Погорецький М. А.,
доктор юридичних наук, професор,
проректор з науково-педагогічної роботи
Київського національного університету
імені Тараса Шевченка
***ORCID ID:** 0000-0003-0936-0929*

DOI: *https://doi.org/10.17721/2413-5372.2023.3-4/84-102*

УДК 343.985:341.322.5

ЗАСТОСУВАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ ТА ДОКАЗУВАННІ ВОЄННИХ ЗЛОЧИНІВ (ПРОБЛЕМНІ ПИТАННЯ)

***Анотація**. Стаття присвячена аналізу ролі та потенціалу новітніх технологій у документуванні, розслідуванні та доказуванні воєнних злочинів в умовах російської агресії проти України.*

Метою статті *є аналіз ролі новітніх технологій у документуванні, розслідуванні та доказуванні воєнних злочинів й обґрунтування необхідності подальшого впровадження найефективніших із них у теорію оперативно-розшукової діяльності, криміналістики та кримінального процесу, а також у практику правоохоронних органів.*

Автор детально аналізує можливості та практичні аспекти використання космічних і геоінформаційних технологій, зокрема супутникових знімків, які дозволяють отримати точні, оперативні та незаперечні докази воєнних злочинів. Наведено приклади успішного застосування таких технологій у випадках масових поховань у Бучі та Ізюмі, а також масштабних руйнувань цивільної інфраструктури у Маріуполі й Харкові.

Дослідження підкреслює особливу ефективність космічних та геоінформаційних технологій (зокрема супутникових знімків), які надають надійні докази злочинів, практично унеможливлюючи фальсифікацію через цифрові електронні підписи.

Обґрунтовується, що 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.

Доводиться, що 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.

Акцентується, що 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.

Робиться висновок, що активне впровадження і нормативне забезпечення новітніх технологій є ключовим фактором підвищення ефективності документувань, розслідувань та доказування воєнних злочинів для забезпечення справедливості у національному та міжнародному кримінальному правосудді. Інтеграція новітніх технологій у процес документування та розслідування воєнних злочинів є критично важливою для досягнення справедли-

вості 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.

Ключові слова: воєнні злочини, космічні технології, геоінформаційні системи, супутникові знімки, штучний інтелект, блокчейн, біометричні технології, OSINT, міжнародне право, права людини, докази, доказування, документування, розслідування, судовий контроль, прокурорський нагляд.

Постановка проблеми. 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[1]. 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.

Традиційні методи розслідування стають недостатньо ефективними в умовах сучасних викликів. Це обумовлює необхідність активного застосування новітніх технологій для ефективного розслідування воєнних злочинів, що включає:

Космічні та геоінформаційні технології. Дистанційне зондування Землі (ДЗЗ) і супутникові знімки дозволяють правоохоронним органам отримати об'єктивну, детальну і актуальну інформацію про стан територій, на яких відбуваються злочини. Супутникові знімки забезпечують високу достовірність доказів, що майже унеможливлює їх підробку, оскільки ці знімки мають цифровий електронний підпис і часто отримані з різних супутників. Космічний моніторинг забезпечує глобальність, оперативність та безперервність контролю територій, що особливо важливо у зонах бойових дійКосмос.

Цифрові та біометричні технології. Впровадження штучного інтелекту, блокчейну, цифрового аналізу даних, систем біометричної ідентифікації та використання безпілотників значно посилює спроможність правоохоронних органів у зборі, аналізі та збереженні доказів. Ці технології дозволяють ефективно ідентифікувати злочинців, аналізувати величезні обсяги цифрових слідів (соціальні мережі, GPS-записи, фото та відеоматеріали), а також гарантувати непідробність та прозорість доказів завдяки використанню технологій блокчейну.

Автоматизація та машинне навчання. Алгоритми машинного навчання дають змогу аналізувати великі масиви інформації, виявляти закономірності злочинної діяльності, передбачати напрямки розслідування і навіть ідентифікувати потенційних злочинців. Це значно прискорює процес розслідування та дозволяє оперативно приймати процесуальні й тактичні рішення у досудовому розслідуванні воєнних злочинів.

Використання спеціальних знань і методик. Застосування спеціальних знань у сферах криміналістики, судових експертиз, методик документування (наприклад, Протоколу Берклі[2], Міннесотського Протоколу[3]) є ключовим для

[1] Статистика. Офіс Генерального прокурора <https://gp.gov.ua/ua/posts/statistika> дата звернення 07.12.2023.
[2] Berkeley Protocol on Digital Open Source Investigations. Office of the United Nations High Commissioner for Human Rights. (Geneva, 2019) <https://www.law.berkeley.edu/wp-content/uploads/2020/05/Berkeley-Protocol-ENG.pdf> дата звернення 07.12.2023.
[3] Minnesota Protocol on the Investigation of Potentially Unlawful Deaths (2016) Minnesota Medical Examiner's Office <https://www.law.umn.edu/sites/law.umn.edu/files/minnesota_protocol.pdf> дата звернення 07.12.2023.

забезпечення визнання доказів на міжнародному рівні, зокрема для Міжнародного кримінального суду. Українські правоохоронці активно використовують пересувні ДНК-лабораторії для швидкої ідентифікації жертв, що є критично важливим у випадках масових загибелей (Буча, Ізюм та ін.).

Застосування новітніх технологій супроводжується низкою правових, етичних та технічних питань, таких як захист персональних даних, уникнення зловживань у використанні технологій, забезпечення конфіденційності, що потребують правового регулювання і впровадження системного підходу з боку державних органів та міжнародних партнерів.

Отже, зростання кількості воєнних злочинів, у зв'язку з загарбницькою війною рф проти України, і складність їх розслідування вимагають активного впровадження та інтеграції новітніх технологій у процес їх документування контррозвідувальними, оперативно-розшуковими, криміналістичними та кримінально-процесуальними засобами. Це дозволяє значно підвищити ефективність розслідування цих злочинів, забезпечити якість доказів як для вітчизняного, так і для міжнародного кримінального судочинства та сприяє досягненню справедливості для потерпілих від воєнних злочинів. Водночас, це ставить на порядок денний й питання створення відповідних правових рамок, етичних стандартів та інституційних механізмів їх реалізації, що актуалізує необхідність комплексного дослідження проблеми застосування новітніх технологій в документуванні, розслідуванні та доказуванні воєнних злочинів.

Аналіз останніх наукових досліджень та публікацій. Окремим аспектам застосування новітніх технологій та їх використання в розслідуванні воєнних злочинів присвятили свої праці вітчизняні фахівці в галузі кримінального процесу, криміналістики, оперативно-розшукової діяльності та контррозвідувальної діяльності, зокрема, В. Арешонков, О. Бех, Р. Благута, В. Бондар, В. Бурлака, І. Гловюк, О. Дрозд, О. Дуфенюк, О. Капліна, В. Корнієнко, Т. Коршикова, О. Кравчук, М. Кузнєцов, О. Литвинов, Ю. Орлов, І. Осипенко, М. Пашковський, В. Присяжний, О. Пчеліна, Є. Свобода, А. Саковський, Т. Савчук, Д. Сергєєва, О. Стрільців, О. Тарасенко, Г. Тетерятник, Т. Фоміна, С. Чернявський, А. Черняк, М. Цуцкіридзе, А. Шевчишен, В. Шепітько, М. Шепітько, В. Юсупов, О. Яновська та ін.

Проблематика використання новітніх технологій у розслідуванні, у тому числі й воєнних злочинів, активно досліджується зарубіжними фахівцями. Зокрема Е. Кейсі (Eoghan Casey) у своїй праці глибоко розкрив питання застосування цифрових технологій та їх важливості у розслідуванні кримінальних проваджень, включаючи воєнні злочини[1].

О. Керр (Orin Kerr) дослідив правові аспекти комп'ютерних злочинів, зокрема використання новітніх технологій у розслідуваннях та судових процесах[2]. Ця робота є ґрунтовним і всебічним дослідженням, яке розглядає як теоретичні, так і практичні аспекти законодавства, що регулює кіберзлочинність. Вона допомагає читачам розібратися в складних питаннях, які виникають під час розслідування кіберзлочинів, і дає чітке розуміння, як правова система може боротися з новими загрозами в цифровому світі.

Р. Голсан (Richard Golsan) досліджував питання відповідальності за воєнні злочини та їх розслідування в контексті міжнародного права. В його роботах аналізується взаємозв'язок між історичною пам'яттю, правосуддям та політичною відповідальністю у контексті післявоєнної Франції[3].

[1] E Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition (Academic Press, 2019) 650.

[2] O S Kerr, Computer Crime Law (West Academic Publishing, 2022)700.

[3] R Golsan, The Papon Affair: Memory and Justice on Trial (2000) 18(2) French Politics, Culture & Society, 1–17; R Golsan, The Trial of Maurice Papon: A Study in the Politics of Memory (2001) *Memory and Justice* 123–145.

Ш. Бреннон (Shannon Brenner) дослідив природу та різноманітні аспекти кіберзлочинності, зокрема, як злочинці використовують Інтернет і комп'ютерні системи для здійснення протиправних дій, а також загрози, пов'язані з кіберзлочинами, такі як хакерські атаки, крадіжка особистих даних, шахрайство в мережі Інтернет та важливість законодавчої регуляції кіберзлочинності[1].

