закупівель: дис. … канд. юрид. наук: спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». – Національна академія внутрішніх справ, Київ, 2019. 258 с.

8. Тимчишин А. М. Особливості використання спеціальних знань під час огляду місця події. Juris Europensis Scientia. 2023. № 1. С. 147–152. URL: http://jes.nuoua.od.ua /archive/1_2023/28.pdf.

9. Участь спеціаліста у проведенні слідчих (розшукових) дій під час розслідування корупційних злочинів: метод. рек. / Б. Б. Теплицький, О. М. Шрамко, В. В. Юсупов. Київ: Нац. акад. внутр. справ, 2019. 68 с.

10. Цимбал П.В. Попередження, виявлення, розкриття та розслідування податкових злочинів: монографія. Ірпінь : Національний університет ДПС України, 2009. 408 с.

Погорецький Микола Анатолійович,
доктор юридичних наук, професор,
проректор з науково-педагогічної роботи
Київського національного університету
імені Тараса Шевченка

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ДОКАЗУВАННІ ТА РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

В останні роки кількість воєнних злочинів значно зросла, особливо у контексті повномасштабного вторгнення рф в Україну. Наприклад, у 2022 році кількість зареєстрованих кримінальних проваджень за фактами порушення законів та звичаїв війни сягнула понад 60 тисяч, що становило 16,65 % усіх злочинів. У 2023 році кількість таких злочинів продовжувала залишатися високою, підтверджуючи тенденцію до зростання цього виду злочинності. Масовість і жорстокість таких злочинів, як розстріли евакуаційних колон, катування, зґвалтування, примусова депортація цивільного населення, руйнування цивільної інфраструктури та культурних об'єктів, створюють виклик для правоохоронних органів щодо їх ефективного документування та розслідування.

У сучасному кримінальному процесі цифрові технології відіграють ключову роль у документуванні й доказуванні воєнних злочинів. Це особливо актуально в умовах повномасштабної збройної агресії, коли міжнародне право

потребує ефективних інструментів збору, обробки, перевірки та захисту доказів. Технологічні рішення, що активно впроваджуються в Україні, дають змогу фіксувати масові порушення міжнародного гуманітарного права з високою точністю і забезпечувати їх прийнятність у міжнародних судових інстанціях.

Геоінформаційні системи (ГІС) використовуються для картографування місць злочинів, фіксації обстрілів, виявлення масових поховань, відстеження переміщень військ та техніки. Приклади включають документування подій у Бучі, Ізюмі, Чернігівській області, де масштабні руйнування та численні факти порушення міжнародного гуманітарного права були зафіксовані за допомогою супутникових знімків та ГІС-інструментів. Також ГІС були використані під час розслідування катастрофи МН17, де зображення дозволили встановити місце запуску ракети та маршрут переміщення озброєння. В Україні супутникові дані застосовуються для фіксації змін у ландшафті, виявлення нових могил та пошкоджень цивільної інфраструктури.

Штучний інтелект (ШІ) дозволяє обробляти великі масиви інформації: фотографії, відео, метадані, дані соцмереж, GPS-треки. Завдяки ШІ можливо швидко виявити закономірності, встановити підозрюваних та зібрати докази. У системах типу Clearview AI або Artellence використовується розпізнавання облич, а також автоматичне порівняння з базами відкритих джерел. ШІ допомагає відслідковувати рухи техніки, визначати місця обстрілів, знаходити акаунти можливих воєнних злочинців. Особливо ефективним є поєднання алгоритмів глибинного навчання із геолокацією та часовими мітками.

Біометричні технології (відбитки пальців, ДНК, розпізнавання обличчя) значно підвищують швидкість і точність ідентифікації жертв та підозрюваних. Пристрої ANDE RAPID DNA, що використовуються Національною поліцією України, дозволяють отримати ДНК-профіль у польових умовах за 90 хвилин. Ці технології застосовувалися під час ексгумації тіл у Бучі, Ізюмі, Херсонській області. Використання пересувних лабораторій стало ключовим для оперативного збору доказів.

Блокчейн-технології використовуються для захисту цифрових доказів від змін. Наприклад, платформа «Воєнний злочин» забезпечує фіксацію, збереження та ланцюг передачі доказів, отриманих у ході досудового розслідування. Така система гарантує автентичність матеріалів для їх подання до

Міжнародного кримінального суду (МКС) та інших міжнародних трибуналів. Блокчейн також може фіксувати логи доступу до файлів, що важливо для захисту прав сторін процесу.

