УДК 343.98:343.326:343.13.

Єрмак Василь Володимирович – здобувач Науково-організаційного центру Національної академії Служби безпеки України,
м. Харків, Україна
https://orcid.org/0009-0008-3217-7851
jockerukra@gmail.com

DOI: https://doi.org/10.59835/2413-5372.2025.3-4/324-346

Виявлення та документування шпигунства на підприємствах оборонно-промислового комплексу України

Статтю присвячено комплексному аналізу виявлення та документування шпигунства на підприємствах оборонно-промислового комплексу України як безперервного процесу, у якому первинне встановлення ознак посягання має одразу проєктуватися на процесуальну перспективу отриманих відомостей. Метою є обґрунтування доказово орієнтованої моделі оперативного пошуку й оперативно-розшукового документування з урахуванням домінування цифрових слідів, режимної чутливості середовища ОПК та підвищених стандартів судової перевірки допустимості. Методологічну основу становлять нормативний і формально-логічний підходи, криміналістичне моделювання способу посягання (підготовка–реалізація–приховування), а також ризик-орієнтований аналіз «вузлів» втрати доказів у цифровому та змішаному доказовому масиві.

Показано, що результативність протидії визначається не стільки обсягом здобутої інформації, скільки її відтворюваністю, контрольованістю походження, здатністю до незалежної перевірки та інтеграції у змагальну процедуру. Запропоновано уточнення категоріального апарату (фактичні дані, оперативно-розшукова інформація, матеріали ОРД, документи ОРД) і визначено типові процесуальні дефекти їх ототожнення, які породжують прогалини в реконструкції походження даних і підвищують ризики недопустимості. Наукова новизна полягає в обґрунтуванні операційної матриці переходу від фактичних даних до процесуальних джерел доказів та у пропозиції «паспорта доказу» як стандартизованого інструмента фіксації траєкторії доказового об'єкта, ключових параметрів середовища, обліку доступів і процедур забезпечення цілісності.

Доведено, що у справах про шпигунство в ОПК судовий контроль виконує не лише гарантійну, а й доказоутворювальну функцію: він має перевіряти пропорційність втручань, межі доступу до цифрових контурів, коректність «вшивки» результатів ОРД і НСРД та відтворюваність процедур. Практичне значення результатів полягає у формуванні рекомендацій щодо мінімізації процесуальних втрат у суді в умовах воєнного стану, коли підвищуються ризики деградації інфраструктури, аномальних режимів доступу та швидкої втрати цифрових артефактів.

Ключові слова: *шпигунство; оборонно-промисловий комплекс; оперативний пошук; оперативно-розшукове документування; легалізація матеріалів ОРД; НСРД; цифрові докази; ланцюг збереження доказів; паспорт доказу; судовий контроль; допустимість доказів; воєнний стан.*

Вступ.

Виявлення та документування шпигунства на підприємствах оборонно-промислового комплексу України в умовах воєнного стану набуває характеру комплексного завдання на стику національної безпеки, криміналістики, оперативно-розшукової діяльності та кримі-

нального процесу. Сучасна шпигунська діяльність щодо ОПК дедалі частіше поєднує класичні агентурні моделі з інсайдерським доступом до технологічних і управлінських даних, а також із використанням цифрових інструментів, які забезпечують швидке копіювання, маскування й транскордонне переміщення інформації. Це змінює сам характер доказового матеріалу: суттєва частина відомостей про подію та причетних осіб існує у вигляді цифрових слідів, метаданих, журналів доступів, версійності документів, резервних копій та електронних комунікацій, які є вразливими до втрати, модифікації й «підчищення», особливо за кризових обставин воєнного часу та підвищеної мобільності виробничих процесів (Погорецький, 2011; 2015; 2023; 2025; Сергєєва, 2025).

Ключова науково-практична суперечність полягає в тому, що високий оперативний потенціал таємних форм здобуття інформації про шпигунську діяльність сам по собі не гарантує її процесуальної придатності для цілей кримінального провадження. Навіть коли відомості здобуті результативно і своєчасно, вони можуть втратити доказове значення через дефекти фіксації, відсутність або розрив ланцюга збереження, неузгодженість із вимогами допустимості та недостатній рівень судового контролю за втручаннями, необхідними для отримання й закріплення даних. У цифровому середовищі ця проблема проявляється особливо гостро: доказова цінність артефактів залежить не лише від змісту, а й від відтворюваності процедури їх одержання, підтвердження цілісності та можливості перевірки походження кожного елемента доказового ланцюга від джерела до судового дослідження (Погорецький, 2011; 2015; 2025; Сергєєва, 2025).

Проблемне поле статті визначається потребою у цілісній відтворюваній моделі, яка зв'язує криміналістичну характеристику шпигунства в ОПК із операційними алгоритмами оперативного пошуку, фіксації фактичних даних у змішаному (матеріальному та цифровому) середовищі, подальшою інтеграцією результатів ОРД і НСРД у доказовий контур та стандартами судового контролю, що забезпечують необхідність, пропорційність і процесуальну придатність втручань. Наявні напрацювання дозволяють окреслити важливі компоненти цієї моделі, зокрема зміст і функціональне призначення оперативно-розшукового документування, роль фіксації фактичних даних, питання співвідношення негласних інструментів і процесуальної форми, а також специфіку цифрових слідів і вимог до ланцюга збереження, однак їх практична «збірка» для предметної сфери шпигунства на підприємствах ОПК потребує окремої криміналістично-процесуальної операціоналізації (Погорецький, 2007; 2010; 2013; Федорчук, 2023; Сайипов, Томма, 2025; Сергєєва, 2025).

Практичне значення дослідження полягає у підвищенні доказової стійкості матеріалів у провадженнях щодо шпигунства в ОПК і, відповідно, у зменшенні ризиків визнання доказів недопустимими через процедурні дефекти, прогалини у фіксації або розриви ланцюга збереження. Запропонований у статті підхід орієнтований на те, щоб результативність виявлення шпигунської діяльності трансформувалася у процесуально повноцінний доказовий масив, придатний для перевірки й оцінки судом, із дотриманням вимог допустимості та відтворюваності, що набуває особливої ваги у цифровізованому середовищі та в умовах воєнного часу (Погорецький, 2025; Сергєєва, 2025).

Отже, актуальність дослідження зумовлена тим, що в умовах воєнного стану шпигунство щодо підприємств ОПК стає одним із найнебезпечніших і водночас найскладніших для доказування посягань, оскільки поєднує високу латентність, інституційну «вбудованість» у виробничі та управлінські процеси й домінування цифрових слідів, які легко втрачаються або спотворюються. За таких обставин вирішальним є

не лише оперативне виявлення загрози, а й здатність забезпечити процесуальну придатність здобутої інформації через відтворювану модель документування, належну фіксацію, легалізацію, безперервний ланцюг збереження та судовий контроль допустимості доказів, що прямо впливає на ефективність кримінального переслідування та захист обороноздатності держави.

Аналіз останніх досліджень і публікацій.

Сучасний стан наукової розробленості проблематики виявлення та документування шпигунства на підприємствах ОПК формується на перетині загальної методики розслідування, криміналістичної тактики, доктрини ОРД/НСРД, теорії доказування та новітніх підходів до цифрових слідів і ланцюга збереження доказів. Умовно можна виокремити низку взаємопов'язаних напрямів, які задають теоретичний каркас для побудови відтворюваної моделі документування. Передусім це праці з методики розслідування та криміналістичної тактики, що формують загальні принципи версійності, планування, поетапності першочергових дій і тактичних рішень, важливих для справ, де доказова інформація є латентною, фрагментарною та швидкоплинною, як у випадку шпигунства; у цьому контексті вагомим є узагальнюючий методичний підхід до розслідування злочинів та прикладні розробки з криміналістичної тактики і розслідування окремих видів злочинів, а також уточнення понятійної основи тактики як елемента криміналістичного забезпечення доказування (Тіщенко, 2007; Погорецький, Сергєєва, 2012; Бишевець, Погорецький, Сергєєва та ін., 2015; Бишевець, Погорецький, Сергєєва та ін., 2017).

Важливий другий напрям становлять кримінологічні та кримінально-правові дослідження правопорушень у сфері ОПК, які дозволяють описати середовище ризиків, суб'єктні й організаційні чинники та типові контури протиправної поведінки у цій чутливій сфері. Їх евристичний потенціал полягає в тому, що вони окреслюють контекст, у якому відбувається злочинна активність, уточнюють уразливості інституційного середовища та задають вихідні орієнтири для криміналістичної характеристики і моделювання предмета доказування у справах, пов'язаних з ОПК, що є принципово важливим для коректного визначення об'єктів пошуку фактичних даних і розуміння механізмів приховування (Кожушко, 2021; Федорчук, 2023).

Третій напрям охоплює роботи з оперативно-розшукової проблематики, у яких послідовно розкривається функціональне призначення ОРД у кримінальному процесі та категоріальний апарат оперативно-розшукового документування, зокрема розуміння пошуку і фіксації фактичних даних, природи оперативно-розшукової інформації та матеріалів ОРД, а також значення документу як носія відомостей і інструмента відтворення походження інформації. У межах цього напряму важливими є підходи, що обґрунтовують орієнтацію оперативного пошуку на майбутню процесуальну перспективу та пояснюють, чому дефекти категоріального розмежування «фактичні дані – інформація – матеріали – документ» здатні породжувати системні помилки у використанні результатів ОРД у кримінальному провадженні; окремо слід відзначити наукові напрацювання щодо співвідношення джерел фактичних даних і джерел доказів як методологічного «моста» між оперативною та процесуальною площинами, а також концептуалізацію кіберпростору як середовища вчинення злочину, що вже на рівні доктрини підкреслює зміну місця виникнення слідів у сучасних кримінальних практиках (Погорецький, 2007, с. 135–145; 2009, с. 80–85; с. 112–113; Погорецький, Шеломенцев, 2009; Погорецький, 2010, с. 26–40; с. 223–225; Погорецький, Шелеменцев, 2010, с. 18–28; Погорецький, Шеломенцев, 2010, с. 192–201; Погорецький, Шеломенцев, 2010, с. 1042–1043). Для побудови приклад-

ної моделі документування шпигунства в ОПК принципове значення має також розвиток уявлень про оперативно-розшукову характеристику злочинів як інструмент управління пошуком і фіксацією, включно з галузевими підходами до оперативно-розшукової характеристики правопорушень, що вчиняються в оборонно-промисловому комплексі (Боднар, 2014; Сайипов, Томма, 2025).