Дж. Клоу (Jonathan Clough) дослідив правові аспекти кіберзлочинності. Розглянув різноманітні типи кіберзлочинів, таких як хакерські атаки, шахрайство в Інтернеті та кібертероризм, аналізуючи законодавчі, етичні та міжнародні аспекти цих злочинів, а також стратегії боротьби з ними на глобальному рівні[2].

С. Манн (Stephen Mann) та К. Робертс (Clifford Roberts) у практичному посібнику для слідчих та правозахисників розглядають різноманітні види Інтернет-злочинів, такі як кіберзлочинність, шахрайство, кібербулінг та крадіжка особистих даних, пропонуючи ефективні стратегії для розслідування та збору доказів. Їх робота охоплює важливі аспекти законодавства та використання новітніх технологій для боротьби з Інтернет-злочинністю[3].

Праці зазначених учених є вагомим теоретичним і практичним внеском у вирішення проблем використання новітніх технології в документування, розслідуванні та доказування воєнних злочинів, створюючи підґрунтя для подальших досліджень у галузі оперативно-розшукового та криміналістичного забезпечення розслідувань цих злочинів з використанням новітніх технологій, а також для доказування таких злочинів. Проте окремі аспекти цієї проблематики залишаються на сьогодні ще недостатньо вивченими, враховуючи як технічний прогрес, так і прояви нових жорстоких форм агресії сучасний війн і, передусім рф проти України та у секторі Газа.

Метою статті є аналіз ролі новітніх технологій у документуванні, розслідуванні та доказуванні воєнних злочинів й обґрунтування необхідності подальшого впровадження найефективніших із них у теорію оперативно-розшукової діяльності, криміналістики та кримінального процесу, а також у практику правоохоронних органів.

Виклад матеріалу дослідження та його основні результати. У документуванні та розслідуваннях сучасних злочинів і воєнних, зокрема, новітні технології відіграють вирішальну роль у підвищенні ефективності збору доказів, а також у забезпеченні їхньої автентичності та збереження протягом судового процесу.

Передусім зазначимо, що загальні питання документування, розслідування та доказування правоохоронними органами різних видів злочинів, у тому числі й воєнних, досліджувалися не лише в працях вище вказаних авторів, а й у наших авторських роботах[4]. Тому враховуючи встановлений обсяг статті, вважаємо доцільним уникати тих дискусійних

[1] S W Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger Security International, 2009) 320.
[2] J Clough, Principles of Cybercrime (Cambridge University Press, 2015) 450.
[3] S Mann, C Roberts, Internet Crimes: A Guide to Effective Investigations (CRC Press, 2017) 380.
[4] М А Погорецький, Проблеми використання матеріалів оперативно-розшукової діяльності в кримінальному процесі: монографія (Київ, РВВ НА СБУ, 2004) 336; М А Погорецький, Оперативно-розшукова діяльність і кримінальний процес: проблеми взаємозв'язку: монографія: у 2 ч (Луганськ, Луганський держ ун-т внутр справ ім. Е.О. Дідоренка, 2008) Ч 1 216; М Є Шумило, М А Погорецький, Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти (2001) 3 *Вісник Луганського ін-ту внутр. справ* 199–209; М А Погорецький, Докази у кримінальному процесі (2003) 2 *Вісник прокуратури* 59–65; М А Погорецький, Закон України «Про оперативно-розшукову-діяльність»: проблеми застосування окремих норм (2001) 3 *Вісник Академії правових наук України* 205–213; М А Погорецький, Теоретичні й практичні проблеми використання матеріалів оперативно-розшукової діяльності в кримінальному процесі (за матеріалами Служби безпеки України) (автореф. дис. … д-ра. юрид. наук: спец. спец. 12.00.09. Київ, КНУВС, 2006) 36; М А Погорецький, Поняття та сутність легалізації оперативно-розшукової інформації (2010) Спец вип 4 *Вісник Луганського держ. ун-ту внутр. справ ім. Е.О. Дідоренка* 26–40; М А Погорецький, Оперативний пошук в контексті реформування кримінальної юстиції. *Шляхи розвитку оперативно-розшукової діяльності в сучасних умовах*: матеріали наук.-практ. конф. на базі Харк. нац. ун-ту внутр. справ, 28 листоп. 2009 р. (МВС України; Харк нац ун-т внутр справ;

питань, по яких вже була висловлена наша авторська позиція.

Зауважимо, що при застосуванні новітніх технологій у документуванні, розслідуванні та доказуванні злочинів слід враховувати інтеграційні тенденції, які простежуються у сфері кримінальної юстиції Європейського Союзу. Необхідність ухвалення єдиного європейського інструменту для отримання доказів, який можна було б застосовувати для проведення будь-яких слідчих дій, наголошувалася в Зеленій книзі «Про отримання доказів між державами-членами ЄС у кримінальних справах та забезпечення їх допустимості»[1]. Дана тенденція простежується і в п. 3.1.1. Стокгольмської програми[2], на що вже зверталася наша увага в попередній роботі[3].

Результати аналізу матеріалів практики (архівних контррозвідувальних, оперативно-розшукових та кримінальних справ)[4] дають підстави для висновку, що у період 2022–2023 років в Україні активно використовувалися новітні технології для документування, розслідування та доказування воєнних злочинів. Зокрема, застосовувалися інформаційно-пошукові, телекомунікаційні та комп'ютерні системи для збору та аналізу доказової інформації про воєнні злочини. Це включало використання спеціальних знань у процесі фіксації та дослідження слідів злочинів як оперативно-розшуковими, так і криміналістичними й процесуальними засобами[5], джерел доказів і власне самих доказів[6] що дозволяло ефективно виявляти та документувати порушення законів і звичаїв війни.

Навч-наук ін-т підготовки фахівців кримінальної міліції) (Харків, ХНУВС, 2009) 7–10; М Погорецький, В Шеломенцев, 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. Оперативно-розшукова діяльність поліції (міліції), 750–751; М А Погорецький, Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія (Харків, Арсіс ЛТД, 2007) 576; М А Погорецький, Про співвідношення джерел фактичних даних і джерел доказів у кримінальному процесі (2009) 1 *Право України* 80–85; М Погорецький, В Шеломенцев, 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. Оперативно-розшукова діяльність поліції (міліції), 750–751; М Погорецький, Співвідношення джерел фактичних даних в оперативно-розшуковій діяльності та кримінальному процесу і джерел кримінально процесуальних доказів 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. Оперативно-розшукова діяльність поліції (міліції), 937–939; М Погорецький, В Шеломенцев, Фактичні дані (дані про факти). 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. Оперативно-розшукова діяльність поліції (міліції), 1041; М Погорецький, В Шеломенцев, Фіксація 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. Оперативно-розшукова діяльність поліції (міліції), 1042–1043; М Погорецький, В Шеломенцев, Пошукові ознаки об'єктів оперативного пошуку: поняття та сутність (2010) 4 *Вісник Акад. управління МВС* 114–121.

[1] Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (Brussels, 2009) 624 <https://eur-lex.europa.eu/legal-content/en/ TXT/?uri=CELEX% 3A52009DC 0624> дата звернення 10.12.2023.

[2] The Stockholm Programme – An open and secure Europe serving and protecting citizens (2010) *Official Journal of the European Union* 115 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52010XG0504 %2801 %29> дата звернення 10.12.2023.

[3] М А Погорецький, Є І Лисаченко, Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України (2022) 3–4 *Вісник кримінального судочинства* 20–34.

[4] За темою досліджено нами вивчено понад 150 архівних контррозвідувальних, оперативно-розшукових та кримінальних справ й опитано понад 300 респондентів із числа оперативних працівників, слідчих та прокурорів.

[5] Докладно див: М Погорецький, Оперативно-розшукові заходи: проблеми правового регулювання (2007) 14 *Боротьба з організованою злочинністю і корупцією (теорія і практика)* 135–145; М Погорецький, Негласні слідчі (розшукові) дії: проблеми провадження та використання результатів у доказуванні (2013) 1 *Юридичний часопис Національної академії внутрішніх справ* 270–277; М Погорецький, Д Сергєєва, Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення (2014) 2(33) *Боротьба з організованою злочинністю і корупцією (теорія і практика)* 137–141.

[6] *Докладно див:* М Погорецький, Докази у кримінальному процесі (2003) 2 *Вісник прокуратури* 59–65; М Погорецький, Джерела судових доказів (2005) 10 *Питання боротьби зі злочинністю: збірник наукових праць* 167–178; М Погорецький, Про співвідношення джерел фактичних даних і джерел доказів у кримінальному

Окрім того, організовувалися навчальні заходи для підвищення кваліфікації правоохоронців у використанні новітніх технологій, зокрема OSINT-технологій (Open Source Intelligence), для документування та розслідування воєнних злочинів[1]. Такі тренінги сприяли поглибленню знань щодо застосування відкритих джерел інформації в кримінальних розслідуваннях.

Огляд основних технологій, які використовуються у розслідуваннях, зокрема космічні та геоінформаційні технології, штучний інтелект, блокчейн, дрони та цифрові сліди і які викладені у наукових джерелах зарубіжних і вітчизняних авторів[2], дозволяє зрозуміти, як інноваційні інструменти допомагають правоохоронним органам у боротьбі з сучасною злочинністю, включаючи воєнні злочини.

