник Херсонського державного університету**.** Серія: «Юридичні науки» Випуск 5. 2024. Гельветика, 2024. С.21-27 URL: https://lj.journal.kspu.edu/index.php/lj/issue/view/20

14. Стратонов В. Актуальні напрями використання електронних інформаційних систем в умовах воєнного стану. Науковий вісник Херсонського державного університету**.** Серія: «Юридичні науки» Випуск 1. 2025. Гельветика, 2025. С. 36-42 DOI https://doi.org/10.32999/ksu2307-8049/2025-1-6 URL: https://lj.journal.kspu.edu/index.php/lj/article/view/ 463/ 417

15. Стратонов В. Використання цифрових технологій у виявленні та документуванні фактів експлуатації людини під час збройних конфліктів: Доказова база в міжнародних судах. Вчені записки ТНУ імені В.І. Вернадского. Серія: юридичні науки Том 36 (75) №1. 2025. С.173-178 DOI https://doi.org/10.32782/TNU-2707-0581/2025.1/28 URL:https://www.juris.vernadskyjournals.in.ua/journals/2025/1_2025/30.pdf