пріоритетним напрямом державної політики у сфері правосуддя, особливо в умовах воєнного стану, коли ефективність доказування безпосередньо впливає на забезпечення національної безпеки, суспільної стабільності та справедливості.

Список використаних джерел

1. Kolodina A. S., Fedorova T. S. DIGITAL FORENSICS: PROBLEMS OF THEORY AND PRACTICE. *Juridical scientific and electronic journal*. 2022. No. 4. P. 378–380. URL: https://doi.org/10.32782/2524-0374/2022-4/90 (date of access: 09.11.2025).

2. Kosokhatko B. S. Problems of using open-source intelligence in the investigation of crimes committed within the framework of an international armed conflict. *Uzhhorod National University Herald*. Series: Law. 2025. Vol. 3, no. 88. P. 277–284. URL: https://doi.org/10.24144/2307-3322.2025.88.3.41 (date of access: 09.11.2025).

3. Metelev O. Problems of determining the admissibility and appropriateness of digital (electronic) evidence in criminal proceedings. *Herald of criminal justice*. 2019. No. 3. P. 224–238. URL: https://doi.org/10.17721/2413-5372.2019.3/224-238 (date of access: 09.11.2025).

4. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ М-ва юстиції України від 08.10.1998 № 53/5 : станом на 30 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text

Єрмак Василь Володимирович,
здобувач при Науково-організаційному центрі Національної академії Служби безпеки України

РОЛЬ КРИМІНАЛІСТИЧНИХ ЗНАНЬ У ВИЯВЛЕННІ ТА ДОКУМЕНТУВАННІ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ ОБОРОННО-ПРОМИСЛОВОГО КОМПЛЕКСУ УКРАЇНИ

Роль криміналістичних знань у виявленні та документуванні злочинів проти основ національної безпеки на підприємствах оборонно-промислового комплексу України визначається тим, що

такі злочини, по-перше, мають підвищену латентність і часто маскуються під легальні управлінські, виробничі, зовнішньоекономічні, кадрові або інформаційно-технологічні процеси, по-друге, характеризуються багатоканальністю слідів і домінуванням документальних, цифрових та оперативно значущих відомостей, а по-третє, супроводжуються особливими режимами доступу до інформації, захисту державної таємниці, охорони критичної інфраструктури та контррозвідувального забезпечення. За цих умов виявлення і документування не можуть зводитися до реактивного фіксування вже відомих фактів, а потребують криміналістично організованої системи дій, у межах якої оперативно-розшукова діяльність, негласні слідчі (розшукові) дії, слідчі дії, цифрове доказування і прокурорський нагляд узгоджуються у єдину доказову архітектуру, орієнтовану на забезпечення як ефективності, так і процесуальної придатності результатів для доказування в суді [1; 3; 8; 10; 17; 19].

Криміналістичні знання у цій сфері виконують щонайменше три взаємопов'язані функції: методологічну, організаційно-тактичну та доказову. Методологічна функція полягає у формуванні правильного уявлення про механізм злочинної діяльності в оборонно-промисловому комплексі, про типові способи посягань на національну безпеку (від розголошення чи втрати інформації, що має обмежений доступ, до диверсійних впливів, саботажу технологічних процесів, зловживань у ланцюгах постачання, компрометації систем кіберзахисту, впровадження агентурних можливостей у цифрову інфраструктуру), а також про закономірності виникнення, відображення і збереження слідів такої діяльності у матеріальному, документальному і цифровому середовищі підприємства. Організаційно-тактична функція полягає у розробленні і застосуванні прийомів планування, взаємодії суб'єктів, вибору оптимальних процесуальних і непроцесуальних засобів отримання інформації та її фіксації з урахуванням слідчих ситуацій і ризиків втрати доказів або їх дискредитації. Доказова функція полягає у забезпеченні переходу від інформації до доказу: від виявлених відомостей, у тому числі оперативно значущих, до процесуально оформлених, перевірюваних і допустимих доказів, здатних витримати судову перевірку та відповідати вимогам верховенства права [1; 8; 15; 17; 19; 20].