Космічні та геоінформаційні технології (ГІС), зокрема супутникові знімки, відіграють важливу роль у виявленні та документуванні воєнних злочинів. ГІС є потужним інструментом для документування, аналізу та картографування воєнних злочинів, зокрема в контексті російської агресії проти України. Ці технології дають можливість створювати точні карти, на яких візуалізуються важливі події, такі як обстріли цивільної інфраструктури, масові поховання, переміщення людей і військових підрозділів. ГІС не тільки допомагають у виявленні слідів злочинів і зборі доказів, але й дозволяють оперативно аналізувати ситуацію на місцях бойових дій, що є надзвичайно важливим для ефективного реагування правоохоронних органів і міжнародних судових інстанцій.

ГІС активно використовуються для вивчення і картографування територій, на яких відбуваються бойові дії, зокрема в Україні, де масштаби руйнувань і переміщень людей є величезними. Важливою особливістю застосування ГІС є їх здатність фіксувати зміни в ландшафті, що допомагає не тільки документувати факти обстрілів чи знищення об'єктів, а й виявляти нові сліди злочинів, зокрема на окупованих територіях.

Важливість геоінформаційних систем для створення карт полягає в тому, що вони допомагають виявляти закономірності в розслідуваннях, зокрема воєнних злочинів, і дозволяють документувати події, а також відслідковувати рух підозрюваних та військових сил на карті. У випадку війни в Україні ці технології дають можливість чітко відобразити ситуацію на різних етапах війни, від бойових зіткнень

процесі (2009) 1 *Право України* 80–85; М Погорецький, Докази у кримінальному процесі: проблемні питання (2011) 1(3) *Часопис Національного університету «Острозька академія». Серія «Право»* <https://lj.oa.edu.ua/articles/2011/n1/11pmappp.pdf> дата звернення 10.12.2023.

[1] EU-funded Project Pravo-Justice. Promoting greater rule of law in Ukraine, in line with European standards and comparative practices. European Union <https://pravojustice.eu/> дата звернення 10.12.2023.

[2] S W Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger Security International, 2009) 320; J Clough, Principles of Cybercrime (Cambridge University Press, 2015) 450; S Mann, C Roberts, Internet Crimes: A Guide to Effective Investigations (CRC Press, 2017) 380; E Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Academic Press, 2021) 450; O S Kerr, Computer Crime Law (West Academic Publishing, 2022) 700; М А Погорецький, В П Шеломенцев, Поняття кіберпростору як середовища вчення злочину (2009) 2 *Інформаційна безпека людини, суспільства, держави* 77–81; М Погорецький, В Шеломенцев, Правове забезпечення боротьби з кіберзлочинами в Україні: проблемні питання (2011) 8 *Вісник прокуратури* 30–38; М Погорецький, В Шеломенцев, Оперативно-рошукова діяльність у кіберпросторі (2011) 3 *Вісник прокуратури* 58–63; В С Бондар, В Ю Парфьонов, Про особливості застосування новітніх технологій у документуванні та розслідуванні окремих видів воєнних злочинів (2022) 1(1) *Криміналістичний вісник* 123–130; О М Дуфенюк, Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації (2022) 1 *Baltic Journal of Legal and Social Sciences* 46–56; Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: метод. рек. / С С Чернявський, В І Присяжний, О М Стрільців та ін,; за заг. ред. М С Цуцкіридзе (Київ, Нац. акад. внутр. справ, 2023) 92; Г К Тетерятник, О В Бех, Ю М Одажиу, Розслідування воєнних злочинів: окремі теоретико-прикладні питання (2023) 6 *Юридичний науковий електронний журнал* 95–105; О Пчеліна, Т Фоміна, Особливості проведення огляду місця події під час досудового розслідування злочинів, пов'язаних зі збройною агресією проти України (2023) 2 *Науковий вісник Дніпропетровського державного університету внутрішніх справ* 254.

до змін, пов'язаних із захопленням територій та руйнуванням цивільних об'єктів[1]. Наприклад, у звітах міжнародних організацій, таких як Human Rights Watch[2] та Amnesty International, часто використовуються карти та супутникові знімки для демонстрації наслідків обстрілів цивільної інфраструктури, таких як руйнування житлових кварталів у Маріуполі, Харкові та інших містах, що підтверджує використання ГІС для аналізу зони бойових дій[3].

ГІС активно використовуються для виявлення злочинів, зокрема воєнних злочинів, пов'язаних з атаками на цивільну інфраструктуру, масовими вбивствами, а також пограбуваннями. Застосування ГІС для картографування та вивчення територій дозволяє точно відстежувати не лише місце і час скоєння злочину, а й прогнозувати його можливі наслідки, що має велике значення для оперативного реагування правоохоронних органів на відповідні ситуації.

В Україні використання супутникових знімків і ГІС для документування злочинів стало особливо актуальним після російського вторгнення у 2022 році. Наприклад, у Київській, Чернігівській і Сумській областях було виявлено масові поховання цивільних осіб, вбитих під час обстрілів російськими військами. Всі ці факти були документовані за допомогою супутникових знімків та ГІС, що дозволяє встановити точне місце і час скоєння злочинів. Так, супутникові знімки, зроблені під час окупації, дозволяють виявляти зміни в ландшафті, такі як нові могили, що вказують на місця масових поховань[4]. Це дозволяє забезпечити точність у зборі доказів та зберіганні цих даних для подальших судових процесів.

Супутникові знімки є важливим джерелом для збору доказів, особливо коли йдеться про знищення цивільної інфраструктури чи масові вбивства. У випадку війни в Україні ці знімки відіграють важливу роль у фіксації порушень міжнародного гуманітарного права, Женевських конвенцій та Римського статуту, а також є основними доказами у міжнародних судах, таких як Міжнародний кримінальний суд (МКС)[5]. Вони допомагають документувати атаки на мирне населення та будувати стратегію і тактику розслідування у справах про воєнні злочини.

В Україні ці технології активно використовуються для відстеження результатів воєнних злочинів, таких як атаки на лікарні, школи, дитячі садки та інші цивільні об'єкти, що є порушенням міжнародних стандартів. Ці технології допомагають не лише виявити факт злочину, але й у подальшому розслідуванні сприяють виявленню зв'язків між різними подіями, що має важливе значення для ефективного правосуддя[6].

Геоінформаційні технології дозволяють не тільки збирати й аналізувати дані, але й використовувати їх для координації зусиль правоохоронних органів, а також для визначення, де саме потрібна допомога або де проводяться пошукові роботи. На деокупованих територіях ГІС використовуються для візуалізації ситуацій на карті, що сприяє ефективному реагуванню та організації гуманітарних місій. Ці технології допомагають створювати точні картографічні моделі, що дозволяють зберігати цілісність даних та забезпечувати їх надійне зберігання для подальшого використання в судових процесах[7].

[1] J Clough, Principles of Cybercrime (Cambridge University Press, 2015) 450.
[2] Human Rights Watch. (2023). World Report 2023: Events of 2022 <https://www.hrw.org/world-report/2023> дата звернення 12.12.2023.
[3] Amnesty International. (2023). Amnesty International Report 2022/23: The State of the World's Human Rights <https://www.amnesty.org/en/documents/pol10/5670/2023/en/> дата звернення 12.12.2023.
[4] Алгоритм дій слідчо-оперативних груп Національної поліції на звільнених від окупації територіях з документування воєнних злочинів (на прикладі звільнених територій Київської області) (Київ, Гол. слідче управління Нац. поліції України, 2022) 14.
[5] S W Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger Security International, 2009) 320.
[6] S Mann, C Roberts, Internet Crimes: A Guide to Effective Investigations (CRC Press, 2017) 380.
[7] O S Kerr, Computer Crime Law (West Academic Publishing, 2022) 700.

Застосування супутникових знімків і ГІС у розслідуванні воєнних злочинів в Україні є критично важливим для забезпечення об'єктивності і точності доказів, що використовуються в міжнародних судах, для забезпечення справедливості потерпілим від таких злочинів[1].

Так, в умовах війни в Україні, особливо після повномасштабного вторгнення росії у 2022 році, супутникові технології набули надзвичайно важливого значення у слідчій та судовій практиці. Зокрема, супутникові знімки стали ключовим доказом у резонансних справах про воєнні злочини. Один з найвідоміших прикладів використання цих технологій – розслідування масових вбивств цивільних осіб у місті Буча Київської області. Російська сторона намагалася заперечити причетність до цих злочинів, стверджуючи, що загиблі цивільні з'явилися на вулицях після виходу російських військ. Однак саме завдяки супутниковим знімкам вдалося встановити, що тіла цивільних мешканців перебували на вулицях Бучі вже з 9 березня 2022 року, коли місто ще контролювалося російськими військами[2]. Це стало вагомим доказом причетності російських військ до цих злочинів.

Ще одним прикладом стало документування масових поховань українців поблизу Ізюма після його звільнення від окупації. Супутникові знімки дозволили зафіксувати нові місця поховань, які з'явилися під час окупації цієї території російськими військами.

Також значну роль супутникові технології відіграли у розслідуванні катастрофи рейсу MH17 у 2014 році, коли російським зенітним ракетним комплексом «Бук-М1» був збитий пасажирський літак. У процесі міжнародного судового розгляду нідерландська прокуратура порівняла супутникові знімки, надані США, Європейською космічною агенцією (ESA) та росією. Це дозволило встановити, що ракета була випущена саме з території, контрольованої проросійськими силами, і що вона була доставлена з території росії. Виявлені розбіжності між супутниковими знімками, наданими російською стороною та міжнародними організаціями, стали підставою для висновку про фальсифікацію доказів росією[3].

