УДК: 343.98:343.9-051:004.056.5
DOI https://doi.org/10.24144/2788-6018.2025.05.3.40

ВИЯВЛЕННЯ І ДОКУМЕНТУВАННЯ СПОСОБІВ УЧИНЕННЯ СЛУЖБОВИХ ПРАВОПОРУШЕНЬ: МЕТОДИКА, ТАКТИКА, ЦИФРОВІ СЛІДИ ТА ЛАНЦЮГ ЗБЕРЕЖЕННЯ ДОКАЗІВ

Сергєєва Д.Б.,
доктор юридичних наук, професор,
Заслужений юрист України,
головний науковий співробітник
Національної академії Служби безпеки України
ORCID: 0000-0003-1005-7046
e-mail: Dianaserhieievaknu@gmail.com

Сергєєва Д.Б. Виявлення і документування способів учинення службових правопорушень: методика, тактика, цифрові сліди та ланцюг збереження доказів.

Вказується, службові правопорушення характеризуються високою латентністю, інституційною «вбудованістю» в управлінські процедури та здатністю швидко адаптуватися до змін нормативного середовища. У статті запропоновано цілісну криміналістично-процесуальну модель виявлення й документування способів учинення службових правопорушень у сучасному цифровому середовищі. На підставі систематизації форм використання/спотворення владних повноважень (зловживання, перевищення, умисна бездіяльність, одержання неправомірної вигоди) і типових «технологій злочинної діяльності» (розкрадання через безтоварні операції та «прокладки», заволодіння майном шляхом обману, маскування вигоди під консалтинг/гранти/благодійність, маніпуляції в EDMS/ERP/реєстрах) автор формує операційну матрицю «ознака способу → джерела відомостей → тактичні дії → процесуальна фіксація → контрольні переліки питань». Показано, як ця матриця забезпечує перехід від реконструкції механізму події до практичних алгоритмів: синхронних тимчасових доступів, оглядів електронних систем, інвентаризацій, побудови графів платіжних ланцюгів і верифікації ринкової еквівалентності. Особливу увагу приділено роботі з цифровими слідами (метадані, історії версій, журнали доступів/погоджень, резервні копії, листування) та підтриманню безперервного ланцюга збереження доказів (read-only копіювання, хешування, опис середовища, журнал доступів і переміщень). Обґрунтовано ризик-орієнтований формат судового контролю і стандартизовані контрольні переліки для слідчого, прокурора й слідчого судді, які забезпечують необхідність і пропорційність втручань та відтворюваність процедур. Окремо розкрито інтеграцію матеріалів оперативно-розшукової діяльності та негласних слідчих (розшукових) дій у доказовий контур через «маршрутизацію за ознакою способу» з мінімізацією даних і належною процесуальною «вшивкою». Наукова новизна полягає у поєднанні криміналістичної типології способів з цифровою форензікою та процесуальною доктриною допустимості/відтворюваності, а практична значущість – у стандартизації «першої доби» розслідування, запровадженні «паспортів доказів» і єдиних операційних алгоритмів для підвищення стійкості доказів у суді.

Ключові слова: службові правопорушення; спосіб учинення; технології злочинної діяльності; цифрові сліди; електронний документообіг (EDMS/ERP); ланцюг збереження доказів; належність; допустимість; відтворюваність; предмет доказування; оперативно-розшукова діяльність (ОРД); негласні слідчі (розшукові) дії (НСРД); судовий контроль; операційна матриця.

Serhieieva, D.B. Detection and documentation of modes of commission of service-related offences: methodology, tactics, digital traces, and the chain of custody.

It is indicated that official misconduct is characterized by high latency, institutional «embeddedness» in management procedures, and the ability to quickly adapt to changes in the regulatory environment. The article proposes an integrated forensic–procedural model for detecting and documenting modes of commission of service-related offences in a contemporary digital environment. Building on the systematization of forms of using or distorting official powers (abuse, excess of authority, intentional non-performance, bribery/undue advantage) and on typical "criminal technologies" (embezzlement through sham or intermediary contracts, deception-based appropriation, masking undue benefits as consulting/grants/charity, manipulations in EDMS/ERP/registries), the author develops an operational matrix "mode indicator → sources of information → tactical actions → procedural recording → standardized checklists." The matrix enables a reproducible transition from reconstructing the mechanism of the