Особливість оборонно-промислового комплексу як об'єкта криміналістичного пізнання полягає в тому, що він одночасно є

виробничою системою, інженерно-технологічним середовищем, інформаційною екосистемою і режимним об'єктом. Це означає, що криміналістичне виявлення злочинів проти основ національної безпеки вимагає розуміння технологічних ланцюгів, логістики, управлінських регламентів, доступів до конструкторської документації, класифікації інформації, цифрових контурів управління виробництвом і комунікацій, а також організаційної структури підприємства, що визначає розподіл повноважень і зон відповідальності. Категорія «організація» в криміналістиці тут набуває подвійного значення: з одного боку, організація як властивість злочинної діяльності (структурованість, ролі, канали, маскування), з іншого — організація як вимір криміналістичної діяльності держави (планування, координація, стандарти документування), що співвідноситься з криміналістичною тактикою [13; 14]. Саме криміналістичні знання дозволяють побачити типові точки вразливості ОПК: етапи закупівель і контрактування, доступ до технічних даних, контроль якості, процеси випробувань, сервісне обслуговування, інтеграцію імпортних компонентів, цифрові системи управління, віддалені канали доступу, використання хмарних сервісів або зовнішніх провайдерів, а також внутрішні комунікації, де можуть виникати як прямі витоки інформації, так і непрямі «слідові» ознаки небезпечних контактів або змін у поведінці персоналу.

Ключовою практичною передумовою успіху є правильний старт кримінального провадження та криміналістично обґрунтоване формування первинних версій. Початок досудового розслідування у справах проти основ національної безпеки на підприємствах ОПК часто відбувається в умовах дефіциту відкритої інформації, фрагментарності сигналів і потреби оперативного реагування для запобігання подальшій шкоді. Саме тому криміналістичні знання визначають, які дані необхідно зберегти першочергово, які джерела інформації є найбільш крихкими (лог-файли, журнали доступу, переписка, тимчасові файли, записи камер, телеметрія систем), які дії можуть призвести до незворотної втрати слідів (наприклад, неконтрольоване "перевстановлення" систем, відключення серверів, зміна паролів без фіксації), і як організувати взаємодію слідчого, прокурора, оперативних і технічних підрозділів для негайного забезпечення доказової перспективи [4; 10; 12]. У цьому контексті первинна криміналістична версія має бути не

абстрактною, а «слідовою»: вона повинна одразу проектуватися на конкретні носії інформації, конкретні середовища її виникнення і конкретні інструменти процесуального закріплення, інакше розслідування ризикує перетворитися на накопичення відомостей без доказового ядра [15; 20].

З огляду на підвищену латентність і конспіративність таких злочинів, вирішальним інструментом виявлення часто стають оперативно-розшукова діяльність та негласні слідчі (розшукові) дії. Їх функціональне призначення в кримінальному процесі полягає в тому, щоб забезпечити отримання інформації, недоступної звичайними відкритими способами, встановити приховані зв'язки, механізми, канали передачі інформації, а також попередити подальші посягання. Однак криміналістична цінність ОРД і НСРД проявляється лише за умови правильного співвідношення і розмежування цих форм діяльності, адже змішування оперативних заходів і процесуальних НСРД, підміна одного іншим або спроба «легалізувати» вже здобуті оперативні відомості без належної процедури створює високі ризики недопустимості доказів і порушення прав людини [1; 5]. Саме тому криміналістичні знання у цій сфері включають не тільки тактичні прийоми конспірації чи спостереження, а й процесуальну грамотність щодо підстав, меж, строків, цільової спрямованості, документування та подальшого використання результатів у доказуванні [3; 16]. Принциповим є й питання провокації у негласних розслідуваннях: в умовах контррозвідувальної та антикорупційної практики на режимних об'єктах завжди існує спокуса "прискорити" отримання результату, але криміналістичні знання, з'єднані з процесуальними стандартами, мають забезпечувати правомірність і виключати провокативні моделі, що підривають легітимність доказування [2].