Геоінформаційні системи активно використовуються і для створення цифрових карт місць подій, що дозволяє чітко встановити обставини злочину та відслідковувати рух військових сил і техніки. У слідчій практиці України ГІС застосовуються для документування пошкоджень цивільної інфраструктури, масових вбивств, пограбувань та інших тяжких злочинів.

Досвід України засвідчив, що інтеграція супутникових знімків та геоінформаційних технологій у кримінальне провадження значно посилює доказову базу, підвищує швидкість і точність розслідування злочинів. Зібрані таким чином докази мають високу достовірність і вже активно використовуються у міжнародних судових інстанціях, включаючи Міжнародний кримінальний суд, для забезпечення справедливості та притягнення винних до відповідальності.

Використання геоінформаційних систем та супутникових знімків у кримінальному процесі має важливе значення для забезпечення об'єктивності доказів та встановлення зв'язків між різними злочинами[4].

---

[1] J Clough, Principles of Cybercrime (Cambridge University Press, 2015) 450.

[2] Алгоритм дій слідчо-оперативних груп Національної поліції на звільнених від окупації територіях з документування воєнних злочинів (на прикладі звільнених територій Київської області) (Київ, Гол. слідче управління Нац. поліції України, 2022) 1–14.

[3] Поліцейські представили результати розслідування воєнних злочинів в Україні на щорічному засіданні експертів в Гаазі (2022) Національна поліція України: офіційний вебпортал <https://www.npu.gov.ua/news/politseiski-predstavyly-rezultaty-rozsliduvannia-voiennykh-zlochyniv-v-ukraini-na-shchorichnomu-zasidanni-ekspertiv-v-haazi> дата звернення 14.12.2023.

[4] М А Погорецький, Є І Лисаченко, Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України (2022) 3–4 *Вісник кримінального судочинства* 20–34.

Штучний інтелект (ШІ) та технології машинного навчання займають дедалі помітніше місце в розслідуванні воєнних злочинів, зокрема завдяки їх здатності швидко обробляти та аналізувати величезні обсяги інформації. Це має особливе значення для розслідувань воєнних злочинів, де часто необхідно опрацювати велику кількість цифрових доказів, таких як електронні повідомлення, історії переміщення через GPS, метадані фото- і відеоматеріалів, записи телефонних дзвінків тощо.

Алгоритми машинного навчання застосовуються для виявлення закономірностей та взаємозв'язків у складних злочинних схемах, дозволяючи правоохоронцям не лише ефективно ідентифікувати підозрюваних, але й визначати можливі напрямки подальших розслідувань. Наприклад, системи штучного інтелекту можуть аналізувати великі масиви інформації з соціальних мереж, виявляти підозрілу активність, пов'язану з фінансовими транзакціями, або автоматично ідентифікувати особи, причетні до скоєння злочинів, через розпізнавання облич на зображеннях або відеоматеріалах.

ШІ широко використовується для автоматизації процесів аналізу даних, класифікації та систематизації доказів, розпізнавання образів, аналізу текстів і відеоматеріалів, що значно скорочує час, необхідний для розслідування злочинів. Зокрема, у випадках масового збору даних ШІ може значно підвищити ефективність відбору і обробки інформації, дозволяючи слідчим зосередитися на найбільш важливих елементах справи.

ШІ може використовуватися в розслідуванні цифрових злочинів, таких як кіберзлочинність, де системи на основі ШІ можуть виявляти аномалії в мережевому трафіку, що вказують на ознаки злочинної діяльності[1].

Практика правоохоронних органів України демонструє ефективне застосування технологій штучного інтелекту у розслідуванні воєнних злочинів під час російської агресії. Зокрема, Національна поліція України широко застосовує сучасні системи розпізнавання облич, які мають доступ до бази, що містить понад 30 мільярдів зображень, отриманих із відкритих джерел.

Також активно використовується верифікація осіб через соцмережі за допомогою таких програмних продуктів, як Clearview та Artellence, використання можливостей супутникового зв'язку та аналізу відеофото матеріалів, отриманих з вилучених мобільних терміналів, камер відеоспостережень, камер відеоспостережень системи «Безпечне місто» тощо, що дозволяє встановлювати акаунти потенційних воєнних злочинців у соціальних мережах.

Особливе значення має використання штучного інтелекту в OSINT-дослідженнях (розслідування за відкритими джерелами інформації), які стали важливим інструментом у фіксуванні воєнних злочинів. Це дозволяє правоохоронцям швидко та ефективно аналізувати фото та відеоматеріали, розміщені в глобальній мережі, що суттєво прискорює процес розслідування та надає високоякісні докази для суду.

Прикладом успішного впровадження новітніх технологій є також створення міжвідомчої бази даних «Воєнний злочин», яка містить інформацію про понад 550 тис. воєнних злочинців, а також докази їх злочинної діяльності, отримані під час розслідувань. Ця система об'єднала ресурси всіх силових структур України, що є унікальним досвідом використання штучного інтелекту для координації дій правоохоронних органів під час документування та розслідування воєнних злочинів[2]. Особливу роль у документуванні та фіксуванні воєнних злочинів

[1] E Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Academic Press, 2021) 450.

[2] Поліцейські представили результати розслідування воєнних злочинів в Україні на щорічному засіданні експертів в Гаазі. Національна поліція України: офіційний вебпортал <https://www.npu.gov.ua/news/politseiski-predstavyly-rezultaty-rozsliduvannia-voiennykh-zlochyniv-vukraini-na-shchorichnomu-zasidanni-ekspertiv-v-haazi> дата звернення 14.12.2023.

відіграють спеціалісти криміналісти, котрі залучаються до проведення окремих процесуальних дій під час досудового розслідування вказаних правопорушень. Наприклад, на сьогоднішній день спеціалісти-криміналісти: – залучені як оператори сучасних БПЛА, що є одним з пріоритетних напрямків фіксації зруйнованих внаслідок російських ракетних атак житлових будинків та об'єктів критичної інфраструктури; – створюють детальні 3-D моделі об'єктів й обставин внаслідок скоєних рф воєнних злочинів за допомогою сучасного сканера Z+F Imager 5016. Прилад дозволяє зробити це не тільки швидко, але й на відстані від зони потенційної небезпеки, адже нерідко росіяни свідомо обстрілюють місця скоєння злочинів повторно, коли поліцейські та медики прибувають туди для порятунку людей; – встановлюють ДНК-профіль людини за півтори години за допомогою мобільних приладів «ANDE RAPID DNA 6C, нерідко – із стовідсотковою ефективністю[1].

Отже, ШІ активно використовується для розпізнавання осіб на відео, що є особливо корисним для ідентифікації злочинців, що брали участь у воєнних злочинах[2] та є ефективним інструментом координації правоохоронних органів у складних умовах бойових дій[3].

Застосування штучного інтелекту та машинного навчання в оперативно-розшуковій, криміналістичній та кримінально-процесуальній практиці значно підвищує ефективність розслідувань воєнних злочинів, дозволяючи оперативно та якісно збирати докази для національних і міжнародних судових процесів. Водночас ці технології потребують подальшого вдосконалення правового та етичного регулювання, аби їх використання відповідало міжнародним стандартам захисту прав людини та забезпечувало належну процесуальну справедливість.

Використання блокчейн-технології для документування, розслідування та доказування воєнних злочинів є перспективним напрямком, який активно розвивається в сучасній криміналістичній практиці. Блокчейн (Blockchain) – це технологія розподіленого реєстру, що дозволяє безпечно зберігати інформацію, гарантуючи її прозорість та неможливість підробки. Особливістю блокчейну є те, що дані, які вносяться до системи, фіксуються у вигляді незмінних записів, кожен з яких містить інформацію про попередні блоки, що забезпечує цілісність і незмінність інформації[4].

Як зазначають українські дослідники, застосування блокчейн у сфері кримінального правосуддя відкриває якісно нові можливості для документування, розслідування та доказування злочинів, особливо у випадках, коли існує значний ризик втрати або навмисного спотворення доказів. Блокчейн дозволяє створювати безпечні та прозорі ланцюги доказів, що гарантує їхню автентичність та прийнятність у суді[5]. Це особливо актуально при розслідуванні воєнних злочинів, де існує високий ризик маніпуляцій з інформацією.

В Україні практика застосування блокчейн-технології для документування та розслідування воєнних злочинів стала набувати значення у зв'язку із пов-

[1] Там само.

[2] O S Kerr, Computer Crime Law (West Academic Publishing, 2022) 700.

[3] Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: методичні рекомендації / С С Чернявський, В І Присяжний, О М Стрільців та ін,; за заг. ред. М С Цуцкіридзе (Київ, Нац. акад. внутр. справ, 2023) 92.

[4] S W Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger Security International, 2009) 320; S Mann, C Roberts, Internet Crimes: A Guide to Effective Investigations (CRC Press, 2017) 380; O S Kerr, Computer Crime Law (West Academic Publishing, 2022) 700.

[5] М Погорецький, Є Лисаченко, Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України (2022) 3–4 *Вісник кримінального судочинства* 20–34; Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: методичні рекомендації / С С Чернявський, В І Присяжний, О М Стрільців та ін,; за заг. ред. М С Цуцкіридзе (Київ, Нац. акад. внутр. справ, 2023) 92.