Четвертий напрям становить доктрина доказування та процесуальної допустимості, у межах якої формуються критерії належності, допустимості, перевірності та відтворюваності доказової інформації, без чого неможливо коректно оцінити процесуальну перспективу матеріалів, отриманих у ході ОРД/НСРД. У цьому контексті істотними є розвідки, що проблематизують природу доказів у кримінальному процесі та уточнюють методологічні підходи до доказування, а також науково-практичні коментарі, які інституціоналізують категорії доказів і доказування у процесуальній логіці та сприяють виробленню вимог до мотивування процесуальних рішень і судового контролю; додатково сучасні праці акцентують на значенні ранньої фази досудового розслідування для збереження доказів і на оновлених стандартах судового контролю як гарантії справедливого та допустимого доказування, що безпосередньо релевантно для проваджень щодо шпигунства в ОПК (Погорецький, 2009, с. 80–85; Погорецький, 2011; Шумило, Погорецький, 2012; Погорецький, 2015, с. 63–79;, 2015, с. 93–103; 2017; 2025, с. 269–279; Погорецький, Старенький, 2018, с. 85–106).

П'ятий напрям об'єднує дослідження, присвячені інтеграції ОРД та НСРД у доказовий контур, використанню результатів негласних джерел і негласних дій, а також ризикам недопустимості, пов'язаним із порушенням меж допустимого втручання та з явищем провокації. Для цієї групи праць характерне прагнення поєднати оперативну доцільність із процесуальною формою, показати співвідношення НСРД та оперативно-розшукових заходів, окреслити вимоги до коректного використання результатів негласної діяльності й запобіжники недопустимості, що у справах про шпигунство, як різновид злочинів проти основ національної безпеки, набуває системоутворювального значення (Шумило, Погорецький, 2001; Погорецький, 2003; Погорецький, 2013; Погорецький, Сергєєва, 2014; Погорецький, 2016: Погорецький, Старенький, 2018, с. 85–106).

Шостий напрям охоплює цифровий вимір доказування: осмислення кіберпростору як середовища вчинення злочину та формування цифрових слідів, розвиток уявлень про цифрові технології як інструмент розслідування і доказування, а також пропозиції щодо криміналістично-процесуальної моделі роботи з цифровими артефактами, включно з вимогами безперервного ланцюга збереження доказів і стандартизації першочергових дій. У цій площині важливими є положення про те, що цифрові артефакти потребують невідкладної консервації, процесуально коректного вилучення та документування відтворюваності процедур, а також запропонована операційна матриця, яка пов'язує індикатор способу з джерелами відомостей, тактичними діями та процесуальною фіксацією під ризик-орієнтованим судовим контролем; для нашої теми принципово, що ці підходи є методично переносними на документування шпигунства в ОПК, де цифровий компонент часто визначає як механізм посягання, так і структуру доказового ланцюга (Погорецький, Шеломенцев, 2009; Погорецький, 2023; Погорецький, 2025, с. 239–256; Сергєєва, 2025). Додатково сучасні навчально-методичні узагальнення у сфері розслідування кримінальних правопорушень у службовій діяльності та спеціалізовані напрацювання щодо розслідування шпигунства підсилюють прикладний аспект проблеми, однак не знімають потреби у спеціальній операціоналізації саме для підприємств ОПК, де поєднуються ре-

жимні обмеження, високотехнологічні виробничі процеси й підвищена вразливість доказової інформації (Погорецький, Сергєєва, 2022; Погорецький, 2025, с. 248–262; Погорецький, Сергєєва, Топорецька, Черняк та ін., 2025).

Отже, наявний масив досліджень забезпечує вагому теоретичну та методичну основу для розуміння сутності ОРД і документування, процесуальної доктрини доказування, цифрових слідів і ланцюга збереження, а також спеціальних аспектів розслідування шпигунства. Водночас зберігається прогалина прикладного рівня: недостатньо опрацьованим залишається відтворюваний «міст» між оперативно-розшуковим пошуком і процесуальною «вшивкою» цифрових артефактів шпигунства в ОПК під судовим контролем, з урахуванням воєнних ризиків втрати даних і необхідності стандартизувати першочергові дії та пакування цифрових доказів у формі, придатній для судового дослідження (Погорецький, Сергєєва, 2022; Федорчук, 2023; Сайипов, Томма, 2025; Сергєєва, 2025).

Попри наявність значного масиву робіт з методики розслідування та криміналістичної тактики, що задають загальний каркас планування і першочергових дій, а також спеціальних узагальнень щодо розслідування окремих видів злочинів і окремих аспектів розслідування шпигунства, у науковій літературі фактично не сформовано відтворюваної криміналістично-процесуальної моделі саме для випадків шпигунства на підприємствах ОПК, яка б у єдиній логіці поєднувала криміналістичну характеристику події з оперативно-розшуковою характеристикою, алгоритмами оперативного пошуку і фіксації, цифровими слідами виробничо-управлінського середовища та стандартизованими вимогами до ланцюга збереження доказів і судового контролю допустимості. Наявні кримінологічні та кримінально-правові дослідження ОПК дають опис ризикового середовища й загальних ознак правопорушень, однак не «перекладають» цей опис у процесуально придатні алгоритми документування шпигунської діяльності з урахуванням домінування цифрових артефактів та режимних обмежень, притаманних ОПК; водночас праці з ОРД та документування ґрунтовно розкривають категоріальний апарат, фіксацію фактичних даних і питання легалізації, але не пропонують спеціальної операціоналізації для доказового контуру шпигунства в ОПК, де ключовими стають версійність цифрових документів, журнали доступів і відтворюваність процедур їх одержання та збереження. Не отримав належного опрацювання і прикладний «міст» між оперативно-розшуковим пошуком та процесуальною «вшивкою» цифрових артефактів у кримінальне провадження під судовим контролем, включно з дисципліною безперервного ланцюга збереження, стандартизацією «першої доби» та формалізацією «паспорта доказу» саме для матеріалів, типових для ОПК, а також з урахуванням воєнних ризиків втрати або спотворення даних (Тіщенко, 2007; Бишевець, Погорецький, Сергєєва та ін., 2015; Бишевець, Погорецький, Сергєєва та ін., 2017; Погорецький, Сергєєва, 2022; Федорчук, 2023; Погорецький, 2025; Сайипов, Томма, 2025; Сергєєва, 2025).

Потребують подальшого дослідження, по-перше, адаптація криміналістичної характеристики шпигунства до умов ОПК як «керуючої» моделі доказування, яка визначає предмет доказування, очікувані вузли появи слідів та пріоритети консервації цифрових артефактів; по-друге, розроблення спеціалізованої операційної матриці документування для шпигунства в ОПК, що з'єднувала б індикатори способу посягання з джерелами відомостей, тактичними діями та процесуальною фіксацією і містила б стандартизовані контрольні переліки питань для слідчого, прокурора та слідчого судді; по-третє, формалізація стандарту безперервного ланцюга збереження доказів і «паспорта доказу» для цифрових і змішаних масивів ОПК з акцентом

на відтворюваності та перевірності процедур; по-четверте, визначення процесуальних правил інтеграції результатів ОРД і НСРД у доказовий контур у спосіб, який мінімізує ризики недопустимості, включно з вимогами належної легалізації та межами допустимого втручання; по-п'яте, вироблення ризик-орієнтованих стандартів судового контролю саме для клопотань і доказових пакетів у справах про шпигунство в ОПК, де цифрова складова і воєнні обставини підвищують вірогідність втрати доказової інформації та потребу в синхронізації процесуальних дій

Мета і завдання дослідження.

Метою цього дослідження є розроблення криміналістично й процесуально узгодженої моделі виявлення та документування шпигунства на підприємствах оборонно-промислового комплексу України, яка враховує поєднання агентурних і цифрових компонентів способу посягання, домінування цифрових слідів у доказовому масиві, воєнні ризики втрати або спотворення інформації, а також потребу забезпечити належність, допустимість, перевірність і відтворюваність доказів під судовим контролем. Досягнення поставленої мети зумовило необхідність розв'язання таких завдань: уточнити теоретико-методологічні засади оперативно-розшукового виявлення і документування у контексті формування доказового контуру та визначити зміст ключових категорій, які забезпечують перехід від фактичних даних до процесуальних доказів; охарактеризувати специфіку шпигунства в середовищі ОПК як об'єкта криміналістичного пізнання, виокремивши типові особливості предмета посягання, стадійність реалізації та механізми приховування, що впливають на структуру слідів і логіку першочергових дій; обґрунтувати оперативно-розшукову характеристику шпигунства в ОПК як інструмент управління оперативним пошуком і фіксацією, пов'язавши її з версійним моделюванням та предметом доказування; визначити коло найбільш значущих джерел доказової інформації в умовах цифровізації виробничо-управлінських процесів та описати типові цифрові артефакти, релевантні для встановлення механізму шпигунського посягання і ролей причетних осіб; сформувати операційну модель документування, що поєднує індикатори способу посягання з джерелами відомостей, тактичними діями та процесуальною фіксацією, включно зі стандартом синхронізації першочергових дій і мінімізації втрат доказів у перші етапи реагування; розробити вимоги до забезпечення безперервного ланцюга збереження доказів і до уніфікованого «паспорта доказу» для цифрових та змішаних доказових масивів у провадженнях щодо шпигунства на підприємствах ОПК; визначити процесуальні умови інтеграції результатів оперативно-розшукової діяльності та негласних слідчих дій у доказовий контур із забезпеченням законності втручань, належної легалізації матеріалів та стійкості доказів у суді; окреслити критерії ризик-орієнтованого судового контролю, які дозволяють обґрунтовувати необхідність і пропорційність процесуальних рішень та одночасно забезпечувати відтворюваність процедур роботи з цифровими слідами; сформулювати практичні рекомендації щодо підвищення якості документування шпигунства в ОПК в умовах воєнного часу з урахуванням організаційних, режимних і технологічних обмежень.