event to practical algorithms: synchronized temporary accesses, examinations of electronic systems, inventories, graphing of payment chains, and verification of market equivalence. Special attention is paid to handling digital traces (metadata, version histories, access/approval logs, backups, correspondence) and maintaining an unbroken chain of custody (read-only imaging, hashing, environment description, access and transfer logs). A risk-based format of judicial control and standardized checklists for investigators, prosecutors, and investigating judges is substantiated to ensure necessity, proportionality, and procedural reproducibility. The paper also details how materials from operational-search activity and covert investigative actions are integrated into the evidentiary framework via "routing by mode indicator," with data minimization and proper procedural incorporation. The novelty lies in coupling a criminological typology of modes with digital forensics and the procedural doctrine of admissibility/reproducibility; the practical value is the standardization of the "first-day" response, introduction of "evidence passports," and unified operational algorithms that increase evidentiary resilience in court.

Key words: service-related offences; mode of commission; criminal technologies; digital traces; electronic document management (EDMS/ERP); chain of custody; relevance; admissibility; reproducibility; subject of proof; operational-search activity; covert investigative actions; judicial control; operational matrix.

Постановка проблеми. Службові правопорушення характеризуються високою латентністю, інституційною «вбудованістю» в управлінські процедури та здатністю швидко адаптуватися до змін нормативного середовища. Їхній спосіб учинення охоплює не лише реалізацію протиправних дій, а й ретельну підготовку та заздалегідь сконструйовані механізми приховування, що спираються на організаційні регламенти, електронний документообіг і формальні атрибути «службового» рішення [1; 16; 18; 19]. В умовах цифровізації слідчий працює з багатошаровими доказовими масивами – версійністю документів, журналами погоджень і доступів, метаданими файлів, логами корпоративних систем, резервними копіями, слідами комунікацій; кожний такий артефакт потребує негайної консервації, процесуально коректного вилучення та безперервного ланцюга збереження доказів для забезпечення відтворюваності й судової придатності [1; 3; 5; 9; 18].

Класична криміналістична доктрина визнає спосіб учинення ключовим елементом характеристики злочину, однак для службових правопорушень цього недостатньо: потрібна процесуальна операціоналізація типології способів у вигляді версійних модулів, першочергових дій, стандартизованих контрольних переліків питань для слідчого, прокурора та слідчого судді, а також уніфікованих алгоритмів роботи з цифровими слідами (ідентифікація джерел, консервація, хешування, протоколювання, перевірка цілісності) [1; 3; 16; 18]. Відсутність такої операціоналізації породжує розрив між встановленими «на папері» обставинами та реальними електронними артефактами: формально виявлені документи не підтверджуються технічними метаданими, ланцюг збереження має прогалини, а «офіційні легенди» не проходять перевірку часовими мітками, маршрутами погоджень чи економічною доцільністю рішень [5; 9; 18].

Проблема ускладнюється тим, що службові правопорушення часто реалізуються як «злочинні технології» – комплексні моделі поведінки з мультиделіктним переплетенням (службове підроблення як модуль способу та спосіб приховування; одержання неправомірної вигоди; зловживання впливом; фальсифікація звітності; удавані правочини; економіко-правові схеми легалізації, у т. ч. на суміжних ринках) [12; 14; 15; 17; 20–22]. Без чіткого розмежування стадій підготовка → реалізація → приховування та без картографування цифрових слідів на кожній із них зростають ризики часткової втрати доказів і визнання їх недопустимими [1; 5; 18–19]. Водночас судовий контроль і стандарти мотивування рішень у сфері допустимості вимагають не лише формальної коректності слідчих дій, а й демонстрації відтворюваності, перевірності та цілісності доказового ланцюга від джерела до представлення в суді [3; 6–7; 9; 11].

Отже, науково-практична проблема полягає у створенні цілісної моделі, яка поєднає криміналістичну типологію способів учинення службових правопорушень із процесуально придатними інструментами їх виявлення, документування й доказування у цифровому середовищі: від побудови версій і визначення предмета доказування до алгоритмів першочергових дій, управління цифровими слідами та підтримання безперервного ланцюга збереження доказів [1; 3; 5; 9; 16; 18].