номасштабною агресією російської федерації. Одним з найбільш вагомих та яскравих прикладів є створення та функціонування вже вище згаданої міжвідомчої інформаційної системи «Воєнний злочин». Вона об'єднує зусилля всіх українських силових відомств, забезпечуючи високий рівень довіри, прозорості та незмінності зафіксованих доказів, що мають використовуватися у міжнародних судових процесах, зокрема у Міжнародному кримінальному суді.

Ще одним прикладом є використання блокчейну у процесі документування вже згаданих злочинів у Бучі, Ірпені, Ізюмі та інших містах, що дозволяють забезпечити збереження цифрових доказів у вигляді фотографій, відеоматеріалів, аудіозаписів свідчень та супутникових знімків. Використання розподілених технологій зберігання інформації у цих випадках забезпечує належне фіксування доказів і гарантує їхню юридичну значущість у судових провадженнях як на національному, так і на міжнародному рівнях.

Конкретні приклади судової практики, що вже застосовують зібрані таким чином докази, включають провадження, які розглядаються українськими судами за фактами воєнних злочинів у звільнених містах Київської, Харківської, Херсонської областей. Вже розпочато низку кримінальних проваджень щодо російських військових за фактами вбивств, тортур, мародерства та інших тяжких злочинів, де використовуються цифрові докази, зафіксовані із застосуванням захищених інформаційних платформ, включно з технологіями, подібними до блокчейну[1].

Крім того, Україна активно передає зібрані докази міжнародним слідчим групам та міжнародним судовим інстанціям, зокрема Міжнародному кримінальному суду та Міжнародному суду ООН[2]. Саме використання блокчейн-подібних технологій дозволяє забезпечити високу довіру та прийнятність цих доказів для міжнародної юридичної спільноти, оскільки такі технології виключають можливість внесення несанкціонованих змін або фальсифікації зібраної інформації.

Практика України у застосуванні блокчейн-технологій та подібних до них розподілених реєстрів свідчить про їх високий потенціал у сфері документування, розслідування і доказування воєнних злочинів. Ці приклади демонструють ефективність, надійність та перспективність таких технологій для сучасної оперативно-розшукової, криміналістичної й кримінально-процесуальної діяльності в умовах збройних конфліктів.

Використання біометричних систем (розпізнавання обличчя, відбитків пальців і ДНК) для документування, розслідування та доказування воєнних злочинів стало важливим елементом криміналістичної діяльності в Україні в умовах російської агресії. Біометричні технології значно підвищують швидкість та точність ідентифікації осіб, причетних до злочинів, а також ідентифікації жертв та встановлення обставин їх загибелі.

Зокрема, правоохоронні органи України активно використовують системи розпізнавання обличчя для ідентифікації злочинців за допомогою спеціалізованих мереж, які налічують, як вже зазначалося, понад 30 мільярдів зображень, зібраних з відкритих джерел в Інтернеті. Також широко застосовуються інструменти для верифікації осіб у соціальних мережах за фотографіями (зокрема, програмні продукти Clearview та Artellence), що дозволяє оперативно ідентифікувати акаунти потенційних воєнних злочинців і підтвердити їхню причетність до протиправних дій.

Особливе значення при розслідуванні воєнних злочинів має використання біометричних технологій у сфері ДНК-а-

[1] Поліцейські представили результати розслідування воєнних злочинів в Україні на щорічному засіданні експертів в Гаазі. Національна поліція України: офіційний вебпортал <https://www.npu.gov.ua/news/politseiski-predstavyly-rezultaty-rozsliduvannia-voiennykh-zlochyniv-vukraini-na-shchorichnomu-zasidanni-ekspertiv-v-haazi> дата звернення 14.12.2023.

[2] М А Погорецький, Є І Лисаченко, Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України (2022) 3–4 *Вісник кримінального судочинства* 20–34.

налізу. В Україні застосовується система швидкої ідентифікації ДНК ANDE RAPID DNA 6C. Це мобільні лабораторні пристрої, що дозволяють встановлювати ДНК-профіль людини лише за півтори години, нерідко зі 100 %-ною точністю. Національна поліція України має 32 таких прилади, що дозволяє їй швидко ідентифікувати загиблих у місцях масових поховань, внаслідок обстрілів цивільних об'єктів та інших злочинів, скоєних окупаційними військами рф.

Ще одним прикладом застосування біометричних технологій є використання спеціалістами-криміналістами пересувних ДНК-лабораторій. Ці лабораторії активно використовуються для ідентифікації тіл загиблих на деокупованих територіях, зокрема, у Київській, Харківській та Херсонській областях. У процесі такої роботи було ідентифіковано близько трьох тисяч загиблих українців. За допомогою ДНК за досліджуваний період ідентифіковано близько трьох тисяч загиблих українців[1].

Використання систем біометричної ідентифікації в Україні підтвердило їхню високу ефективність та практичне значення для розслідування воєнних злочинів. Завдяки цим технологіям стало можливим не лише оперативно ідентифікувати підозрюваних і жертв, але й створити надійну доказову базу для судових процесів як в національних судах, так і на міжнародному рівні, включаючи Міжнародний кримінальний суд.

Разом із тим, науковці обґрунтовано звертають увагу на необхідність правового регулювання застосування цих технологій, оскільки вони породжують питання щодо приватності осіб та дотримання прав людини[2].

Практика застосування біометричних систем демонструє значні перспективи для підвищення якості розслідування воєнних злочинів, а також наголошує на необхідності вдосконалення нормативної бази для гарантування дотримання прав людини під час їх використання.

Розслідування воєнних злочинів є складним процесом, що вимагає залучення фахівців з різних галузей для забезпечення об'єктивності та повноти слідства. Зокрема, використання спеціальних знань у військовій справі, вибухотехніці та судовій медицині є критично важливим для встановлення обставин злочину та притягнення винних до відповідальності.

Під час розслідування воєнних злочинів, пов'язаних з обстрілами, залучаються фахівці з ракетних військ, артилерії та військової авіації. Ці спеціалісти допомагають визначити ймовірні напрямки обстрілів, типи використаного озброєння та інші важливі деталі, що сприяють встановленню обставин злочину.

Фахівці-вибухотехніки відповідають за розмінування місця події та перевірку на наявність вибухонебезпечних предметів. Їхня робота є необхідною для забезпечення безпеки слідчих дій та збереження доказів.

Судово-медичні експерти визначають причину та час настання смерті, механізм і характер тілесних ушкоджень, що є важливим для встановлення обставин злочину[3].

У своїй роботі по забезпеченню документування та розслідування воєнних злочинів в Україні зазначені фахівці також використовують новітні технології. Така практика набуває поширення.

---

[1] За допомогою ДНК ідентифіковано близько трьох тисяч загиблих українців. Національна поліція України: офіційний вебпортал <https://www.npu.gov.ua/news/za-dopomohoiu-dnk-identyfikovano-blyzko-trokh-tysiach-zahyblykh-ukraintsiv-maksym-tsutskiridze> дата звернення 15.12.2023.

[2] М А Погорецький, Є І Лисаченко, Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України (2022) 3–4 *Вісник кримінального судочинства* 20–34.

[3] Докладно див: Алгоритм дій слідчо-оперативних груп Національної поліції на звільнених від окупації територіях з документування воєнних злочинів (на прикладі звільнених територій Київської області) (Київ, Гол. слідче управління Нац. поліції України, 2022) 14; Алгоритм реагування працівників Національної поліції на події, пов'язані із обстрілами населених пунктів, унаслідок яких сталися масштабні руйнування цивільної інфраструктури, насамперед критичної, та/або значні людські втрати (Київ, Національна поліція

В забезпеченні законності використання новітніх технологій в документуванні, розслідуванні та доказуванні воєнних злочинів важливу роль відіграє відомчий та судовий контроль й прокурорський нагляд. Зокрема, судовий контроль є основним механізмом, який забезпечує, щоб використання новітніх технологій, таких як біометричні системи, аналіз великих даних, розпізнавання обличчя, або слідчі дії за допомогою дронів, відповідало нормам кримінального процесу. Зокрема, суд контролює, чи не порушуються права підозрюваних і свідків, а також чи не перевищують правоохоронці свої повноваження. Це особливо важливо у випадках, коли технології збирають персональні дані або використовують інтерцепцію комунікацій, що потребує спеціальних дозволів.

Ефективне застосування новітніх технологій в розслідуванні та доказуванні воєнних злочинів відіграє важливу роль у реалізації процесуального статусу потерпілих[1] від таких злочинів.

Важливу роль у підтримці технологічного прогресу для документування та розслідування воєнних злочинів відіграють міжнародних організацій, які забезпечують необхідну підтримку у створенні та інтеграції сучасних технологій у правову практику, що дозволяє підвищити ефективність розслідувань та забезпечення справедливості в міжнародних судових процесах. Міжнародні організації надають технічну, правову та фінансову допомогу, сприяють створенню стандартів для документування злочинів, а також забезпечують інтеграцію інноваційних технологій у кримінальний процес.

Судовий контроль також включає перевірку допустимості доказів, отриманих за допомогою новітніх технологій. Важливо, щоб усі докази, отримані за допомогою технологій, таких як цифрові сліди, супутникові знімки або дані з безпілотників, відповідали вимогам законодавства щодо їх збору та збереження. Суд перевіряє, чи були дотримані процесуальні норми при їх збиранні, чи не було порушено право на конфіденційність або право на захист. Якщо будь-який з цих аспектів порушено, то докази можуть бути визнані недопустимими.