Матеріали та методи.

Матеріальну основу дослідження становить корпус наукових і навчально-методичних праць із криміналістики, оперативно-розшукової діяльності та кримінального процесуального доказування, який охоплює загальнотеоретичні й прикладні розробки з методики розслідування та криміналістичної тактики, доктринальні положення про функціональне призначення ОРД у кримінальному процесі, категоріальний апарат оперативно-розшукового документування, фіксацію фактичних даних

і процесуалізацію результатів негласної діяльності, а також сучасні напрацювання щодо цифрових слідів, відтворюваності процедур і ланцюга збереження доказів. До матеріалів дослідження включено монографічні та статейні праці, що задають методологічні орієнтири доказування та допустимості, навчальні посібники й коментарні розробки, які відображають практикоорієнтовані підходи до побудови тактики і алгоритмів першочергових дій, а також спеціальні публікації, присвячені правопорушенням у сфері ОПК та оперативно-розшуковій характеристиці відповідних кримінальних проявів. Окремий пласт матеріалів становлять джерела, що дозволяють інтегрувати цифровий вимір у криміналістично-процесуальну модель документування, зосереджуючи увагу на метаданих, журналах доступів, версійності та стандартах збереження доказів у судово придатній формі (Тіщенко, 2007; Погорецький, 2007; 2009; 2011; 2015; 2017; Шумило, Погорецький, 2012; Погорецький, 2023; 2025; Сергєєва, 2025; Кожушко, 2021; Федорчук, 2023; Сайипов, Томма, 2025).

Методологічну основу становить поєднання діяльнісного та гносеологічного підходів до документування як процесу пізнання й фіксації фактичних даних із їх подальшою процесуальною перспективою, системно-структурного аналізу взаємозв'язків між криміналістичною характеристикою події, оперативним пошуком, механізмами фіксації та судовим контролем, а також формально-логічного методу для уточнення понятійних меж і розмежування категорій «фактичні дані», «інформація», «матеріали», «документ» у площині їх доказового значення. Застосовано метод криміналістичного моделювання способу вчинення як каркаса для побудови версій і визначення предмета доказування, що дає змогу зв'язати стадійність посягання з очікуваними вузлами утворення слідів у матеріальному та цифровому середовищі підприємства ОПК. Для розроблення відтворюваної практикоорієнтованої моделі використано інструменти систематизації й типологізації, які дозволяють трансформувати загальні доктринальні підходи до тактики і доказування в операційні алгоритми виявлення, консервації та пакування доказових артефактів, а також метод аналізу процесуальної придатності доказової інформації, зорієнтований на критерії допустимості, перевірності та відтворюваності процедур у суді. Урахування воєнних ризиків забезпечено через метод проблемно-орієнтованого аналізу вразливостей доказового контуру, зосередженого на запобіганні втраті цифрових слідів, мінімізації дефектів фіксації та підтриманні безперервного ланцюга збереження доказів як необхідної умови їх судової стійкості.

Виклад основного матеріалу

Виявлення та документування шпигунства на підприємствах оборонно-промислового комплексу України доцільно розглядати як єдиний безперервний процес, у межах якого первинне встановлення ознак посягання має одразу проєктуватися на майбутню процесуальну перспективу отриманих відомостей. Це зумовлює необхідність виходити не лише з факту підвищеної загрозовості ОПК, а й із специфіки середовища, у якому формується доказова інформація, та з особливостей способів шпигунської діяльності, що впливають на структуру слідів, їхню крихкість і можливості перевірки в суді.

Оборонно-промисловий комплекс є середовищем підвищеної розвідувальної активності, оскільки саме тут концентруються критично важливі для обороноздатності держави технологічні рішення, організаційні й управлінські процеси, а також цифрові масиви даних, що відображають виробничі цикли, коопераційні зв'язки, логістику, результати досліджень і випробувань. Предметом шпигунського посягання в таких умовах виступає не лише формалізована документація, але й інформація, яка існує у цифровому вигляді та опосередковано характеризує технологічні можливості,

режим функціонування підприємства, його уразливості та критичні вузли. Це зумовлює комплексність способу вчинення шпигунства, який здатен поєднувати інсайдерський доступ до інформаційних ресурсів, прикриття легальними процедурами в межах повсякденної діяльності підприємства та використання цифрових каналів для копіювання, передачі й маскування слідів такого доступу. У результаті значна частина релевантних відомостей постає не як «очевидні» матеріальні сліди, а як цифрові артефакти та їхні взаємозв'язки, що потребують правильної інтерпретації та своєчасного закріплення в належній формі.

З огляду на це логіка побудови доказового контуру у справах про шпигунство в ОПК має виходити з того, що виявлення інформації саме по собі не є достатнім, якщо не забезпечено її подальшу перевірність, відтворюваність походження та процесуальну придатність для судового розгляду. Ключовою вимогою стає орієнтація документування на формування доказової перспективи: від первинної фіксації ознак посягання і визначення носіїв відомостей до забезпечення умов, за яких отримані дані можуть бути належним чином інтегровані в кримінальне провадження та витримати перевірку на допустимість і переконливість у суді. Саме тому для цієї категорії проваджень визначальним є поєднання кримінально-правового та кримінологічного розуміння специфіки правопорушень у сфері ОПК з прикладними підходами до розслідування шпигунства, які дозволяють коректно окреслити об'єкти пошуку, механізми приховування та пріоритети фіксації доказової інформації (Кожушко, 2021; Погорецький, Сергєєва, 2022; Федорчук, 2023).

Криміналістична характеристика шпигунства в оборонно-промисловому комплексі має розглядатися не як описова «довідка» про типові прояви посягання, а як робоча модель, що організовує пізнання події, задає логіку висування і перевірки версій та структурує предмет доказування. Її методологічна цінність полягає в тому, що вона дозволяє пов'язати спосіб учинення з очікуваними слідами і джерелами відомостей, а отже – з пріоритетами першочергового виявлення, консервації та процесуальної фіксації доказової інформації. У справах цієї категорії ключовим є уявлення про спосіб як про організовану послідовність дій на стадіях підготовка–реалізація–приховування, де кожна стадія залишає специфічні, часто різнорідні сліди у матеріальному та цифровому середовищі підприємства, а також створює свої «вузли» появи доказової інформації, що вимагають пріоритетного реагування. Такий підхід забезпечує перехід від загальної постановки завдання «виявити шпигунство» до керованого конструювання версій: що саме було предметом інтересу, яким способом забезпечено доступ, які механізми передання або підготовки до передання інформації могли бути використані, які елементи маскування інтегровані в повсякденні процедури, і, відповідно, де саме повинні існувати підтверджувальні відомості, придатні для перевірки (Тіщенко, 2007; Бишевець, Погорецький, Сергєєва та ін., 2015; Бишевець, Погорецький, Сергєєва та ін., 2017).

Структурування способу за стадіями дозволяє чітко окреслити рамку предмета доказування, не зводячи її лише до формального встановлення факту незаконного отримання відомостей. На підготовчій стадії предмет доказування конкретизується через встановлення мотивованості доступу до певних інформаційних масивів, формування можливостей для такого доступу та створення умов приховування, що відображається у змінах організаційних процесів і конфігурацій доступу. На стадії реалізації ключового значення набуває відтворення фактичного механізму отримання відомостей і встановлення кореляції між діями особи та цифровими/матеріальними слідами, що підтверджують саме незаконний характер доступу і його спря-

мованість на конкретний інформаційний ресурс. На стадії приховування предмет доказування доповнюється фактами, які свідчать про умисне маскування, спотворення або знищення слідів, у тому числі через використання формально легальних процедур і документальних «обгорток», а в цифровому середовищі – через маніпуляції версійністю, журналами та іншими артефактами. Саме тому криміналістична характеристика виконує функцію «карти ризиків втрати доказів»: вона визначає, які дані потребують першочергового «замороження», щоб уникнути їх зникнення або трансформації, і які з них мають бути зафіксовані таким чином, аби зберегти відтворюваність походження та можливість подальшої судової перевірки. У результаті формується цілісний підхід, за якого версії будуються не абстрактно, а на основі прогнозованих вузлів доказової інформації, а процесуальна фіксація планується як невід'ємна частина криміналістичного моделювання події шпигунства в ОПК (Тіщенко, 2007; Бишевець, Погорецький, Сергєєва та ін., 2015; Бишевець, Погорецький, Сергєєва та ін., 2017).

Результативність протидії шпигунству на підприємствах ОПК значною мірою визначається тим, наскільки правильно організовано оперативний пошук як особлива форма пізнання події, спрямована на встановлення носіїв інформації про посягання та локалізацію фактичних даних, що відображають механізм злочинної діяльності. У таких провадженнях вирішальним є не лише реагування на вже відому подію, а здатність виявляти латентні ознаки підготовки, реалізації та приховування шпигунських дій у середовищі, де значна частина релевантних відомостей не має «очевидних» матеріальних проявів і існує у вигляді розпорошених слідів у документах, технологічних ланцюгах, інформаційних системах, режимних процедурах і комунікаціях. Саме тому оперативний пошук виступає центральним механізмом встановлення того, де саме зосереджені фактичні дані, які можуть бути використані для подальшого доказування, а також які об'єкти мають першочергово потрапити в поле фіксації, щоб запобігти їх втраті або спотворенню.

Оперативний пошук у цьому контексті не може розумітися як фрагментарний збір відомостей за ситуативними ознаками, оскільки така логіка ускладнює подальшу процесуальну перспективу результатів, створює прогалини в походженні даних і підвищує ризики їхньої неперевірності в суді. Навпаки, він має будуватися як керований процес пізнання, у якому об'єкти пошуку визначаються з урахуванням предмета доказування та прогнозованих вузлів утворення слідів, а отримані відомості від початку орієнтуються на критерії доказової якості. Це означає, що оперативний працівник, здійснюючи пошук, має мислити категоріями майбутнього кримінального провадження: які факти повинні бути встановлені, які зв'язки підлягають підтвердженню, які дані здатні стати доказовою інформацією за умови належної фіксації та легалізації, і які дефекти збору або документування унеможливлять їх використання в суді. У такій логіці оперативний пошук стає не автономною «оперативною» активністю, а функціонально підпорядкованою завданню формування процесуально перспективного доказового масиву (Погорецький, 2007; Погорецький, 2009; Погорецький, Шеломенцев, 2010; Сайипов, Томма, 2025).