Аналіз останніх досліджень і публікацій. Дослідження способів учинення службових правопорушень і їх доказового забезпечення формується на перетині класичної криміналістики, спеціальних праць про службову злочинність, антикорупційної та фінансово-моніторингової літератури, а також сучасної процесуальної доктрини доказування й цифрових слідів. Базу методології становлять узагальнення з криміналістичної тактики та структури розслідування – версійність, планування слідчих (розшукових) дій, поетапність «підготовка → реалізація → приховування» і типові тактичні рішення, викладені у навчальних виданнях і прикладних посібниках [1; 18; 19]. Вони

задають каркас для подальшої операціоналізації способів у службових справах: побудови «технологій злочинної діяльності», визначення першочергових дій і моделювання предмета доказування.

Спеціальні дослідження службової злочинності рухаються кількома комплементарними векторами. По-перше, типологізація способів та форм використання/спотворення повноважень у посадових правопорушеннях (зловживання, перевищення, умисна бездіяльність, одержання неправомірної вигоди) на матеріалі окремих складів і практичних ситуацій [16; 17]. По-друге, фокус на доведенні корупційних діянь – насамперед, прийняття пропозиції, обіцянки або одержання неправомірної вигоди – із фіксацією типових помилок сторони обвинувачення та алгоритмів збирання/перевірки доказів, релевантних нашій операційній матриці [14; 23]. По-третє, нові комплексні посібники щодо розслідування правопорушень у сфері службової діяльності консолідують попередні підходи у практикоорієнтованих схемах, але потребують глибшої інтеграції з цифровою форензікою та стандартизованими переліками питань для судового контролю [18].

Окремою лінією розвивається антикорупційний і фінансово-моніторинговий напрям, що показує реалізацію значної частини службових правопорушень як економіко-правових «технологій» – через документальну фальсифікацію, удавані правочини та схеми легалізації, у т. ч. на «гральному» та суміжних ринках [15; 20; 21; 22]. Ці праці формують набір індикаторів способу (ланцюги платежів, посередники, «офіційні обгортки» виплат) для матриці «ознака способу → джерела → тактика → фіксація», але потребують чіткішого перекладу в процесуальні алгоритми консервації цифрових слідів і підтримання ланцюга збереження доказів.

Процесуальну рамку вибудовує доктрина доказування. Ранні праці М. Погорецького окреслили проблематику теорії кримінального процесуального доказування з акцентом на належності, допустимості та, особливо, відтворюваності й перевірності доказової інформації [4]. «Нова концепція» розвинула вимір процесуальної форми та стандартів мотивування й судового контролю – це безпосередньо релевантно для перевірки «офіційних легенд» у службових справах і для оцінки цифрових артефактів [7]. Роботи про початок досудового розслідування підсилили увагу до ризиків втрати доказів на ранній фазі та необхідності тактичної синхронізації дій – методологічна основа модулів «першочергові дії» і «точки незворотності» [8]. Сучасні дослідження судового контролю деталізують критерії необхідності, пропорційності та допустимості, що важливо для формування стандартизованих контрольних переліків питань у нашій моделі [9]. Новітні публікації про розслідування воєнних злочинів і цифрові дані додають форензійні стандарти: хешування, журналювання доступів, відтворюваність процедур фіксації та представлення цифрових слідів у суді – підходи, які методично переносні в площину службових правопорушень [5]. Сукупно ця лінія робіт забезпечує теоретико-процесуальне підґрунтя для інтеграції криміналістичної типології способів із цифровою форензікою і ланцюгом збереження доказів [4; 5; 7–9].

У площині оперативно-розшукових та негласних слідчих (розшукових) дій ключовим є питання співвідношення НСРД і ОРЗ та їх доказового потенціалу в справах про службові правопорушення [11]. Це надає критерії коректного включення результатів таких заходів до загального доказового масиву з урахуванням судового контролю за втручаннями у приватність та вимог допустимості [3; 11]. Додатково рання праця щодо способів у кредитно-банківській сфері продемонструвала, як «банківські» технології стають матрицею для інших службових діянь і як вибудовується логіка їх виявлення та документування – принципи, що екстраполюються на наш об'єкт дослідження [12].

Нарешті, законодавча база (КК, КПК) встановлює формальні межі допустимості, підстави та процедури одержання доказів і інструменти судового контролю [2; 3]. Однак саме доктрина і прикладні посібники «перекладають» ці рамки у практичні алгоритми – від структурування предмета доказування до перевірки причинно-наслідкових зв'язків між управлінськими рішеннями та вигодами, відбитими в документах і цифрових логах [1; 18; 19].