Однією з найбільш значущих міжнародних організацій, яка активно підтримує технологічний прогрес у розслідуванні воєнних злочинів, є Міжнародний кримінальний суд (МКС)[2]. МКС забезпечує важливу підтримку у розслідуванні і переслідуванні осіб, які вчинили воєнні злочини, злочини проти людяності та геноцид. Важливим аспектом роботи МКС є використання передових технологій, таких як блокчейн для зберігання доказів і штучний інтелект для аналізу великих масивів даних, що дозволяє ефективно організувати процес збору та збереження доказів, а також забезпечити їх недоторканність протягом усього процесу судового розгляду.

Іншою значущою міжнародною організацією є Європол[3], який активно сприяє розвитку інформаційно-комуні-

України, 2022) 11; Пам'ятка щодо особливостей організації і проведення слідчих (розшукових) дій під час розслідування нападів (обстрілів) на цивільне населення та об'єкти цивільної інфраструктури (Київ, Офіс Генерального Прокурора України); Тренінговий центр прокурорів України (2022) <https://docs.google.com/document/d/ 1TyileSKvDjvKYtsRb6VgGRRVI2DAln_M/edit> дата звернення 16.12.2023; Пам'ятка «Особливий режим кримінального провадження в умовах воєнного стану» (Київ, Офіс Генерального Прокурора України; Тренінговий центр прокурорів України, 2022) 32; Пам'ятка щодо особливостей проведення допитів потерпілих/свідків стосовно дослідження фактів сексуального насильства в умовах збройного конфлікту (Київ, Офіс Генерального Прокурора України; Тренінговий центр прокурорів України, 2022) 13 <https://surl.li/btvno> дата звернення 16.12.2023.

[1] М А Погорецький, Д Б Сергєєва, Проблемні питання реалізації процесуального статусу потерпілого у кримінальному провадженні (2017) 46 (2) *Науковий вісник Ужгородського національного університету. Серія «Право»* 118–123.

[2] Римський статут Міжнародного кримінального суду. Верховна Рада України <https://zakon.rada.gov.ua/go/995_588> дата звернення 16.12.2023

[3] European Parliament and Council. (2016). Regulation (EU) 2016/794 of the European Parliament and of the

каційних технологій у розслідуваннях злочинів, включаючи воєнні злочини. Європол створює платформи для обміну даними між правоохоронними органами різних країн, що дозволяє швидко реагувати на міжнародні загрози та злочинність. Також Європол активно підтримує дослідження та розвиток нових технологій для аналізу доказів, зокрема у випадках, що пов'язані з кіберзлочинністю та воєнними злочинами. Ця організація сприяє створенню баз даних, де зберігаються зібрані докази, що дозволяє забезпечити їх доступність для міжнародних судів і правозахисних організацій.

Ще одним важливим міжнародним інститутом є Організація Об'єднаних Націй (ООН), яка через свій Офіс Верховного комісара з прав людини (OHCHR)[1] забезпечує підтримку у документуванні воєнних злочинів, зокрема через впровадження сучасних технологій збору та зберігання доказів. ООН також активно працює над розробкою міжнародних стандартів для фіксації воєнних злочинів, в тому числі через Протокол Берклі, який визначає стандарти для збору, верифікації та збереження цифрових доказів з відкритих джерел. Цей протокол був розроблений Офісом Верховного комісара ООН у співпраці з Центром прав людини Університету Берклі[2] і активно застосовується для документування злочинів, скоєних у зонах конфліктів.

Не менш важливою є роль таких громадських міжнародних організацій, як Truth Hounds[3], які з 2014 року займаються документуванням воєнних злочинів. Ці організації використовують інноваційні методи збору та аналізу доказів, включаючи роботу з відкритими джерелами та дистанційне зондування Землі для фіксації слідів злочинів. Їхня діяльність сприяє не лише національним, але й міжнародним розслідуванням, надаючи правоохоронним органам важливу інформацію для подальших юридичних процедур.

Крім того, Міжнародний центр з розслідування злочинів, пов'язаних з російською агресією проти України (ICPA)[4], який був створений у 2023 році в Гаазі, активно використовує новітні технології для збору доказів воєнних злочинів. Цей центр об'єднує прокурорів з України, ЄС, США та Міжнародного кримінального суду, що дозволяє ефективно інтегрувати інноваційні методи аналізу і збору доказів для міжнародних судових процесів.

Міжнародні організації не лише надають технічну та фінансову допомогу, а й активно сприяють розвитку технологій у криміналістиці, що дозволяє підвищити ефективність розслідувань воєнних злочинів. Їхня діяльність охоплює не лише створення технічних стандартів, а й надання практичної допомоги в зборі, збереженні та аналізі доказів, що має вирішальне значення для забезпечення справедливості на міжнародному рівні.

Висновки. 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 нада-

Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (2016) L 135 *Official Journal of the European Union* 53–114.

[1] United Nations General Assembly. (1993). Resolution 48/141: High Commissioner for the promotion and protection of all human rights <https://undocs.org/en/A/RES/48/141> дата звернення 16.12.2023.

[2] Berkeley Protocol on Digital Open Source Investigations (2020) United Nations Human Rights Office & Human Rights Center, UC Berkeley School of Law. <https://www.ohchr.org/sites/default/files/Documents/Publications/BerkeleyProtocol.pdf> дата звернення 16.12.2023.

[3] Truth Hounds. (2023) <https://truth-hounds.org/en/document/code/> дата звернення 16.12.2023.

[4] History in the making: International Centre for the Prosecution of the Crime of Aggression against Ukraine starts operations at Eurojust (2023) Eurojust <https://www.eurojust.europa.eu/ua/news/history-making-international-centre-prosecution-crime-aggression-against-ukraine-starts-operations-at-eurojus> дата звернення 16.12.2023.

ють 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.

REFERENCES

LIST OF LEGAL DOCUMENTS

LEGISLATION

1. European Parliament and Council. (2016). Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (2016) L 135 Official Journal of the European Union 53–114 [in English].

2. United Nations General Assembly. (1993). Resolution 48/141: High Commissioner for the promotion and protection of all human rights <https://undocs.org/en/A/RES/48/141> date of application 16.12.2023.

3. Rymskyi statut Mizhnarodnoho kryminalnoho sudu [Rome Statute of the International Criminal Court] Verkhovna Rada Ukrainy <https://zakon.rada.gov.ua/go/995_588> data zvernenia 16.12.2023 [in Ukrainian].

BIBLIOGRAPHY

AUTHORED BOOKS

4. Brenner S W, *Cybercrime: Criminal Threats from Cyberspace* (Praeger Security International, 2009) 320 [in English].

5. Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition* (Academic Press, 2019) 650 [in English].

6. Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Academic Press, 2021) 450 [in English].

7. Clough J, *Principles of Cybercrime* (Cambridge University Press, 2015) 450 [in English].

8. Mann S, Roberts C, *Internet Crimes: A Guide to Effective Investigations* (CRC Press, 2017) 380 [in English].

9. Kerr O S, *Computer Crime Law* (West Academic Publishing, 2022) 700 [in English].

10. *Alhorytm dii slidcho-operatyvnykh hrup Natsionalnoi politsii na zvilnenykh vid okupatsii terytoriiakh z dokumentuvannia voiennykh zlochyniv (na prykladi zvilnenykh terytorii Kyivskoi oblasti)* [Algorithm of actions of investigative and operational groups of the National Police in the territories liberated from occupation

for documenting war crimes (on the example of the liberated territories of the Kyiv region)] (Kyiv, Hol. slidche upravlinnia Nats. politsii Ukrainy, 2022) 14 [in Ukrainian].

11. *Alhorytm reahuvannia pratsivnykiv Natsionalnoi politsii na podii, pov'iazani iz obstrilamy naselenykh punktiv, unaslidok yakykh stalysia masshtabni ruinuvannia tsyvilnoi infrastruktury, nasampered krytychnoi, ta/abo znachni liudski vtraty* [Algorithm of response of National Police employees to events related to shelling of settlements, which resulted in large-scale destruction of civilian infrastructure, primarily critical, and/or significant human losses] (Kyiv, Natsionalna politsiia Ukrainy, 2022) 11 [in Ukrainian].

12. *Pam'iatka «Osoblyvyi rezhym kryminalnoho provadzhennia v umovakh voiennoho stanu»* [Memoir «Special regime of criminal proceedings under martial law»] (Kyiv, Ofis Heneralnoho Prokurora Ukrainy; Treninhovyi tsentr prokuroriv Ukrainy, 2022) 32 [in Ukrainian].

13. Pohoretskyi M A, *Problemy vykorystannia materialiv operatyvno-rozshukovoi diialnosti v kryminalnomu protsesi* [Problems of using materials of operational and investigative activities in criminal proceedings] monohrafiia (Kyiv, RVV NA SBU, 2004) 336 [in Ukrainian].

14. Pohoretskyi M A, *Funktsionalne pryznachennia operatyvno-rozshukovoi diialnosti u kryminalnomu protsesi* [Functional purpose of operational-search activity in criminal process] monohrafiia (Kharkiv, Arsis LTD, 2007) 576 [in Ukrainian].