Особливість пошуку у справах про шпигунство в ОПК полягає в тому, що носії інформації часто мають змішану природу: це можуть бути як матеріальні документи, носії та предмети, так і цифрові середовища, у яких відображаються факти доступу, копіювання, переміщення даних і взаємодії з інформаційними ресурсами. Відтак встановлення об'єктів пошуку потребує поєднання організаційно-тактичного підходу з чіткою доказовою орієнтацією: необхідно не лише виявити релевантні відомості, а й забезпечити їх відтворюваність через

правильне відбиття походження, контексту і порядку одержання, що згодом стане критичним для оцінки належності та допустимості. У цьому полягає принципова вимога: оперативний пошук має оцінюватися не лише за критерієм оперативної ефективності, а й за критерієм доказової перспективи, оскільки саме вона визначає реальну спроможність держави трансформувати виявлену шпигунську активність у переконливий і процесуально стійкий доказовий контур у суді (Погорецький, 2007; Погорецький, 2009; Погорецький, Шеломенцев, 2010; Сайипов, Томма, 2025).

Оперативно-розшукове документування: категоріальний апарат, фактичні дані, фіксація і документ як носій доказової інформації. У провадженнях щодо шпигунства в ОПК вирішальним є не лише здобуття відомостей про посягання, а й правильне категоріальне «пакування» цих відомостей у межах оперативно-розшукового документування, оскільки саме від цього залежить подальша процесуальна перспектива результатів. Для уникнення доказових втрат необхідно чітко розрізняти принаймні чотири взаємопов'язані, але не тотожні категорії: фактичні дані, оперативно-розшукову інформацію, матеріали ОРД та документи ОРД. Фактичні дані в оперативно-розшуковому вимірі є відомостями про факти та обставини, які потенційно мають значення для встановлення події, механізму та причетних осіб, однак самі по собі ще не є процесуальним доказом, доки не набудуть відповідної процесуальної форми та не стануть перевірними у кримінальному провадженні. Оперативно-розшукова інформація за своїм обсягом ширша, оскільки може включати як відомості, що прямо орієнтують на предмет доказування, так і дані, необхідні для прийняття оперативних рішень, планування пошуку, оцінки ризиків, визначення напрямів перевірки, тобто не завжди має безпосередній доказовий «вихід». Матеріали ОРД слід розуміти як матеріально зафіксований результат і «слід» оперативно-розшукової діяльності, в якому відображено здобуті відомості, порядок їх одержання та значущі рішення, прийняті у ході документування, і саме матеріалізація надає можливість відтворити походження й контекст інформації. Документ ОРД при цьому є конкретним носієм, у якому в установленій формі зафіксовано оперативно-розшукову інформацію; він є структурним елементом матеріалів ОРД, але не вичерпує їх змісту й функцій, оскільки матеріали можуть охоплювати сукупність різних носіїв і відображень процесу пізнання події, необхідних для подальшої перевірки (Погорецький, 2009, с. 112–113; 2010, с. 223–225).

Підміна або ототожнення цих категорій породжує типові процесуальні дефекти, що у справах про шпигунство набувають критичного значення через високі стандарти судової перевірки допустимості та вразливість цифрових артефактів. Коли оперативно-розшукову інформацію фактично ототожнюють із доказом, у суду та сторін провадження зникає можливість перевірити походження відомостей, законність і відтворюваність способу їх одержання та цілісність ланцюга переходу від фактичних даних до процесуальної форми. Коли матеріали ОРД зводяться лише до окремого документа, втрачається контекст фіксації, логіка послідовності дій і рішень, що унеможливлює належну оцінку повноти, релевантності та перевірності відомостей. Коли ж документування підміняється суто «документальним оформленням», без відображення істотних елементів пізнання події та контролю шляху формування інформації, виникають прогалини, які згодом трансформуються у сумніви щодо належності, допустимості й переконливості доказового масиву (Погорецький, 2011).

У цьому контексті фіксація фактичних даних має розумітися як ключова умова процесуальної перспективи: вона повинна забезпечувати не лише збереження змісту відомостей, а й відтворю-

ваність їх походження, контрольованість шляху отримання та можливість перевірки того, як саме ці дані були здобуті, ким, у яких межах повноважень і за яких умов. Інакше кажучи, для шпигунства в ОПК критичним є принцип, за яким фіксується не тільки результат, а й суттєві параметри процесу його формування, що надалі дозволяє легалізувати матеріали та інтегрувати їх у кримінальне провадження без втрати доказового значення. Саме така логіка забезпечує перетворення фактичних даних, здобутих у ході оперативного пошуку, на процесуально придатну доказову інформацію, здатну витримати перевірку у суді (Погорецький, 2009, с. 80–85; Погорецький, Шеломенцев, 2010, с. 1042–1043).

Ключовим переходом у справах про шпигунство на підприємствах ОПК є перетворення результатів оперативно-розшукового документування з масиву матеріалів ОРД на процесуально придатні джерела доказів, придатні для судової перевірки, тобто їх належна легалізація і подальша інтеграція в кримінальне провадження з дотриманням вимог допустимості. Самі по собі матеріали ОРД виконують передусім функцію орієнтації, формування версій і обґрунтування необхідності подальших процесуальних кроків, але доказове значення вони набувають лише за умови, що фактичні дані, відбиті у цих матеріалах, будуть одержані, закріплені та перевірені у формах і порядку, які забезпечують належність, допустимість і відтворюваність, а також дозволяють суду й сторонам відстежити походження інформації та оцінити законність втручань, що лежать в її основі (Погорецький, 2003; 2010).

Специфіка проваджень щодо шпигунства в ОПК полягає в тому, що значна частина релевантної інформації існує у режимно чутливому, технологічно складному та цифровізованому середовищі, а отже ризики процесуальної неспроможності матеріалів виникають не лише через формальні порушення, а й через неможливість відтворити шлях формування даних, підтвердити їх цілісність і забезпечити судову перевірку без розкриття відомостей, що становлять охоронювані законом таємниці. Тому легалізація має бути спроєктована наперед як частина загальної доказової стратегії: уже на стадії оперативного документування слід закладати логіку того, які саме факти підлягають доведенню, які відомості мають бути переведені у процесуальні форми, які елементи потребують розсекречення чи спеціального режиму використання, і як забезпечити безперервність контролю за походженням і цілісністю даних, щоб уникнути сумнівів у їх допустимості на етапі судового розгляду (Погорецький, 2010; 2013).

«Вшивка» результатів ОРД у кримінальне провадження у таких справах має означати не механічне долучення наявних матеріалів, а їх системну трансформацію у процесуально перевірний доказовий контур через належні процесуальні інструменти та, за потреби, через застосування негласних слідчих (розшукових) дій у межах установлених підстав і гарантій. Саме тому співвідношення ОРД, оперативно-розшукових заходів і НСРД набуває прикладного значення: воно визначає, які саме результати можуть бути використані як орієнтири для процесуальних рішень, які потребують додаткового процесуального «підкріплення», а також які вимоги мають бути виконані, щоб інформація, здобута негласним шляхом, не втратила доказової перспективи через порушення меж допустимого втручання або дефекти фіксації й подальшої легалізації (Погорецький, 2013; Погорецький, Сергєєва, 2014).

НСРД та ОРЗ у справах про шпигунство: співвідношення, межі застосування і ризики провокації. У провадженнях щодо шпигунства на підприємствах ОПК негласний інструментарій має об’єктивно підвищене значення, оскільки подія злочину, як правило, є латентною, а ключові епізоди підготовки, доступу до інформації та передання відомостей відбуваються приховано й залишають

обмежену кількість «очевидних» слідів. Водночас саме у цій категорії справ найбільш виразно проявляється залежність доказової стійкості від правильного співвідношення оперативно-розшукових заходів і негласних слідчих (розшукових) дій, від визначення меж їх застосування та від того, наскільки коректно результати негласної діяльності інтегруються у процесуальний контур без дефектів допустимості. Вирішальним є підхід, за якого ОРЗ і НСРД не використовуються як універсальний «паралельний» спосіб добування будь-яких відомостей, а підпорядковуються моделі способу посягання й предмету доказування, тобто спрямовуються на встановлення саме тих фактів і зв'язків, які необхідні для доведення складу злочину, ролі особи та механізму події, із попереднім прогнозуванням, яким шляхом ці результати будуть процесуально «підхоплені», перевірені й представлені в суді. За такої логіки негласні інструменти виконують не самодостатню функцію, а функцію цілеспрямованого заповнення доказових прогалин, підтвердження критичних вузлів версії та забезпечення контрольованого переходу від фактичних даних до процесуальних джерел доказів, що мінімізує ризики фрагментарності та «розірваності» доказового ланцюга.

Співвідношення НСРД та ОРЗ у доказовому вимірі означає, що кожне втручання має бути обґрунтованим необхідністю для встановлення конкретних обставин, співмірним із завданням і здійсненим у такій формі, яка дозволяє відтворити його законність, межі та результати. Для шпигунства це набуває особливої ваги, оскільки саме негласні результати часто стають ядром доказової конструкції, а отже будь-який дефект правової підстави, процедури, меж дозволу або фіксації здатен трансформуватися у втрату допустимості ключових відомостей. Тому інтеграція негласних результатів повинна здійснюватися не шляхом їх «накопичення», а шляхом процесуально коректного включення у загальний доказовий масив із забезпеченням перевірності: по-перше, через чітке відображення походження, часу, умов одержання та меж втручання, по-друге, через кореляцію з іншими доказовими джерелами, які підтверджують або конкретизують отримані відомості, і, по-третє, через дотримання логіки предмета доказування, щоб негласні результати не залишалися «самодостатніми» фрагментами без доказового контексту.