Застосування відкритих джерел (OSINT) набуває великого значення. Це включає відео, фото, пости з соцмереж, супутникові знімки. Протокол Берклі, ухвалений ООН, встановлює критерії перевірки, збереження та обробки таких даних. Українські правоохоронці, зокрема в рамках співпраці з Truth Hounds, успішно використовують OSINT для фіксації порушень, верифікації місць злочину та ідентифікації виконавців.

Міжнародні організації (МКС, Європол, ICPA, ООН, Truth Hounds) надають методологічну, технічну та ресурсну підтримку Україні. ООН розробила стандарти верифікації цифрових доказів (OHCHR Digital Evidence Standards), а МКС надає правову оцінку зібраним матеріалам. ICPA в Гаазі координує спільну роботу слідчих груп, а Європол сприяє стандартизації цифрових процедур у рамках міжнародного співробітництва.

Судовий контроль і прокурорський нагляд мають забезпечувати законність використання новітніх технологій. Це включає забезпечення допустимості доказів, дотримання прав людини, конфіденційності персональних даних. Зокрема, збір даних через супутники або дрони має здійснюватися з дотриманням вимог щодо інтервенцій у приватне життя.

Отже, цифрова трансформація кримінального процесу під тиском війни демонструє, що сучасні технології не лише підвищують ефективність документування, але й змінюють підходи до доказування. Інтеграція таких технологій потребує оновлення нормативної бази, чіткої регламентації процедур, міжнародного визнання інструментів та етичного балансу між ефективністю й правами людини. Український досвід у цьому контексті може стати зразком для інших держав у постконфліктному відновленні правосуддя.

Зростання кількості воєнних злочинів, зокрема через агресію рф проти України, значно ускладнює завдання їх документування та розслідування традиційними методами, що вимагає активного застосування новітніх технологій. Дослідження підкреслює особливу ефективність космічних та геоінформаційних технологій (зокрема супутникових знімків), які надають надійні докази злочинів, практично унеможливлюючи фальсифікацію через цифрові електронні підписи. Приклади їхнього використання – масові поховання у

Бучі та Ізюмі, руйнування цивільної інфраструктури в Маріуполі, Херсоні, Запоріжжі, Чернігові, Сумах, Харкові та інших містах і селах – демонструють значення цих технологій у міжнародних судових процесах, включаючи Міжнародний кримінальний суд.

Важливими є також цифрові та біометричні технології, зокрема штучний інтелект, блокчейн, розпізнавання обличчя та ДНК-аналіз. Використання цих технологій в Україні забезпечило швидку ідентифікацію як жертв, так і потенційних злочинців. Системи на основі блокчейн створюють надійні та прозорі ланцюги доказів, важливі для подальших міжнародних судових розглядів.

Алгоритми машинного навчання допомагають ефективно аналізувати великі масиви цифрових даних, значно скорочуючи час розслідування та забезпечуючи високий рівень доказової бази. Такі технології активно використовуються в OSINT-дослідженнях та міжвідомчих базах даних, що суттєво покращує координацію правоохоронних органів.

Разом з тим, використання новітніх технологій ставить низку правових, етичних та технічних питань, таких як захист персональних даних, запобігання зловживанням і дотримання прав людини. Це потребує створення відповідних правових та етичних рамок на національному і міжнародному рівнях.

Таким чином, інтеграція новітніх технологій у процес розслідування воєнних злочинів є критично важливою для досягнення справедливості для потерпілих та ефективного притягнення винних до відповідальності. Водночас необхідні подальші дослідження та нормативне регулювання цього процесу для забезпечення відповідності міжнародним стандартам і захисту прав людини.

Попри значні переваги, використання цифрових технологій у доказуванні супроводжується низкою складних викликів. Насамперед, йдеться про правову невизначеність щодо допустимості новітніх цифрових доказів, зібраних, наприклад, через OSINT або автоматичні ШІ-системи. Деякі категорії цифрових слідів можуть викликати сумніви у судах через відсутність підтвердженої автентичності, порушення ланцюга збереження або недостатню прозорість джерел.

Також проблемою залишається ризик порушення прав людини. Застосування ШІ, розпізнавання облич, біометричних засобів і аналізу поведінки в мережі може втручатися в приватність, а їх автоматичні висновки не завжди піддаються

ефективному оскарженню. Інституційний контроль, включно із судовим і прокурорським, часто не має достатніх процедур для оцінки правомірності таких даних. У міжнародному праві також відсутні єдині критерії прийнятності доказів, зібраних дронами, через блокчейн або засобами дистанційного моніторингу в реальному часі.

