

т імені Ярослава Мудрого, 2024. URL: <https://doi.org/10.24144/2307-3322.2024.81.2.50>

3. Злочини проти встановленого порядку несення військової служби (військові злочини) : навч. посіб. Харків : Нац. юрид. акад. України ім. Ярослава Мудрого, 2011. 320 с. – URL: https://library.nlu.edu.ua/POLN_TEXT/POSIBNIKI_2012/ViiskoviZlochini_20pf

4. Забезпечення військового правопорядку заходами кримінально-правового впливу в умовах режиму воєнного стану в Україні. URL: <https://dspace.nadpsu.edu.ua/bitstream/123456789/4304/1/Zabezpechennia%20viiskovoho%20pravoporiadku%20zakhodamy%20kryminalnopravovoho%20vplyvu%20v%20umovakh%20rezhyumu%20voiennoho%20stanu%20v%20Ukraini.pdf>

Тимчишин Павло Андрійович,

здобувач вищої освіти Навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ

Науковий керівник:

Патик Леся Леонідівна,

доцент кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ БАЗ ДАНИХ ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ У РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

Використання криміналістичних баз даних та інформаційно-аналітичних систем у розслідуванні воєнних злочинів стало одним із ключових інструментів доказування у сучасних умовах. Повномасштабна збройна агресія Російської Федерації призвела до безпрецедентного збільшення кількості кримінальних проваджень, пов'язаних із воєнними злочинами, а це, у свою чергу, потребує системного накопичення, обробки й зіставлення великого масиву даних. Традиційні форми документування та обробки інформації виявилися недостатніми для опрацювання такої кількості епізодів, свідків, підозрюваних та об'єктів. Тому цифрові криміналістичні бази даних і сучасні

інформаційно-аналітичні системи стали важливим інструментом координації розслідувань, встановлення зв'язків між подіями та формування комплексної доказової бази. Вони дозволяють накопичувати відомості про обставини злочинів, аналізувати сліди та речові докази, ідентифікувати зразки озброєння, маршрути пересування осіб та техніки, а також оперативно виявляти закономірності у скоєних протиправних діях.

Нормативне підґрунтя використання таких систем закріплено в чинному кримінальному процесуальному законодавстві. Відповідно до статті 93 Кримінального процесуального кодексу України, сторони кримінального провадження мають право збирати докази в будь-який спосіб, не заборонений законом, зокрема шляхом отримання інформації з баз даних, документів і матеріалів, у тому числі в електронній формі. Стаття 99 визначає документи як матеріальні носії інформації, що містять відомості, які можуть бути використані як доказ. До них належать витяги з баз даних та аналітичні довідки, сформовані уповноваженими органами в межах їхніх повноважень [1]. Це дає можливість слідчим і прокурорам використовувати результати автоматизованої обробки інформації та порівняльного аналізу як повноцінні докази, за умови належного оформлення та процесуального долучення.

Судова практика Верховного Суду додатково закріплює підхід до допустимості цифрових доказів у кримінальних провадженнях. У дайджестах та оглядах практики Касаційного кримінального суду (далі – ККС) за перше півріччя 2024 року системно підтверджено, що електронні документи, цифрові записи, відеоматеріали та телекомунікаційні дані є допустимими доказами за умови дотримання процесуальних правил їх отримання, фіксації та збереження [2]. В огляді ККС за червень 2024 року наголошено, що дотримання вимог статей 84, 93 та 99 КПК України під час вилучення, документування та долучення таких матеріалів забезпечує їх повноцінну доказову силу у судовому розгляді [1]. Така орієнтація судової практики підсилює важливість належного оформлення інформації, що отримується з криміналістичних баз даних та аналітичних систем, і засвідчує їх значення у сучасному доказовому процесі.

В умовах розслідування воєнних злочинів такі системи виконують одразу декілька функцій. По-перше, вони слугують засобом централізованого накопичення відомостей про події: кожен факт обстрілу, захоплення населеного пункту, знищення

цивільного об'єкта або виявлення тіл загиблих фіксується у вигляді окремого запису, який містить усі відомі параметри – дату, координати, тип боєприпасу, характер руйнувань, інформацію про можливих виконавців та свідків. По-друге, системи дають змогу порівнювати нові дані з уже наявними, що допомагає виявляти повторювані ознаки злочинів: однакові типи озброєння, характерні траєкторії обстрілів, участь одних і тих самих військових формувань у різних епізодах. Такий аналіз має ключове значення для доведення системності злочинів та встановлення зв'язку між окремими епізодами, що часто є необхідним для кваліфікації діянь як воєнних злочинів, зокрема за статтею 438 Кримінального кодексу України [4, с. 142–144].