Окремого акценту потребує запобіжник недопустимості у вигляді недопущення провокації та забезпечення коректної процесуальної форми використання негласних результатів. У справах про шпигунство ризик провокації може виникати тоді, коли активність уповноважених суб'єктів не обмежується фіксацією та перевіркою вже наявної злочинної ініціативи, а переходить у площину ініціювання або стимулювання вчинення діяння, яке без такого впливу могло б не відбутися. З позицій допустимості доказів принциповим є, щоб негласні заходи були спрямовані на документування реальної поведінки особи в межах вже наявних ознак посягання та перевірки обґрунтованих версій, а не на конструювання події. Водночас коректна процесуальна форма використання негласних результатів передбачає, що отримані відомості мають бути належним чином відображені й легалізовані у межах кримінального провадження таким чином, щоб суд міг оцінити як зміст, так і законність та відтворюваність шляху одержання цих даних, а сторона захисту мала реальні можливості для їх перевірки й спростування у змагальній процедурі. Саме поєднання доказово орієнтованого планування негласних заходів, їх підпорядкування моделі способу і предмету доказування та чіткого дотримання меж допустимого втручання формує практичний механізм, який одночасно підвищує результативність викриття шпигунства і знижує ризики процесуальних втрат на стадії судового розгляду (Шумило, Погорецький, 2001; Погорецький, 2013;

Погорецький, Сергєєва, 2014; Погорецький, 2016).

У справах про шпигунство на підприємствах ОПК цифрове середовище виступає самостійним місцем утворення слідів і, по суті, окремим «простором події», у якому фіксуються як підготовчі дії, так і реалізація доступу, копіювання чи переміщення інформації, а також подальше приховування. Це означає, що доказове значення мають не лише «змістовні» файли або повідомлення, а й цифрові артефакти процесу, які відображають траєкторію доступу до даних, послідовність операцій і часову структуру події. Саме тому кіберпростір і корпоративні інформаційні системи підприємства ОПК слід розглядати як середовище, де формуються і зберігаються фактичні дані, здатні підтвердити або спростувати версії про спосіб посягання, роль конкретних осіб та механізм отримання відомостей, причому вирішальною стає спеціальна криміналістично-процесуальна дисципліна роботи з такими даними, орієнтована на перевірність і відтворюваність (Погорецький, Шеломенцев, 2009; Погорецький, 2023; Погорецький, 2025; Сергєєва, 2025).

Типові групи цифрових артефактів, релевантні для середовища ОПК, охоплюють, по-перше, дані про ідентифікацію та авторизацію користувачів у корпоративних системах, що відображають факти входу, зміну прав доступу, використання облікових записів і параметри сесій; по-друге, журнали доступу до інформаційних ресурсів, у яких фіксуються звернення до файлів, баз даних, сховищ, реєстрів, внутрішніх порталів та спеціалізованих виробничих систем; по-третє, сліди документообігу і версійності, які відображають, ким і коли створювалися, змінювалися та погоджувалися документи, які редагування вносилися, як рухалися документи маршрутами узгодження і чи були ці маршрути узгоджені з внутрішніми процедурами; по-четверте, метадані файлів і об'єктів, що містять відомості про час створення, модифікації, авторство, середовище створення, атрибути носія і технічні властивості, які дозволяють встановлювати «технічну біографію» об'єкта; по-п'яте, дані комунікацій у межах корпоративних каналів, які відображають взаємодії, узгодження дій та інформування, а також сліди резервного копіювання і відновлення, що часто є критичними для реконструкції первісного стану даних у разі спроб їх знищення або модифікації. У контексті ОПК ці артефакти набувають особливої ваги тому, що дозволяють виявляти не лише сам факт доступу, а й організаційно-технологічний контекст події, включно з тим, чи відповідає поведінка суб'єкта його службовим функціям, чи існують аномалії у траєкторії доступу та чи узгоджується цифровий «слід процесу» з заявленими поясненнями.

Логіка доказового прочитання цифрових слідів базується на поєднанні атрибуції, темпоральної кореляції та перевірки узгодженості. Атрибуція спрямована на встановлення того, хто саме здійснював дію у цифровому середовищі, в яких межах прав і доступів та в якому технологічному контексті, при цьому значення мають не тільки формальні атрибути облікового запису, а й сукупність узгоджених ознак, що відбиваються у журналах доступу, параметрах сесій і метаданих. Темпоральна кореляція дозволяє зіставляти часові мітки різних артефактів і вибудовувати послідовність подій, виявляти розриви, неузгодженості та «аномальні» інтервали, які не пояснюються звичайною виробничо-управлінською логікою. Саме часові кореляції у поєднанні з метаданими й журналами доступів часто стають інструментом викриття «легенд» і приховування, коли формально правдоподібні пояснення не підтверджуються цифровим слідом процесу, а заявлена послідовність дій суперечить технічним відбиткам у системах. Перевірка узгодженості означає зіставлення цифрових артефактів між собою та з організаційною реальністю: якщо певна дія справді мала місце

як елемент службового процесу, вона повинна залишити узгоджені сліди в декількох взаємопов'язаних джерелах, тоді як шпигунська поведінка, навіть маскована під легальні процедури, зазвичай продукує специфічні невідповідності у часових мітках, версійності, маршрутах доступу й логіці погоджень.

Отже, цифрові сліди у справах про шпигунство в ОПК мають подвійне значення: вони, з одного боку, відображають об'єктивні параметри події, а з іншого – дозволяють перевіряти достовірність пояснень і реконструкцій через відтворювані технічні маркери. Саме тому робота з такими артефактами повинна здійснюватися як криміналістично й процесуально дисциплінований процес, орієнтований на те, щоб кожен цифровий елемент міг бути атрибутований, часово співвіднесений, перевірений на узгодженість і підготовлений до судового дослідження без втрати перевірності та доказової переконливості (Погорецький, Шеломенцев, 2009; Погорецький, 2023; Погорецький, 2025; Сергєєва, 2025).

Для проваджень щодо шпигунства в ОПК центральною умовою судової придатності доказової інформації є безперервний ланцюг збереження доказів, оскільки саме він забезпечує можливість відтворити шлях доказового об'єкта від моменту його виявлення до моменту дослідження в суді та підтвердити незмінність його стану на кожному етапі. У цифровізованому середовищі підприємства ОПК доказовий масив, як правило, має змішану природу і включає електронні дані, їхні метадані та журнали подій, цифрові копії документів, носії з інформацією, а також матеріальні об'єкти, пов'язані з доступом до відомостей або їх переміщенням; тому вимога ланцюга збереження поширюється не тільки на «файл» чи «носій», а на всю траєкторію формування й контролю доказу, включно з фіксацією умов, у яких він існував, і процедур, за допомогою яких із ним здійснювалися дії. Зміст ланцюга збереження у цьому контексті полягає, по-перше, у контролі незмінності доказового об'єкта, тобто у підтвердженні того, що після вилучення або копіювання він не був модифікований, пошкоджений чи підмінений; по-друге, у фіксації середовища, з якого отримано дані, включно з параметрами, що мають значення для правильного тлумачення цифрових артефактів і часових міток; по-третє, в обліку доступів і переміщень, що дозволяє встановити, хто саме, коли і з якою метою мав доступ до об'єкта, які операції здійснювалися та де і в яких умовах він зберігався. Саме ці елементи роблять процедуру роботи з доказом відтворюваною і перевірною, а відтак знижують ризики сумнівів щодо допустимості та переконливості доказової інформації у суді, що особливо важливо для шпигунства в ОПК, де доказовий масив часто ґрунтується на цифрових слідах і є вразливим до швидких змін або втрати.

Формалізація ланцюга збереження потребує уніфікованого інструмента подання походження та перевірки доказового об'єкта, яким доцільно використовувати «паспорт доказу» як стандартизовану форму опису доказу й усіх критично значущих параметрів його існування та обробки. Такий «паспорт» виконує дві функції. Перша є ідентифікаційною й полягає у точному визначенні, який саме об'єкт є доказом, з якого джерела та за яких умов він отриманий, у якій формі існує оригінал і які похідні копії створено. Друга є контрольної-протокольною й полягає у відображенні заходів, що забезпечують незмінність і перевірність: які процедури застосовано для консервації, як зафіксовано середовище, яким чином документовано доступи й переміщення, як підтверджувалася цілісність на етапах зберігання, експертного дослідження та підготовки до судового розгляду. У результаті «паспорт доказу» перетворює ланцюг збереження з «внутрішньої» організаційної практики на процесуально зрозумілий і перевірний для суду механізм,

який дозволяє оцінювати не лише зміст доказу, а й надійність процедури його формування та збереження. Для шпигунства в ОПК це має системоутворювальне значення, оскільки саме від відтворюваності й контрольованості шляху доказу залежить, чи буде цифровий або змішаний доказовий масив сприйнятий судом як допустимий і переконливий, чи ж буде дискредитований через прогалини у фіксації, нез'ясоване походження копій або невизначеність щодо змін у процесі обігу доказового об'єкта (Погорецький, 2015; Погорецький, 2025; Сергєєва, 2025). У кримінальних провадженнях про шпигунство на підприємствах ОПК захисник виступає не лише процесуальним гарантом прав особи, а й самостійним суб'єктом доказування на досудовому провадженні: ініціює перевірку версій, подає докази та клопотання, здатні впливати на оцінку допустимості й достатності зібраних матеріалів (Погорецький, 2014: 480–482). Тактика захисника як складова криміналістичної тактики орієнтована на виявлення дефектів фіксації, легалізації та ланцюга збереження фактичних даних, що є критичним за домінування цифрових слідів у справах про шпигунство (Погорецький, Сергєєва, 2016: 113–123).

У провадженнях щодо шпигунства в ОПК судовий контроль набуває не лише формально-гарантійного, а й визначального доказового значення, оскільки саме через нього забезпечується легітимність втручань, необхідних для здобуття та закріплення відомостей, і саме він часто визначає, чи буде сформований доказовий масив стійким на стадії судового розгляду. Особливість цієї категорії справ полягає в тому, що доказова інформація переважно є високоризиковою з погляду втрати або спотворення, часто існує у цифровому середовищі, а доступ до неї нерідко пов'язаний із втручанням у сфери, що потребують підвищених гарантій законності та процесуальної обґрунтованості. У зв'язку з цим судовий контроль має бути ризик-орієнтованим, тобто будуватися навколо оцінки реальної необхідності втручання, його пропорційності меті та здатності обраної процедури забезпечити перевірність і відтворюваність результатів. У практичному вимірі це означає, що клопотання сторони обвинувачення повинні містити не декларативне посилання на важливість справи, а логічно вибудувану аргументацію: які саме обставини підлягають доведенню, чому вони не можуть бути встановлені менш інтенсивними засобами, які ризики втрати доказової інформації існують у разі зволікання або обмеження доступу, та як саме запланована дія забезпечить збереження, цілісність і можливість подальшої перевірки одержаних даних. Аналогічно, фіксація результатів повинна бути мотивованою не лише з позицій формальної правильності, а й з позицій відтворюваності процедури: суд має мати можливість переконатися, що отриманий доказ є наслідком контрольованого і правомірного процесу, а не «випадкового» накопичення матеріалів із невизначеним походженням.