Документування злочинів проти основ національної безпеки в ОПК вимагає інтеграції класичних криміналістичних підходів із цифровою криміналістикою та кіберпросторовою методологією, оскільки значна частина посягань сьогодні реалізується або супроводжується цифровими каналами. Розуміння кіберпростору як середовища вчинення злочину підкреслює, що сліди можуть існувати у вигляді метаданих, журналів подій, мережевого трафіку, артефактів доступу, токенів автентифікації, змін конфігурацій, а також у вигляді "слідів взаємодії" між системами, які не є очевидними для неспеціаліста

[6]. Криміналістичні знання дають змогу не лише ідентифікувати ці сліди, а й правильно організувати їх збереження, вилучення, копіювання, хешування, протоколювання та подальшу експертну інтерпретацію. У цьому контексті європейські стандарти цифрового доказування та процесуальні проблеми використання цифрових технологій у справах проти основ національної безпеки вимагають від органів розслідування, а відтак і від прокурора як процесуального керівника, забезпечити перевірюваність цифрових джерел, відтворюваність процедур, мінімізацію ризиків підміни/модифікації даних та дотримання балансу між потребами безпеки і правами людини [11; 13]. Цей баланс є не декларацією, а практичним критерієм: порушення прав людини в цифровому доказуванні підриває верховенство права і створює ризики несправедливого вироку або виправдання через дефекти доказової бази [11; 17].

Сучасні технології істотно розширюють можливості виявлення і документування посягань на ОПК, але одночасно підвищують вимоги до криміналістичної підготовки суб'єктів розслідування. Аналіз застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів показує загальну закономірність, релевантну і для злочинів проти основ національної безпеки: технологічний інструментарій ефективний лише тоді, коли він вбудований у процесуальну форму, а його результати придатні до перевірки та судового використання [9]. Для ОПК це особливо важливо, оскільки документування може включати мультисенсорні дані, аналітику з різних джерел, технічні журнали, системи контролю доступу, відеоспостереження, телеметрію, геопросторові дані, а також результати інтелектуального аналізу даних. Без криміналістичного "каркасу" такі дані можуть бути переконливими лише на рівні оперативної інформації, але не на рівні доказу [15; 20]. Відповідно, криміналістичні знання формують вимогу до стандартизації: опису процедур отримання, забезпечення цілісності, формування ланцюга походження, організації експертної оцінки та документального відтворення всіх кроків роботи з даними.

Важливою умовою легітимного документування у сфері національної безпеки є належний прокурорський нагляд за оперативно-розшуковою діяльністю та чітке визначення повноважень прокурора. Це має не суто інституційне, а криміналістичне значення, оскільки нагляд визначає рамки

допустимих тактичних рішень, контроль за пропорційністю втручань, своєчасне перетворення оперативної інформації в процесуально допустимі докази та запобігання свавільним практикам на режимних об'єктах [7; 8]. Наглядова функція, будучи спрямованою на законність ОРД, фактично є елементом управління доказовими ризиками: будь-яка помилка в оперативному блоці, якщо вона не виявлена і не компенсована належною процесуальною дією, може зруйнувати доказування або підважити довіру суду до результатів розслідування [7; 19]. У системі кримінально-процесуальних правовідносин це означає, що прокурор, слідчий і оперативні підрозділи мають взаємодіяти як елементи єдиної системи, де кожний крок підзвітний правовим стандартам і спрямований на досягнення перевірюваного доказового результату [12; 17].

Криміналістична тактика як система прийомів і рекомендацій у виявленні та документуванні злочинів проти основ національної безпеки на підприємствах ОПК має особливий режимний контекст. Тут тактичні рішення повинні одночасно забезпечувати конспірацію і безпеку, не створюючи процесуальних дефектів. Наприклад, виявлення витоку інформації може потребувати негласного спостереження, контролю контактів, аналізу цифрових артефактів і доступів, але кожен із таких інструментів має бути співвіднесений із правовими підставами і процесуальними межами, а результати — придатними для доказування. Саме тому криміналістична тактика в цій сфері є тісно пов'язаною з організацією розслідування: тактичні прийоми реалізуються через організаційні рішення, які забезпечують узгодженість дій і запобігають втраті доказів [13; 14]. У підсумку документування на режимному об'єкті є не просто фіксацією фактів, а складним процесом, що включає управління доступом до інформації, захист джерел, взаємодію з внутрішніми службами безпеки підприємства, забезпечення збереження технічної документації і цифрових систем, а також контроль за тим, щоб режим секретності не перетворювався на бар'єр для процесуальної перевірки доказів судом.