15. Pohoretskyi M A, *Operatyvno-rozshukova diialnist i kryminalnyi protses: problemy vzaiemozv'iazku* [Operational-search activity and criminal process: problems of interrelation] monohrafiia: u 2 ch (Luhansk, Luhanskyi derzh un-t vnutr sprav im. E. O. Didorenka, 2008) Ch 1 216 [in Ukrainian].

16. Pohoretskyi M, Shelomentsev V, *Poshuk faktychnykh danykh pro zlochyny* [Search for factual data about crimes] Mizhnarodna politseiska entsyklopediia: u 10 t. / vidp red V V Kovalenko, Ye V Moiseiev, V Ya Tatsii, Yu S Shemshuchenko (Kyiv, Atika, 2010) T. VI. Operatyvno-rozshukova diialnist politsii (militsii), 750–751 [in Ukrainian].

17. Pohoretskyi M, *Spivvidnoshennia dzherel faktychnykh danykh v operatyvno-rozshukovii diialnosti ta kryminalnomu protsesu i dzherel kryminalno protsesualnykh dokaziv* [The correlation of sources of factual data in operational-search activities and criminal proceedings and sources of criminal-procedural evidence] Mizhnarodna politseiska entsyklopediia: u 10 t. / vidp red V V Kovalenko, Ye V Moiseiev, V Ya Tatsii, Yu S Shemshuchenko (Kyiv, Atika, 2010) T. VI. Operatyvno-rozshukova diialnist politsii (militsii), 937–939 [in Ukrainian].

18. Pohoretskyi M, Shelomentsev V, *Faktychni dani (dani pro fakty)* [Factual data (data about facts)] Mizhnarodna politseiska entsyklopediia: u 10 t. / vidp. red. V V Kovalenko, Ye V Moiseiev, V Ya Tatsii, Yu S Shemshuchenko (Kyiv, Atika, 2010) T. VI. Operatyvno-rozshukova diialnist politsii (militsii), 1041 [in Ukrainian].

19. Pohoretskyi M, Shelomentsev V, *Fiksatsiia faktychnykh danykh pro zlochyny* [Fixation of factual data on crimes] Mizhnarodna politseiska entsyklopediia: u 10 t. / vidp. red. V V Kovalenko, Ye V Moiseiev, V Ya Tatsii, Yu S Shemshuchenko (Kyiv, Atika, 2010) T. VI. Operatyvno-rozshukova diialnist politsii (militsii), 1042–1043 [in Ukrainian].

20. *Zastosuvannia kosmichnykh i heoinformatsiinykh tekhnolohii pid chas vyiavlennia ta rozsliduvannia kryminalnykh pravoporushen* [Application of space and geoinformation technologies during the detection and investigation of criminal offenses] metod. rek. / S S Cherniavskyi, V I Prysiazhnyi, O M Striltsiv ta in,; za zah. red. M S Tsutskiridze (Kyiv, Nats. akad. vnutr. sprav, 2023) 92 [in Ukrainian].

JOURNAL ARTICLES

21. Lutz M C, Full Automatic Conversions for AR-15 Rifles (1985) 17 *AFTE Journal Volume* 18–21 [in English].

22. Golsan R, The Papon Affair: Memory and Justice on Trial (2000) 18(2) *French Politics, Culture & Society* 1–17 [in English].

23. Golsan R, The Trial of Maurice Papon: A Study in the Politics of Memory (2001) *Memory and Justice* 123–145 [in English].

24. The Stockholm Programme – An open and secure Europe serving and protecting citizens (2010) *Official Journal of the European Union* 115 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52010XG0504 %2801 %29> date of application 10.12.2023 [in English].

25. Bondar V S, Parfonov V Yu, Pro osoblyvosti zastosuvannia novitnikh tekhnolohii u dokumentuvanni ta rozsliduvanni okremykh vydiv voiennykh zlochyniv [On the features of the application of new technologies in the documentation and investigation of certain types of war crimes] (2022) 1(1) *Kryminalistychnyi visnyk* 123–130 [in Ukrainian].

26. Dufeniuk O M, Rozsliduvannia voiennykh zlochyniv v Ukraini: vyklyky, standarty, innovatsii [Investigation of war crimes in Ukraine: challenges, standards, innovations] (2022) 1 *Baltic Journal of Legal and Social Sciences* 46–56 [in Ukrainian].

27. Pohoretskyi M A, Lysachenko Ye I, Dopustymist dokaziv u kryminalnomu protsesualnomu pravi krain Yevropeiskoho Soiuzu ta yoho vplyv na dopustymist dokaziv u kryminalnomu sudochynstvi Ukrainy [Admissibility of evidence in the criminal procedural law of the European Union countries and its impact on the admissibility of evidence in criminal proceedings in Ukraine] (2022) 3–4 *Visnyk kryminalnoho sudochynstva* 20–34 [in Ukrainian].

28. Pohoretskyi M, Operatyvno-rozshukovi zakhody: problemy pravovoho rehuliuvannia [Operational-search measures: problems of legal regulation] (2007) 14 *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)* 135–145 [in Ukrainian].

29. Pohoretskyi M, Nehlasni slidchi (rozshukovi) dii: problemy provadzhennia ta vykorystannia rezultativ u dokazuvanni [Covert investigative (search) actions: problems of conducting and using the results in proving] (2013) 1 *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav* 270–277 [in Ukrainian].

30. Pohoretskyi M, Serhieieva D, Nehlasni slidchi (rozshukovi) dii ta operatyvno-rozshukovi zakhody: poniattia, sutnist i spivvidnoshennia [Covert investigative (search) actions and operational-search measures: concept, essence and correlation] (2014) 2(33) *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)* 137–141 [in Ukrainian].

31. Pohoretskyi M, Dzherela sudovykh dokaziv [Sources of judicial evidence] (2005) 10 *Pytannia borotby zi zlochynnistiu: zbirnyk naukovykh prats* 167–178 [in Ukrainian].

32. Pohoretskyi M, Dokazy u kryminalnomu protsesi: problemni pytannia [Evidence in Criminal Proceedings: Problematic Issues] (2011) 1(3) *Chasopys Natsionalnoho universytetu «Ostrozka akademiia». Seriia «Pravo»* <https://lj.oa.edu.ua/articles/2011/n1/11pmappp.pdf> data zvernennia 10.12.2023 [in Ukrainian].

33. Pohoretskyi M A, Zakon Ukrainy «Pro operatyvno-rozshukovu-diialnist»: problemy zastosuvannia okremykh norm [The Law of Ukraine «On Operational-Investigative Activities»: Problems of Application of Certain Norms] (2001) 3 *Visnyk Akademii pravovykh nauk Ukrainy* 205–213 [in Ukrainian].

34. Pohoretskyi M A, Dokazy u kryminalnomu protsesi [Evidence in Criminal Proceedings] (2003) 2 *Visnyk prokuratury* 59–65 [in Ukrainian].

35. Pohoretskyi M A, Pro spivvidnoshennia dzherel faktychnykh danykh i dzherel dokaziv u kryminalnomu protsesi [On the correlation of sources of factual data and sources of evidence in criminal proceedings] (2009) 1 *Pravo Ukrainy* 80–85 [in Ukrainian].

36. Pohoretskyi M A, Poniattia ta sutnist lehalizatsii operatyvno-rozshukovoi informatsii [The concept and essence of legalization of operational-search information] (2010) Spets vyp 4 *Visnyk Luhanskoho derzh. un-tu vnutr. sprav im. E. O. Didorenka* 26–40 [in Ukrainian].

37. Pohoretskyi M, Shelomentsev V, Poshukovi oznaky ob'iektiv operatyvnoho poshuku: poniattia ta sutnist [Search features of operational search objects: concept and essence] (2010) 4 *Visnyk Akad. upravlinnia MVS* 114–121 [in Ukrainian].

38. Pohoretskyi M A, Shelomentsev V P, Poniattia kiberprostoru yak seredovyshcha vchennia zlochynu [The concept of cyberspace as a learning environment for crime] (2009) 2 *Informatsiina bezpeka liudyny, suspilstva, derzhavy* 77–81 [in Ukrainian].

39. Pohoretskyi M, Shelomentsev V, Pravove zabezpechennia borotby z kiberzlochynamy v Ukraini: problemni pytannia [Legal support for combating cybercrime in Ukraine: problematic issues] (2011) 8 *Visnyk prokuratury* 30–38 [in Ukrainian].

40. Pohoretskyi M, Shelomentsev V, Operatyvno-roshukova diialnist u kiberprostori [Operational and investigative activities in cyberspace] (2011) 3 *Visnyk prokuratury* 58–63 [in Ukrainian].

41. Pohoretskyi M A, Serhieieva D B, Problemni pytannia realizatsii protsesualnoho statusu poterpiloho u kryminalnomu provadzhenni [Problematic issues of implementing the procedural status of the victim in criminal proceedings] (2017) 46 (2) *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Pravo»* 118–123 [in Ukrainian].

42. Pchelina O, Fomina T, Osoblyvosti provedennia ohliadu mistsia podii pid chas dosudovoho rozsliduvannia zlochyniv, pov'iazanykh zi zbroinoiu ahresiieiu proty Ukrainy [Peculiarities of conducting a scene inspection during a pre-trial investigation of crimes related to armed aggression against Ukraine] (2023) 2 *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav* 254 [in Ukrainian].