Логіка оцінки доказів у таких провадженнях спирається на доктринальне розрізнення фактичних даних і процесуальних доказів, яке дозволяє пояснити, чому не будь-яка інформація, навіть достовірна за змістом, може бути використана як доказ без належної процесуальної форми та перевірності. У цьому сенсі фактичні дані, здобуті в ході оперативного пошуку або негласної діяльності, становлять лише вихідний інформаційний матеріал, який набуває статусу процесуального доказу лише тоді, коли він одержаний і закріплений у формах, що відповідають вимогам належності та допустимості, а також забезпечують можливість його перевірки у змагальній процедурі. Саме тому «нова концепція» доказування та пов'язані з нею науково-практичні підходи до доказів і доказування підкреслюють значення процесуальної форми, мотивованості рішень і відтворюваності процедур як критеріїв судової придатності доказової ін-

формації: доказ оцінюється не тільки за тим, що він містить, а й за тим, як він був здобутий, чи може інша сторона перевірити його походження, чи збережено цілісність і чи можна повторити ключові елементи процедури одержання та фіксації без втрати змісту і доказової сили. У справах про шпигунство в ОПК ці вимоги набувають особливої ваги, оскільки саме цифрові артефакти та негласні результати часто є центральними для встановлення механізму посягання, а будь-які сумніви щодо законності, пропорційності або відтворюваності їх одержання безпосередньо трансформуються у процесуальні втрати в суді (Погорецький, 2009, с. 80–85; Погорецький, 2011; Шумило, Погорецький, 2012; Погорецький, 2015, с. 63–79; Погорецький, 2017; Погорецький, 2025, с. 269–279).

Мінімізація процесуальних втрат у суді передбачає, що ризик-орієнтований судовий контроль повинен бути інтегрований у доказову стратегію від початку, а не розглядатися як «формальна стадія» санкціонування. Клопотання про проведення дій, спрямованих на здобуття чи фіксацію доказів, мають відображати внутрішню логіку предмета доказування і моделі способу посягання, демонструвати необхідність саме таких меж доступу й обсягу даних, а також пояснювати, яким чином буде забезпечено контроль незмінності, фіксацію середовища, облік доступів і переміщень та інші елементи, що зумовлюють відтворюваність. У свою чергу, протокольна і документальна фіксація результатів повинна бути побудована так, щоб суд у подальшому міг перевірити не тільки відповідність дії санкціонованим межам, а й наявність логічного і технологічного «містка» між джерелом інформації та представленим доказом. Саме поєднання мотивованого судового контролю, належної процесуальної форми і відтворюваних процедур роботи з доказовими об'єктами забезпечує доказову стійкість у справах про шпигунство в ОПК і знижує ризики того, що ключові відомості будуть виключені із доказового масиву як недопустимі або втратять переконливість через процедурні прогалини (Погорецький, 2009, с. 80–85; Погорецький, 2011; Погорецький, 2015, с. 93–103; Погорецький, 2017; Погорецький, 2025, с. 269–279; Шумило, Погорецький, 2012).

Воєнний час виступає самостійним фактором доказового ризику у провадженнях щодо шпигунства на підприємствах ОПК, оскільки він одночасно підсилює мотивацію противника до отримання критичної інформації та ускладнює контроль середовищ, у яких формуються сліди посягання. Умови війни змінюють режим функціонування підприємств, посилюють динаміку організаційних процесів, збільшують мобільність персоналу, підрядників і логістичних ланцюгів, а також створюють додаткові технічні ризики, пов'язані з аварійними режимами енергозабезпечення, релокаціями, частковою деградацією цифрової інфраструктури та нерівномірністю захисних контурів. У такому середовищі цифрові сліди, які у мирний час могли б бути доступними для ретроспективного аналізу, у воєнних умовах стають значно вразливішими: журнали подій можуть перезаписуватися, резервні копії не завжди зберігаються повно, системи можуть працювати у спрощених режимах, а доступи можуть тимчасово розширюватися з міркувань безперервності виробництва, що створює додатковий простір для маскування шпигунської активності. Одночасно зростає імовірність втрати матеріальних носіїв та документів унаслідок переміщень або пошкоджень, що підсилює потребу в оперативному, відтворюваному та технологічно дисциплінованому документуванні.

За таких умов стандарти «першої доби» у справах про шпигунство в ОПК набувають визначального значення, оскільки саме початкова фаза реагування часто визначає, чи буде збережено критичні вузли доказової інформації, чи ж вони будуть втрачені безповоротно або

спотворені настільки, що їхня судова придатність стане сумнівною. Практично це означає, що першочергові дії мають бути спрямовані на негайну консервацію найбільш уразливих цифрових артефактів і середовищ, у яких вони існують, а також на забезпечення безперервного ланцюга збереження доказів від моменту виявлення до передачі в подальшу процесуальну роботу. У воєнних умовах критичною стає синхронізація дій, що запобігає «вікнам» для підчищення слідів, і своєчасне документування параметрів середовища, включно з тими, які у мирний час могли б сприйматися як другорядні, але в кризовому режимі можуть визначати можливість коректної інтерпретації метаданих і часових кореляцій. Саме тому пріоритетом стає не збільшення обсягу зібраних даних, а забезпечення їх відтворюваності та контрольованості, тобто здатності підтвердити, що конкретний цифровий артефакт походить із певного середовища, отриманий у визначений спосіб і не зазнав неконтрольованих змін на шляху до судового дослідження.

Організаційні висновки щодо забезпечення доказової стійкості у змінному середовищі ОПК полягають у тому, що документування шпигунства має плануватися як система, здатна працювати під умовами нестабільності, а не як набір процедур, розрахованих на «ідеальний» режим функціонування інфраструктури. По-перше, необхідно виходити з домінування цифрової складової і, відповідно, розглядати цифрові контури підприємства як основне місце утворення слідів, що потребує першочергової консервації. По-друге, стандарти консервації мають бути поєднані зі стандартами ланцюга збереження, оскільки у воєнний час зростають ризики неконтрольованого переміщення носіїв, зміни конфігурацій доступу та втрати контексту походження даних. По-третє, необхідно забезпечити таку організацію документування, за якої навіть за умов релокації, аварійних режимів або часткової втрати інфраструктури зберігається можливість довести цілісність і походження доказового об'єкта та відтворити процедуру його одержання. По-четверте, у доказовій стратегії слід враховувати, що воєнний час підсилює роль інсайдерських моделей і організаційного прикриття шпигунської активності, а отже зростає значення темпоральних кореляцій, версійності та журналів доступу як інструментів викриття приховування, за умови, що ці артефакти своєчасно законсервовані та збережені у процесуально придатній формі. Сукупно це означає, що в умовах війни якість документування шпигунства в ОПК визначається здатністю поєднати оперативність реагування з процесуальною дисципліною, забезпечивши відтворюваний перехід від виявлених ознак посягання до стійкого доказового контуру, придатного для судової перевірки (Кожушко, 2021; Погорецький, 2023; Федорчук, 2023; Погорецький, 2025; Сергєєва, 2025).

Висновки. Ефективність протидії шпигунству на підприємствах оборонно-промислового комплексу України визначається не лише результативністю оперативного пошуку та своєчасністю встановлення ознак посягання, а насамперед процесуальною придатністю отриманої інформації для цілей кримінального провадження і судового розгляду. У цій категорії справ вирішальним є перехід від виявлених фактичних даних до доказового масиву, здатного витримати перевірку належності, допустимості, перевірності та відтворюваності, що забезпечується належною фіксацією, коректною легалізацією результатів, безперервним ланцюгом збереження доказів і ризик-орієнтованим судовим контролем допустимості. В умовах цифровізації виробничо-управлінського середовища ОПК і воєнних ризиків втрати або спотворення слідів саме відтворюваність процедур здобуття та закріплення інформації стає ключовим критерієм доказової стійкості: судово значущим є не тільки зміст отриманих даних, а й можливість об'єктивно встановити їх походження,

цілісність і контрольованість шляху від джерела до дослідження в суді.

Авторське визначення оперативно-розшукового документування шпигунства в ОПК доцільно сформулювати як діяльнісний комплекс взаємопов'язаних дій і рішень уповноважених суб'єктів, спрямований на пізнання події шпигунства, виявлення та фіксацію фактичних даних про спосіб посягання, його стадії, причетних осіб і предмет інтересу, достовірне відбиття порядку одержання цих даних у матеріальних і цифрових носіях, збереження їх цілісності та створення процесуальної перспективи для подальшого використання у кримінальному провадженні шляхом належної легалізації й перевірки у формах, придатних для судового контролю та змагального дослідження.

Запропонована операційна матриця документування, яка пов'язує індикатор способу посягання з джерелами відомостей, тактичними діями, процесуальною фіксацією та контрольними переліками питань для сторони обвинувачення і судового контролю, забезпечує відтворюваний перехід від версій до керованих процедур збирання й закріплення доказової інформації. Вона дозволяє уникати фрагментарності доказового масиву, синхронізувати першочергові дії та мінімізувати втрати слідів у найуразливішій початковій фазі. «Паспорт доказу» виступає інструментом стандартизації пакування цифрових і змішаних доказових об'єктів, уніфікуючи подання їх походження, параметрів середовища, процедур консервації, контролю незмінності та обігу об'єкта в межах безперервного ланцюга збереження, що підвищує судову придатність і знижує ризики сумнівів щодо допустимості.