У теоретико-доказовому вимірі центральним залишається питання трансформації інформації у доказ і забезпечення допустимості. Проблематика доказів у кримінальному процесі, зокрема питання їх отримання, перевірки та оцінки, набуває в справах проти основ національної безпеки специфіки, пов'язаної з конфіденційністю джерел, використанням технічних засобів,

залученням спеціальних знань і ризиками “закритості” доказової бази від сторони захисту та суду [15; 20]. Сучасна концепція кримінального процесуального доказування підкреслює, що доказування має бути контрольованим і справедливим, а отже, будь-яка доказова інформація повинна бути обґрунтовано включена в процес, належно оформлена і доступна для перевірки, у тому числі через судовий контроль [8; 19]. Саме судовий контроль у забезпеченні справедливого та допустимого доказування виступає кінцевим “фільтром” криміналістично організованого документування: якщо доказова інформація не витримує перевірки законності, пропорційності та процесуальної форми, її криміналістична переконливість не має значення [19; 17].

Отже, роль криміналістичних знань у виявленні та документуванні злочинів проти основ національної безпеки на підприємствах оборонно-промислового комплексу України полягає у створенні цілісної методології і практичного інструментарію, який дозволяє, з одного боку, ефективно і своєчасно виявляти латентні посягання в складному режимному і технологічному середовищі, а з іншого – забезпечувати процесуальну придатність результатів для доказування, дотримання прав людини та стандартів верховенства права. У сучасних умовах цифровізації та гібридних загроз криміналістичні знання стають системоутворюючим чинником: вони поєднують ОРД, НСРД, слідчі дії, цифрове доказування, експертні технології та прокурорський нагляд в одну доказову архітектуру, спроможну забезпечити законність, перевірюваність і переконливість доказів у суді [1; 3; 8; 11; 13; 15; 17; 19]. Саме такий підхід дає змогу уникнути двох крайнощів – або “оперативної ефективності” без процесуальної чистоти, або “формальної процесуальності” без реальної здатності виявляти й документувати посягання, – і забезпечує легітимний кримінально-правовий захист національної безпеки України на стратегічно важливих підприємствах ОПК [11; 17; 19].

Список використаних джерел

1. Погорецький М. А. Початок досудового розслідування: окремі проблемні питання. *Вісник кримінального судочинства*. 2015. № 1. С. 93–103. URL: https://vkslaw.com.ua/index.php/journal/article/download/431/400/

2. Погорецький М. А., Сергєєва Д. Б. 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. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_34

3. Погорецький М. А., Коровайко О. І. Застосування тимчасового доступу до речей і документів у кримінальних провадженнях про злочин, учинені організованими злочинними угрупуваннями. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*: наук.-практ. журн. Київ : Міжвід. наук.-досл. центр з проблем б-би з орг. злоч. 2013. № 1 (29). С. 234–242. URL: http://nbuv.gov.ua/UJRN/boz_2013_1_28

4. Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчення злочину. *Інформаційна безпека людини, суспільства, держави* : наук.-практ. журнал. Київ : НАСБУ, 2009. № 2 (2). С. 77–81.

5. Погорецький М. А. Прокурорський нагляд за оперативно-розшуковою діяльністю. *Вісник Ун-ту внутр. справ*. 2000. Вип. 10. С. 117–125.

6. Погорецький М. А. Повноваження прокурора при здійсненні нагляду за оперативно-розшуковою діяльністю. *Реформування органів прокуратури України: проблеми і перспективи:* матеріали. міжн. наук.-практ. конф., 2–3 жовт. 2006 р. Київ : Вид-во Ген. прокуратури України; Акад. прокуратури України, 2007. С. 124–127.

7. Погорецький М. Прокурор у кримінальному процесі: щодо визначення функцій. *Право України*. 2015. № 6. С. 86–95. URL: https://pravoua.com.ua/storage/files/magazines/files/content-pravoukr-2015-6-pravoukr_6_15-3.pdf

8. Погорецький М. А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства України*. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf.

9. Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства.* 2023. № 3-4. С. 84–102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf

10.Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство*. 2025. № 5. Ч. 3. С. 239–256. DOI https://doi.org/10.24144/2788-6018.2025.05.3.37.