Суттєву роль у роботі з криміналістичними базами даних відіграють спеціалізовані аналітичні підрозділи. У структурі Національної поліції України створено Департамент кримінального аналізу, який спеціалізується на збиранні, систематизації та опрацюванні даних із різних джерел. Його фахівці працюють з інформаційно-аналітичними системами, формують узагальнені звіти, проводять порівняльний аналіз, ідентифікують закономірності та можливі зв'язки між подіями. Результати цієї роботи оформлюються у вигляді аналітичних звітів, що містять відомості про джерела інформації, схеми зв'язків, аналітичні висновки та графічні матеріали (карти, схеми, часові лінії). Такі документи долучаються до матеріалів кримінального провадження як докази у вигляді документів відповідно до статті 99 КПК України. Вони відіграють важливу роль під час прийняття процесуальних рішень, пред'явлення обвинувачення та подальшого судового розгляду, особливо у справах, де йдеться про багатоепізодні злочини або дії організованих структур.

Однією з ключових переваг інформаційно-аналітичних систем є можливість інтеграції даних різного походження. Наприклад, у рамках одного провадження можуть бути зіставлені результати балістичних експертиз, дані з OSINT-джерел (відкритих джерел інформації), результати аерофотозйомки, відомості з Єдиного реєстру досудових розслідувань, бази даних зброї та боєприпасів, відомості про пересування транспортних засобів, телефонні з'єднання та геолокацію. Таке поєднання дозволяє вибудовувати повну картину злочину – від моменту планування до конкретних дій виконавців. Особливо цінною є можливість просторово-часового аналізу: за допомогою інформаційних систем

можна встановити, які підрозділи противника перебували у визначений час у певному районі, які типи озброєння були зафіксовані, а також співставити це з місцем та часом обстрілу. У багатьох випадках саме аналітична обробка даних дає змогу перейти від загальних відомостей до конкретних осіб, відповідальних за скоєння кримінального правопорушення [3].

Окрему увагу приділяють створенню єдиних централізованих баз, що накопичують докази системних злочинів. Наприклад, у таких базах фіксуються всі випадки застосування конкретних видів ракет або артилерійських систем, що дозволяє відстежувати повторюваність застосування певних зразків озброєння одними й тими самими підрозділами. Це має велике значення для доведення намірів та планомірності дій, що є однією з ознак воєнних злочинів. Крім того, інформаційно-аналітичні системи забезпечують можливість швидкого обміну інформацією між правоохоронними органами, військовими структурами та міжнародними партнерами [3]. Така інтеграція особливо важлива у випадках, коли одні й ті самі злочини розслідуються паралельно кількома органами або коли результати розслідування готуються для подання до міжнародних судових інституцій.

Попри значні досягнення, існують певні проблеми, що ускладнюють повноцінне використання криміналістичних баз і аналітичних систем. Серед них – різний рівень технічного оснащення територіальних підрозділів, відсутність повної уніфікації форматів даних, обмеженість кадрових ресурсів для глибокої аналітичної роботи. Перспективи розвитку полягають у розбудові єдиної інтегрованої інформаційної системи, яка охоплюватиме всі елементи фіксації та аналізу воєнних злочинів – від первинної реєстрації фактів до формування аналітичних матеріалів для суду. Також важливим напрямом є підвищення кваліфікації аналітиків та слідчих, розширення можливостей для міжнародного обміну даними та впровадження інноваційних технологій, зокрема інструментів штучного інтелекту для автоматизованої обробки великих масивів інформації.

Отже, криміналістичні бази даних та інформаційно-аналітичні системи є невід'ємною складовою сучасного механізму розслідування воєнних злочинів. Вони дозволяють ефективно накопичувати, зіставляти та аналізувати різномірну інформацію, формуючи системну доказову базу, яка охоплює

широкий часовий та географічний контекст. У поєднанні з діяльністю аналітичних підрозділів Національної поліції ці інструменти забезпечують якісно новий рівень розслідування складних, багатоепізодних злочинів, що мають міжнародно-правовий вимір, і стають важливою складовою майбутнього правосуддя.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9–13. Ст. 88. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 10.10.2025).

2. Огляд судової практики Касаційного кримінального суду у складі Верховного Суду. Вип. 06/2024. Київ : Верховний Суд України, 2024. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Oglyad_KKS_06_2024.pdf?utm_source=chatgpt.com (дата звернення: 10.10.2025).

3. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. Прес-реліз Верховного Суду України. *Верховний Суд України*. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1883443?utm_source (дата звернення: 10.10.2025).

4. Бондар В. С. Особливості використання спеціальних знань під час документування та розслідування воєнних злочинів. *IV Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2024 року). Чернівці : Чернівець. нац. ун-т ім. Ю. Федьковича, 2025. С. 141–147.