Перспективними напрямами подальших досліджень є поглиблення процесуальних стандартів роботи з цифровими доказами у справах про злочини проти основ національної безпеки, формалізація мінімальних вимог до безперервного ланцюга збереження для різних типів цифрових артефактів та змішаних масивів, а також уточнення меж і критеріїв допустимого втручання під судовим контролем з урахуванням принципів необхідності, пропорційності та мінімізації даних. Окремого розвитку потребують методики адаптації стандартів «першої доби» до воєнних умов функціонування ОПК, коли нестабільність середовища підвищує доказові ризики, а тому вимагає ще більшої дисципліни відтворюваності, контрольованості та процесуальної передбачуваності процедур документування.

Подяки

Немає

Конфлікт інтересів

Немає

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

Бишевець О. В., Погорецький М. А., Сергєєва Д. Б. та ін. *Криміналістична тактика*: навч. посіб. / за ред. М. А. Погорецького, Д. Б. Сергєєвої. 2-ге вид., переробл. та доп. Київ: Алерта, 2017. 244 с. URL: https://fpk.in.ua/images/biblioteka/4bac_pravo/Kryminalistyka-Navchalnyy-posibnyk-taktyka-2017–1.pdf

Бишевець О. В., Погорецький М. А., Сергєєва Д. Б. та ін. *Розслідування окремих видів злочинів*: навч. посіб. / за ред. М. А. Погорецького та Д. Б. Сергєєвої. Київ: Алерта, 2015. 536 с. URL: https://alerta.kiev.ua/pravo/463-rozsliduvannya-okremikh-vidiv-zlochiniv.html

Боднар В. Є. Оперативно-розшукова характеристика злочинів у сфері службової діяльності, що вчиняють працівники ОВС. *Південноукраїнський правничий часопис*. 2014. № 3. С. 183–186.

Кожушко С. О. *Кримінологічні засади протидії злочинності в оборонно-промисловому комплексі України*: дис. … доктора філософії за спеціальністю 081 «Право». Харків, 2021. 240 с.

Погорецький М. А. Використання інформації, одержаної від негласних джерел, для отримання доказів у кримінальному процесі зарубіжних країн. *Вісник Ун-ту внутр. справ*. 2003. Вип. 22. С. 131–138. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2003_22_29

Погорецький М. А. *Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі*: монографія. Харків: Арсіс ЛТД, 2007. 576 с. URL: https://library.nlu.edu.ua/POLN_TEXT/UP/POGORECKIY_2007.pdf

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

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

Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*: наук. – практ. журнал. Київ: НАСБУ, 2009. № 2 (2). С. 77–81. URL: https://ir.library.knu.ua/handle/15071834/8415

Погорецький М. А. Категоріальний апарат оперативно-розшукового документування. *Наука – 2009: теоретичні і прикладні дослідження*: матеріали Міжнар. наук. – практ. конф. (м. Черкаси, 23–24 квіт. 2009 р.). Черкаси: СУЕМ, 2009. С. 112–113.

Погорецький М. А. Поняття та сутність легалізації оперативно-розшукової інформації. *Вісник Луганського держ. ун-ту внутр. справ ім. Е. О. Дідоренка*. Луганськ: Вид-во ЛДУВС, 2010. Спец. вип. № 4. С. 26–40.

Погорецький М. А. Документ в оперативно-розшуковій діяльності. *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)*. С. 223–225.

Погорецький М. А., Шелеменцев В. П. Поняття організації оперативно-розшукової діяльності. *Кримський юрид. вісник*. Сімферополь, 2010. Вип. 1 (8). Ч. І. С. 18–28.

Погорецький М. А., Шеломенцев В. П. Поняття оперативно-розшукової характеристики злочинів. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*: зб. наук. праць. Дніпропетровськ: Дніпр. держ. ун-т внутр. справ, 2010. Вип. № 1. С. 192–201.

Погорецький М., Шеломенцев В. 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)*. С. 1042–1043.

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

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

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 наук. – практ. конф. (м. Дніпропетровськ, 18–19 квітня 2013 року). Київ: Хлі-Тек Прес, 2013. С. 186–193.

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

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

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

Погорецький М. А. Застосування провокації в ході негласних розслідувань: питання правомірності. *Вісник кримінального судочинства*. 2016. № 1. С. 33–43. URL: https://vkslaw.com.ua/index.php/journal/article/view/525/479

Погорецький М. А. Сучасні концепції кримінального процесуального доказування. *Сучасні тенденції розвитку криміналістики та кримінального процесу*. Харків, 2017. С. 309–312. URL: https://univd.edu.ua/general/publishing/konf/08_11_2017/pdf/146.pdf

Погорецький М. А., Сергєєва Д. Б. Розслідування шпигунства. У кн.: *Кваліфікація та розслідування окремих видів злочинів проти основ національної безпеки та воєнних злочинів*: навч. посіб. / О. Ф. Бантишев, Гора, В. В. Малюк, М. А. Погорецький та ін.; за заг. ред. В. А. Колесника. Київ: 7БЦ, 2022. 356 с.

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

Погорецький М. А., Сергєєва Д. Б., Топорецька З. М., Черняк А. М. та ін. *Розслідування кримінальних правопорушень у сфері службової діяльності*: навч. посіб. / за ред. проф. М. А. Погорецького. Київ: Алерта, 2025. 376 с. URL: https://alerta.kiev.ua/img/cms/PDF/Pogoreckiy_Roslyd_krim_pravopor_Zmist.pdf

Погорецький М. А. Захисник – суб'єкт доказування на досудовому провадженні за чинним КПК України: проблемні питання. *Актуальні питання державотворення в Україні*: матеріали міжнародної науково-практичної конференції (м. Київ, 23 травня 2014 р.). Київ: Прінт-Сервіс, 2014. С. 480–482

Погорецький М. А., Сергєєва Д. Б. Тактика захисника: поняття, зміст та місце в системі криміналістичної тактики. *Вісник кримінального судочинства*. 2016. № 2. С. 113–123. URL: https://vkslaw.knu.ua/images/verstka/2_2016_Sergeeva.pdf

Погорецький М. А., Старенький О. С. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України*. 2018. № 8. С. 85–106. URL: http://nbuv.gov.ua/UJRN/prukr_2018_8_9

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. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42–2.pdf

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. URL: https://app-journal.in.ua/wp-content/uploads/2025/10/APP_05_2025_part-3–2.pdf

Погорецький М. А. Новели Кримінального процесуального кодексу України в період воєнного стану: проблемні питання. *Право і суспільство*. 2025. № 3, т. 2. С. 248–262. DOI: https://doi.org/10.32842/2078–3736/2025.3.2.35.

Сайипов Р. Ч., Томма Р. П. Оперативно-розшукова характеристика кримінальних правопорушень, що вчиняються в оборонно-промисловому комплексі України. *Аналітично-порівняльне правознавство*: електронне наукове видання. 2025. Вип. № 04, ч. 3. С. 295–301. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/44–2.pdf

Сергєєва Д. Б. Виявлення і документування способів учинення службових правопорушень: методика, тактика, цифрові сліди та ланцюг збереження доказів. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2025. Вип. 91: ч. 4. С. 438–451. DOI: 10.24144/2307–3322.2025.91.4.60. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/62–1.pdf

Тіщенко В. В. *Теоретичні і практичні основи методики розслідування злочинів*: монографія. Одеса: Фенікс, 2007. 260 с.

Федорчук Я. І. Кримінально-правова характеристика кримінальних правопорушень, що вчиняються в оборонно-промисловому комплексі України. *Науковий вісник публічного та приватного права*. 2023. Вип. 6. С. 131–135.

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.

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. Блажівський, Є. П. Бурдоль та ін.; за заг. ред. В. Я. Тація та ін. Харків: Право, 2012. С. 247–308. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20794.

REFERENCES

Byshevets, O. V., Pohoretskyi, M. A., Serhieieva, D. B., et al. (2017). Forensic tactics: Textbook (2nd ed., revised and expanded) (M. A. Pohoretskyi & D. B. Serhieieva, Eds.). Kyiv: Alerta. 244 p. URL: https://fpk.in.ua/images/biblioteka/4bac_pravo/Kryminalistyka-Navchalnyy-posibnyk-taktyka-2017–1.pdf

Byshevets, O. V., Pohoretskyi, M. A., Serhieieva, D. B., et al. (2015). Investigation of certain types of crimes: Textbook (M. A. Pohoretskyi & D. B. Serhieieva, Eds.). Kyiv: Alerta. 536 p. URL: https://alerta.kiev.ua/pravo/463-rozsliduvannya-okremikh-vidiv-zlochiniv.html

Bodnar, V. Ye. (2014). Operational-search characteristics of crimes in the sphere of official activity committed by employees of internal affairs bodies. *South Ukrainian Law Journal*, No. 3, 183–186.

Kozhushko, S. O. (2021). Criminological foundations of combating crime in Ukraine's defence-industrial complex (PhD dissertation, specialty 081 «Law»). Kharkiv. 240 p.

Pohoretskyi, M. A. (2003). Using information obtained from covert sources to obtain evidence in the criminal process of foreign countries. *Bulletin of the University of Internal Affairs*, Issue 22, 131–138. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2003_22_29

Pohoretskyi, M. A. (2007). Functional purpose of operational-search activity in criminal proceedings: Monograph. Kharkiv: Arsis LTD. 576 p. URL: https://library.nlu.edu.ua/POLN_TEXT/UP/POGORECKIY_2007.pdf

Pohoretskyi, M. A. (2007). Operational-search measures: Issues of legal regulation. *Combating Organized Crime and Corruption (Theory and Practice)*, No. 14, 135–145.

Pohoretskyi, M. A. (2009). On the correlation between sources of factual data and sources of evidence in criminal proceedings. *Law of Ukraine*, No. 1, 80–85.

Pohoretskyi, M. A., & Shelomentsev, V. P. (2009). The concept of cyberspace as an environment for committing crime. *Information Security of the Individual, Society and the State*, 2(2), 77–81. URL: https://ir.library.knu.ua/handle/15071834/8415

Pohoretskyi, M. A. (2009). Categorical framework of operational-search documentation. In Science 2009: Theoretical and applied research: Proceedings of the International Scientific and Practical Conference (Cherkasy, April 23–24, 2009) (pp. 112–113). Cherkasy: SUEM.

Pohoretskyi, M. A. (2010). The concept and essence of legalization of operational-search information. *Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko*, Special Issue No. 4, 26–40.