11.Погорецький М. А. Забезпечення прав людини в цифровому доказуванні як умова реалізації принципу верховенства права та постановлення справедливого вироку. *Право України.* 2025. № 9. С. 60–74. DOI: 10.33498/louu-2025-09-060.

12.Погорецький М. А. Кримінально-процесуальні правовідносини: структура і система : монографія. Харків : Арсіс ЛТД, 2002. 160.

13.Погорецький М. А., Сергєєва Д. Б. Криміналістична тактика: щодо визначення поняття.*Часопис Національного університету «Острозька академія». Серія «Право»*. 2012. № 1 (5). URL : https://lj.oa.edu.ua/articles/2012/n1/12pmasvp.pdf

14.Погорецький М., Сергєєва Д. Щодо визначення поняття "організація" у криміналістичній науці та його співвідношення із криміналістичною тактикою. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2012. Вип. 93. С. 14–17. URL: https://ir.library.knu.ua/handle/15071834/8569

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. Проведення негласних слідчих (розшукових) дій та використання їх результатів у доказуванні. *Актуальні питання досудового розслідування слідчими органів внутрішніх справ: проблеми теорії та практики*: матеріали всеукраїнської науково-практичної (м. Дніпропетровськ, 18-19 квітня 2013 року). Київ : Хлі-Тек Прес, 2013. С. 186–193.

17.Погорецький М. А. Верховенство права у кримінальному процесуальному доказуванні: методологія та практика застосування. *Вісник Національної академії правових наук України*. 2025. Т. 32. № 3. С. 275–299. DOI: https://doi.org/10.31359/1993-0909-2025-32-3-275

18.Шумило М. Є., Погорецький М. А. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти. *Вісник Луганського ін-ту внутр. справ*. Луганськ : РВВ ЛІВС, 2001. Вип. 3. С. 199–209.

19.Погорецький М. А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство.* 2025. № 4. Ч. 3. С. 269–279. DOI: https://doi.org/10.24144/2788-6018.2025.04.3.40.

20. Шумило М. Є., Погорецький М. А. Докази і доказування. Кримінально-процесуальний кодекс України. *Науково-практичний коментар: у 2 т. Т. 1* / О.М. Бандурка, Є.М. Блажіський, Є. П. Бурдоль та ін.; за заг. ред. В.Я. Тація, В. П. Пшонки, А.В. Портнова. Харків : Право, 2012. С. 247–308.

Кирюхіна Руслана Ярославівна,
ад'юнкт кафедри криміналістичного забезпечення та судових експертиз Національної академії внутрішніх справ

ПОНЯТТЯ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ, ЩО СПРИЧИНИЛИ ЗАГИБЕЛЬ ЛЮДИНИ

Сучасні виклики, зумовлені повномасштабною збройною агресією проти України, поставили перед національною системою правосуддя безпрецедентні завдання – документування, розслідування та доведення фактів воєнних злочинів, пов'язаних із загибеллю цивільних та військовослужбовців. Розкриття таких злочинів вимагає високого рівня криміналістичного забезпечення, яке охоплює систему наукових знань, методів і практичних рекомендацій, що є основою для формування належної доказової бази, встановлення обставин події та притягнення винних до відповідальності як на національному, так і на міжнародному рівнях.

Окремі питання криміналістичного забезпечення розслідування кримінальних правопорушень досліджували такі вчені, як А. С. Бондарчук, О. Л. Дульський, О. М. Дуфенюк, М. М. Єфімов, В. О. Коновалова, С П. Лапта, А. О. Левицький, О. М. Москалюк, В. Б. Пчелін, О. В. Пчеліна, В. В. Сокуренко, Р. Л. Степанюк, Ю. М. Чорноус, В. Ю. Шепітько та інші.

Водночас у науковій літературі належна увага питанням криміналістичного забезпечення розслідування воєнних злочинів, що спричинили загибель людини, досі не приділялася. Водночас у цьому контексті воно набуває специфічного змісту, оскільки включає не лише класичні криміналістичні прийоми та методи, а й адаптовані методики для умов бойових дій, документування руйнувань, масових поховань та інших наслідків агресії. В національному законодавстві відповідальність за воєнні злочини регламентується статтею 438 Кримінального кодексу