Проблемою є і нерівномірний доступ слідчих до технологій: деякі регіони мають обмежені ресурси для роботи з супутниковими зображеннями, ГІС або ШІ. Також спостерігається недостатня підготовка кадрів до роботи з високотехнологічними засобами — як у зборі, так і в поданні та захисті цифрових доказів у суді. Відсутність уніфікованих національних інструкцій і підзаконних актів лише ускладнює ситуацію.

Необхідною є подальша гармонізація процесуальних кодексів із цифровими реаліями, розробка механізмів перевірки достовірності та допустимості новітніх доказів, а також створення судової практики, що визнає їх повноцінним елементом доказування при дотриманні гарантій змагальності, рівності сторін та справедливості процесу.

Отже, цифрова трансформація кримінального процесу під тиском війни демонструє, що сучасні технології не лише підвищують ефективність документування, але й змінюють підходи до доказування. Інтеграція таких технологій потребує оновлення нормативної бази, чіткої регламентації процедур, міжнародного визнання інструментів та етичного балансу між ефективністю й правами людини. Український досвід у цьому контексті може стати зразком для інших держав у постконфліктному відновленні.

Список використаних джерел:

1. Berkeley Protocol on Digital Open Source Investigations. Office of the United Nations High Commissioner for Human Rights. Geneva, 2019. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/05/Berkeley-Protocol-ENG.pdf

2. Бондар В. С., Парфьонов В. Ю. Про особливості застосування новітніх технологій у документуванні та розслідуванні окремих видів воєнних злочинів. Криміналістичний вісник. 2022. № 1(1). С. 123–130.

3. Brenner, Susan W. Cybercrime: Criminal Threats from Cyberspace. Praeger Security International, 2009. 320 p.

4.Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2019. 650 p.

5. Clough J. Principles of Cybercrime. Cambridge University Press, 2015. 450 p.

6. Golsan R. The Papon Affair: Memory and Justice on Trial. French Politics, Culture & Society. 2000. Vol. 18(2). P. 1–17.

7. Golsan R. The Trial of Maurice Papon: A Study in the Politics of Memory. In: Golsan R. (ed.). *Memory and Justice*. Lincoln: University of Nebraska Press, 2001. P. 123–145.

8. Memory and Justice. Ed. R. Golsan. Lincoln: University of Nebraska Press, 2001. P. 123–145.

9. Kerr O. S. Computer Crime Law. West Academic Publishing, 2022. 700 p.

10. Mann S., Roberts C. Internet Crimes: A Guide to Effective Investigations. CRC Press, 2017. 380 p.

11. Minnesota Protocol on the Investigation of Potentially Unlawful Deaths. Minnesota Medical Examiner's Office. 2016. URL:
https://www.law.umn.edu/sites/law.umn.edu/files/minnesota_protocol.pdf

12. Офіс Генерального прокурора. Статистика. URL: https://gp.gov.ua/ua/posts/statistika

13. Погорецький М. А. Джерела судових доказів. Питання боротьби зі злочинністю: збірник наукових праць. 2005. № 10. С. 167–178.

14. Погорецький М. А. Докази у кримінальному процесі. Вісник прокуратури. 2003. № 2. С. 59–65.

15. Погорецький М. А. Докази у кримінальному процесі: проблемні питання. Часопис Національного університету «Острозька академія». Серія «Право». 2011. № 1(3). URL: https://lj.oa.edu.ua/articles/2011/n1/11pmappp.pdf

16. Погорецький М. А. Негласні слідчі (розшукові) дії: проблеми провадження та використання результатів у доказуванні. Юридичний часопис Національної академії внутрішніх справ. 2013. № 1. С. 270–277.

17. Погорецький М. А. Оперативно-розшукові заходи: проблеми правового регулювання. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2007. № 14. С. 135–145.

18. Погорецький М. А. Про співвідношення джерел фактичних даних і джерел доказів у кримінальному процесі. Право України. 2009. № 1. С. 80–85.

19. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Харків: Арсіс ЛТД, 2007. 576 с.

20. Погорецький М. А., Лисаченко Є. І. Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України. Вісник кримінального судочинства. 2022. № 3–4. С. 20–34. DOI: 10.17721/2413-5372.2022.3-4/20-34.

21. Погорецький М. А., Сергєєва Д. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2014. № 2(33). С. 137–141.

22. Погорецький М. А., Шеломенцев В. Пошук фактичних даних про злочини. Міжнародна поліцейська енциклопедія: у 10 т. / відп. ред. В. В. Коваленко, Є. В. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. Київ: Атіка, 2010. Т. VI. С. 750–751.

23. Чернявський С. С., Присяжний В. І., Стрільців О. М. та ін. Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: метод. рек. / за заг. ред. М. С. Цуцкірідзе. Київ: Нац. акад. внутр. справ, 2023. 92 с.