Pohoretskyi, M. A. (2010). Document in operational-search activity. In V. V. Kovalenko, Ye. V. Moiseiev, V. Ya. Tatsii, & Yu. S. Shemshuchenko (Eds.), International Police Encyclopedia (in 10 vols.) (Vol. VI: Operational-search activity of the police (militia), pp. 223–225). Kyiv: Atika.

Pohoretskyi, M. A., & Shelemen(t)sev, V. P. (2010). The concept of organization of operational-search activity. *Crimean Legal Bulletin*, Issue 1(8), Part I, 18–28.

Pohoretskyi, M. A., & Shelomentsev, V. P. (2010). The concept of operational-search characteristics of crimes. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs*, Issue 1, 192–201.

Pohoretskyi, M., & Shelomentsev, V. (2010). Fixation of factual data about crimes. In V. V. Kovalenko, Ye. V. Moiseiev, V. Ya. Tatsii, & Yu. S. Shemshuchenko (Eds.), International Police Encyclopedia (in 10 vols.) (Vol. VI: Operational-search activity of the police (militia), pp. 1042–1043). Kyiv: Atika.

Pohoretskyi, M. A. (2011). Evidence in criminal proceedings: Problematic issues. *Journal of the National University of Ostroh Academy. Series: Law*, No. 1(3). URL: https://lj.oa.edu.ua/articles/2011/n1/11pmappp.pdf

Pohoretskyi, M. A., & Serhieieva, D. B. (2012). Forensic tactics: On defining the concept. *Journal of the National University of Ostroh Academy. Series: Law*, No. 1(5). URL: https://lj.oa.edu.ua/articles/2012/n1/12pmasvp.pdf

Pohoretskyi, M. A. (2013). Conducting covert investigative (search) actions and using their results in proving. In Current issues of pre-trial investigation by investigative bodies of internal affairs: Problems of theory and practice: Proceedings of the All-Ukrainian Scientific and Practical Conference (Dnipropetrovsk, April 18–19, 2013) (pp. 186–193). Kyiv: Khli-Tek Press.

Pohoretskyi, M. A., & Serhieieva, D. B. (2014). Covert investigative (search) actions and operational-search measures: Concept, essence and correlation. *Combating Organized Crime and Corruption (Theory and Practice)*, No. 2(33), 137–141. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_34

Pohoretskyi, M. A. (2015). Commencement of pre-trial investigation: Certain problematic issues. *Bulletin of Criminal Proceedings*, No. 1, 93–103. URL: https://vkslaw.com.ua/index.php/journal/article/download/431/400

Pohoretskyi, M. A. (2015). A new concept of criminal procedural proving. *Bulletin of Criminal Proceedings of Ukraine*, No. 3, 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf

Pohoretskyi, M. A. (2016). Use of provocation during covert investigations: Issues of lawfulness. *Bulletin of Criminal Proceedings*, No. 1, 33–43. URL: https://vkslaw.com.ua/index.php/journal/article/view/525/479

Pohoretskyi, M. A. (2017). Modern concepts of criminal procedural proving. In Contemporary trends in the development of criminalistics and criminal procedure (pp. 309–312). Kharkiv. URL: https://univd.edu.ua/general/publishing/konf/08_11_2017/pdf/146.pdf

Pohoretskyi, M. A., & Serhieieva, D. B. (2022). Investigation of espionage. In O. F. Bantyshev, Hora, V. V. Maliuk, M. A. Pohoretskyi, et al., Qualification and investigation of certain types of crimes against the foundations of national security and war crimes: Textbook (V. A. Kolesnyk, Ed.). Kyiv: 7BC. 356 p.

Pohoretskyi, M. A. (2023). Application of latest technologies in the investigation and proving of war crimes (problematic issues). *Bulletin of Criminal Proceedings*, No. 3–4, 84–102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3–4_23_v2_250425_avt2–84–102.pdf

Pohoretskyi, M. A., Serhieieva, D. B., Toporetska, Z. M., Cherniak, A. M., et al. (2025). Investigation of criminal offenses in the sphere of official activity: Textbook (M. A. Pohoretskyi, Ed.). Kyiv: Alerta. 376 p. URL: https://alerta.kiev.ua/img/cms/PDF/Pogoreckiy_Roslyd_krim_pravopor_Zmist.pdf

Pohoretskyi, M. A. (2014). Defense counsel as a subject of proof at the pre-trial stage under the current CPC of Ukraine: Problematic issues. In Current issues of state-building in Ukraine: Proceedings of the International Scientific and Practical Conference (Kyiv, May 23, 2014) (pp. 480–482). Kyiv: Print-Service.

Pohoretskyi, M. A., & Serhieieva, D. B. (2016). Defense counsel's tactics: Concept, content and place in the system of forensic tactics. *Bulletin of Criminal Proceedings*, No. 2, 113–123. URL: https://vkslaw.knu.ua/images/verstka/2_2016_Sergeeva.pdf

Pohoretskyi, M. A., & Starenkyi, O. S. (2018). Covert investigative (search) actions as means of obtaining evidence: Certain problematic issues. *Law of Ukraine*, No. 8, 85–106. URL: http://nbuv.gov.ua/UJRN/prukr_2018_8_9

Pohoretskyi, M. A. (2025). Judicial control in ensuring fair and admissible proof in Ukraine's criminal proceedings. *Analytical and Comparative Jurisprudence*, No. 4, Part 3, 269–279. DOI: https://doi.org/10.24144/2788–6018.2025.04.3.40 URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42–2.pdf

Pohoretskyi, M. A. (2025). Digital technologies and evidence in the investigation of crimes against the foundations of Ukraine's national security: Procedural problems and European standards. *Analytical and Comparative Jurisprudence*, No. 5, Part 3, 239–256. DOI: https://doi.org/10.24144/2788–6018.2025.05.3.37 URL: https://app-journal.in.ua/wp-content/uploads/2025/10/APP_05_2025_part-3–2.pdf

Pohoretskyi, M. A. (2025). Amendments to the Criminal Procedure Code of Ukraine during martial law: Problematic issues. *Law and Society*, No. 3, Vol. 2, 248–262. DOI: https://doi.org/10.32842/2078–3736/2025.3.2.35

Saiipov, R. Ch., & Tomma, R. P. (2025). Operational-search characteristics of criminal offenses committed in Ukraine's defence-industrial complex. *Analytical and Comparative Jurisprudence* (electronic scientific edition), Issue No. 04, Part 3, 295–301. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/44–2.pdf

Serhieieva, D. B. (2025). Detection and documentation of methods of committing official offenses: Methodology, tactics, digital traces and chain of custody. *Scientific Bulletin of Uzhhorod National University. Series: Law*, Issue 91, Part 4, 438–451. DOI: 10.24144/2307–3322.2025.91.4.60 URL: https://visnyk-jurisuzhnu.com/wp-content/uploads/2025/11/62–1.pdf

Tishchenko, V. V. (2007). Theoretical and practical foundations of the methodology for investigating crimes: Monograph. Odesa: Feniks. 260 p.

Fedorchuk, Ya. I. (2023). Criminal-law characteristics of criminal offenses committed in Ukraine's defence-industrial complex. *Scientific Bulletin of Public and Private Law*, Issue 6, 131–135.

Shumylo, M. Ye., & Pohoretskyi, M. A. (2001). Problems of using operational-search materials in proving in criminal cases: Theoretical and practical aspects. *Bulletin of the Luhansk Institute of Internal Affairs*, Issue 3, 199–209.

Shumylo, M. Ye., & Pohoretskyi, M. A. (2012). Evidence and proof. In O. M. Bandurka, Ye. M. Blazhivskyi, Ye. P. Burdol, et al., Criminal Procedure Code of Ukraine: Scientific and practical commentary (in 2 vols., Vol. 1, pp. 247–308) (V. Ya. Tatsii et al., Eds.). Kharkiv: Pravo. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/20794

UDC343.98:343.326:343.13.

Yermak Vasyl Volodymyrovych –
degree-seeking researcher, Scientific and Organizational Center,
National Academy of the Security Service of Ukraine,
Kharkiv, Ukraine
https://orcid.org/0009-0008-3217-7851
jockerukra@gmail.com

Detection and documentation of espionage at enterprises of Ukraine's defence-industrial complex

The article provides a comprehensive analysis of the detection and documentation of espionage at enterprises of Ukraine's defence-industrial complex (DIC) as a continuous process in which the initial identification of indicators of an encroachment must be immediately projected onto the procedural perspective of the information obtained. The aim is to substantiate an evidence-oriented model of operational search and operational-search documentation, taking into account the predominance of digital traces, the security-regime sensitivity of the DIC environment, and heightened standards of judicial scrutiny of admissibility. The methodological basis comprises normative and formal-logical approaches, forensic modelling of the modus operandi (preparation–execution–

concealment), as well as a risk-oriented analysis of «nodes» of evidence loss within digital and mixed evidentiary sets.

It is shown that the effectiveness of counteraction is determined not so much by the volume of information obtained as by its reproducibility, traceable provenance, capacity for independent verification, and integration into an adversarial procedure. A refinement of the conceptual framework (factual data, operational-search information, materials of operational-search activity (OSA), OSA documents) is proposed, and typical procedural defects in their conflation are identified, which generate gaps in reconstructing data provenance and increase the risks of inadmissibility. Scientific novelty lies in substantiating an operational matrix for the transition from factual data to procedural sources of evidence and in proposing an «evidence passport» as a standardized instrument for documenting the trajectory of an evidentiary object, key environmental parameters, access logging, and integrity assurance procedures.

It is proven that in espionage cases within the DIC, judicial control performs not only a safeguard function but also an evidence-forming one: it must verify the proportionality of interferences, the boundaries of access to digital contours, the correctness of procedural integration of OSA and covert investigative (search) actions (CISA) results, and the reproducibility of procedures. The practical significance of the findings consists in formulating recommendations aimed at minimizing procedural losses in court under martial law, when the risks of infrastructure degradation, abnormal access regimes, and rapid loss of digital artefacts increase.

Keywords: *espionage; defence-industrial complex; operational search; operational-search documentation; legalization of OSA materials; CISA; digital evidence; chain of custody; evidence passport; judicial control; admissibility of evidence; martial law.*