43. Teteriatnyk H K, Bekh O V, Odazhyu Yu M, Rozsliduvannia voiennykh zlochyniv: okremi teoretyko-prykladni pytannia [Investigation of war crimes: some theoretical and applied issues] (2023) 6 *Yurydychnyi naukovyi elektronnyi zhurnal* 95–105 [in Ukrainian].

44. Shumylo M Ye, Pohoretskyi M A, Problemy vykorystannia materialiv operatyvno-rozshukovoi diialnosti v dokazuvanni u kryminalnykh spravakh: teoretychnyi ta praktychnyi aspekty [Problems of using materials of operational-detective activities in proving criminal cases: theoretical and practical aspects] (2001) 3 *Visnyk Luhanskoho in-tu vnutr. sprav* 199–209 [in Ukrainian].

CONFERENCE PAPERS

45. Pohoretskyi M A, Operatyvnyi poshuk v konteksti reformuvannia kryminalnoi yustytsii [Operational search in the context of criminal justice reform] *Shliakhy rozvytku operatyvno-rozshukovoi diialnosti v suchasnykh umovakh*: materialy nauk. – prakt. konf. na bazi Khark. nats. un-tu vnutr. sprav, 28 lystop. 2009 r. (MVS Ukrainy; Khark nats un-t vnutr sprav; Navch-nauk in-t pidhotovky fakhivtsiv kryminalnoi militsii) (Kharkiv, KhNUVS, 2009) 7–10 [in Ukrainian].

DISSERTATIONS

46. Pohoretskyi M A, Teoretychni y praktychni problemy vykorystannia materialiv operatyvno-rozshukovoi diialnosti v kryminalnomu protsesi (za materialamy Sluzhby bezpeky Ukrainy) [Theoretical and practical problems of using materials of operational-detective activities in criminal proceedings (based on materials of the Security Service of Ukraine)] (avtoref. dys. … d-ra. yuryd. nauk: spets. spets. 12.00.09. Kyiv, KNUVS, 2006) 36 [in Ukrainian].

WEBSITES

47. Amnesty International. (2023). Amnesty International Report 2022/23: The State of the World's Human Rights <https://www.amnesty.org/en/documents/pol10/5670/2023/en/> date of application 12.12.2023 [in English].

48. Berkeley Protocol on Digital Open Source Investigations. Office of the United Nations High Commissioner for Human Rights. (Geneva, 2019) <https://www.law.berkeley.edu/wp-content/uploads/2020/05/Berkeley-Protocol-ENG.pdf> date of application 07.12.2023 [in English].

49. Berkeley Protocol on Digital Open Source Investigations (2020) United Nations Human Rights Office & Human Rights Center, UC Berkeley School of Law. <https://www.ohchr.org/sites/default/files/Documents/Publications/ BerkeleyProtocol.pdf> date of application 16.12.2023 [in English].

50. Human Rights Watch. (2023). World Report 2023: Events of 2022 <https://www.hrw.org/world-report/2023> date of application 12.12.2023 [in English].

51. EU-funded Project Pravo-Justice. Promoting greater rule of law in Ukraine, in line with European standards and comparative practices. European Union <https://pravojustice.eu/> date of application 10.12.2023 [in English].

52. Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (Brussels, 2009) 624 <https://eur-lex.europa.eu/legal-content/en/ TXT/?uri=CELEX%3A52009DC 0624> date of application 10.12.2023 [in English].

53. Minnesota Protocol on the Investigation of Potentially Unlawful Deaths (2016) Minnesota Medical Examiner's Office <https://www.law.umn.edu/sites/law.umn.edu/ files/minnesota_protocol.pdf> дата звернення 07.12.2023 [in English].

54. Truth Hounds. (2023) <https://truth-hounds.org/en/document/code/> date of application 16.12.2023 [in English].

55. History in the making: International Centre for the Prosecution of the Crime of Aggression against Ukraine starts operations at Eurojust (2023) Eurojust <https://www.eurojust.europa.eu/ua/news/history-making-international-centre-prosecution-crime-aggression-against-ukraine-starts-operations-at-eurojus> date of application 16.12.2023 [in English].

56. Pam'iatka shchodo osoblyvostei orhanizatsii i provedennia slidchykh (rozshukovykh) dii pid chas rozsliduvannia napadiv (obstriliv) na tsyvilne naselennia ta ob'iekty tsyvilnoi infrastruktury [Memorandum on the specifics of organizing and conducting investigative (search) actions during the investigation of attacks (shelling) on the civilian population and civilian infrastructure] (Kyiv, Ofis Heneralnoho Prokurora Ukrainy; Treninhovyi tsentr prokuroriv Ukrainy (2022) <https://docs.google.com/document/d/ 1TyileSKvDjvKYtsRb6VgGRRVI2DAln_M/edit> data zvernennia 16.12.2023.

57. Pam'iatka shchodo osoblyvostei provedennia dopytiv poterpilykh/svidkiv stosovno doslidzhennia faktiv seksualnoho nasylstva v umovakh zbroinoho konfliktu [Memo on the specifics of conducting interrogations of victims/witnesses regarding the investigation of facts of sexual violence in armed conflict] (Kyiv, Ofis Heneralnoho Prokurora Ukrainy; Treninhovyi tsentr prokuroriv Ukrainy, 2022) 13 <https://surl.li/btvno> data zvernennia 16.12.2023.

58. Politseiski predstavyly rezultaty rozsliduvannia voiennykh zlochyniv v Ukraini na shchorichnomu zasidanni ekspertiv v Haazi [Police presented the results of the investigation of war crimes in Ukraine at the annual meeting of experts in The Hague] (2022) Natsionalna politsiia Ukrainy: ofitsiinyi vebportal <https://www.npu.gov.ua/news/politseiski-predstavyly-rezultaty-rozsliduvannia-voiennykh-zlochyniv-v-ukraini-na-shchorichnomu-zasidanni-ekspertiv-v-haazi> data zvernennia 14.12.2023.

59. Statystyka [Statistics] Ofis Heneralnoho prokurora <https://gp.gov.ua/ua/posts/statistika> data zvernennia 07.12.2023.

60. Za dopomohoiu DNK identyfikovano blyzko trokh tysiach zahyblykh ukraintsiv [Nearly three thousand dead Ukrainians identified using DNA] Natsionalna politsiia Ukrainy: ofitsiinyi vebportal <https://www.npu.gov.ua/news/za-dopomohoiu-dnk-identyfikovano-blyzko-trokh-tysiach-zahyblykh-ukraintsiv-maksym-tsutskiridze> data zvernennia 15.12.2023.

Pohoretskyi M. A.,
Doctor of Science in Law, Professor,
Vice-rector for scientific and pedagogical work,
Taras Shevchenko National University of Kyiv
ORCID ID: *0000-0003-0936-0929*

DOI: *https://doi.org/10.17721/2413-5372.2023.3-4/84-102*

APPLICATION OF ADVANCED TECHNOLOGIES IN THE INVESTIGATION AND PROOF OF WAR CRIMES (PROBLEMATIC ISSUES)

Abstract. *The article is devoted to analyzing the role and potential of advanced technologies in documenting, investigating, and proving war crimes amid Russian aggression against Ukraine.*

There is an analysis of the role of advanced technologies in documenting, investigating, and proving war crimes, as well as a justification for the necessity of further implementing the most effective among them into the theory of operational-investigative activities, criminalistics, and criminal procedure, as well as into the practice of law enforcement agencies.

The author thoroughly analyzes the capabilities and practical aspects of using space and geoinformation technologies, particularly satellite imagery, which enable obtaining precise, timely, and indisputable evidence of war crimes. Examples of successful application of these technologies include cases of mass graves in Bucha and Izium, as well as large-scale destruction of civilian infrastructure in Mariupol and Kharkiv.

The study emphasizes the exceptional effectiveness of space and geoinformation technologies (especially satellite images) in providing reliable crime evidence, virtually eliminating falsification through digital electronic signatures.

It is argued that digital and biometric technologies, such as artificial intelligence, blockchain, facial recognition, and DNA analysis, are also essential. The use of these technologies in Ukraine has facilitated rapid identification of both victims and potential perpetrators. Blockchain-based systems create secure and transparent chains of evidence crucial for subsequent international judicial proceedings.

The study demonstrates that machine learning algorithms effectively analyze large volumes of digital data, significantly reducing investigation time and ensuring a high level of evidential quality. Such technologies are actively used in OSINT investigations and interagency databases, substantially improving law enforcement coordination.

The article highlights that employing advanced technologies raises numerous legal, ethical, and technical challenges, such as personal data protection, prevention of misuse, and compliance with human rights standards. This necessitates establishing relevant legal and ethical frameworks at both national and international levels.

The conclusion emphasizes that active implementation and regulatory support for advanced technologies are crucial for enhancing the effectiveness of documentation, investigation, and proof of war crimes, thus ensuring justice in national and international criminal justice systems. Integrating advanced technologies into the documentation and investigation processes of war crimes is critically important for achieving justice for victims and effectively holding perpetrators accountable. Further research and regulatory oversight of this process are necessary to comply with international standards and protect human rights.

Keywords: *war crimes, space technologies, geoinformation systems, satellite imagery, artificial intelligence, blockchain, biometric technologies, OSINT, international law, human rights, evidence, proof, documentation, investigation, judicial control, prosecutorial supervision.*