Отже, наявний масив літератури забезпечує: (а) методологію криміналістичної реконструкції способу [1; 18; 19]; (б) типології службових правопорушень і індикатори «злочинних технологій» [16; 17]; (в) антикорупційно-фінансовий контекст і канали легалізації як елементи способу [15; 20–22]; (г) процесуальну рамку доказування та судового контролю, включно з цифровими слідами [4; 5; 7–9]; (д) співвідношення НСРД/ОРЗ та їх доказову релевантність [11]. Водночас наявна прогалина – відсутність уніфікованої *операційної матриці* для службових правопорушень, що поєднувала б типологію способів із алгоритмами ідентифікації, консервації, хешування, протоколювання і представлення цифрових артефактів у межах безперервного *ланцюга збереження доказів*, а також стандартизованими переліками питань для слідчого, прокурора, слідчого судді й захисника [1; 5; 7–9; 18]. Запропонована в цій статті модель покликана закрити цю прогалину.

Метою статті є розроблення криміналістично й процесуально узгодженої моделі виявлення та документування способів учинення службових правопорушень, що інтегрує типологію способів із цифровою форензікою та безперервним ланцюгом збереження доказів; створення операційної

матриці «ознака способу → джерела відомостей → тактичні дії → процесуальна фіксація → стандартизовані контрольні переліки питань»; а також формулювання практичних рекомендацій щодо першочергових дій, визначення предмета доказування, перевірки «офіційних легенд» і забезпечення належності, допустимості та відтворюваності цифрових слідів під судовим контролем.

Виклад основного матеріалу. У службових правопорушеннях *спосіб учинення* розуміємо як структуровану послідовність дій суб'єкта на стадіях *підготовка → реалізація → приховування,* що зумовлена поєднанням об'єктивних умов (регуляторне середовище, організаційні процеси, властивості предмета посягання) та суб'єктивних чинників (мотив, мета, знання, навички) [1; 18; 19]. Цей підхід спирається на класичну криміналістичну доктрину тактики й планування розслідування та оновлюється з урахуванням електронного документообігу, цифрових журналів і метаданих як носіїв слідів способу [1; 18].

Критичною рисою службових посягань є *вбудоване приховування* вже на підготовчій стадії: заздалегідь формуються посередницькі ланки, удавані правочини, «офіційні обгортки» виплат (консалтинг, гранти, подарунки), сценарії легалізації та канали «очищення» документів (версійність файлів, погодження «заднім числом», селективні витяги з реєстрів) [14; 15; 20–22]. У цьому сенсі спосіб постає як *керована технологія,* що може містити мультиделіктні компоненти: службове підроблення — одночасно елемент способу та засіб приховування; зловживання впливом – як канал монетизації повноважень; економіко-правові схеми легалізації – як «фаза виходу» неправомірної вигоди [14; 15; 20–22].

Процесуальне значення способу подвійне. По-перше, *версійне моделювання* способу задає каркас розслідування: коло причетних, маршрути документів/коштів, точки виникнення цифрових слідів, очікувані «вузли» для невідкладної консервації [1; 18]. По-друге, спосіб слугує «мостом» між криміналістикою та процесуальною формою: визначає *орієнтири предмета доказування* (мотив і вигода; повноваження та фактичний вплив; дії на кожній стадії; роль посередників; використані регуляторні прогалини) і конкретизує потребу в судовому контролі (необхідність/пропорційність втручань, межі доступу до даних, обґрунтування ризику втрати доказів) [3; 7; 9].

Цифровий вимір способу потребує дотримання стандартів *відтворюваності та цілісності* доказових артефактів: ідентифікація джерел (EDMS/ERP/CRM, поштові сервери, системи доступу), консервація стану систем, *read-only* копіювання, створення контрольних сум (хешів), повний опис середовища та часових налаштувань, ведення документації *ланцюга збереження доказів* від виявлення до судового дослідження [5; 7; 9]. Будь-який розрив цього ланцюга або невідповідність метаданих (розсинхронізація часових міток, відсутні журнали змін, невідоме походження копій) безпосередньо загрожує допустимості та переконливості доказів у межах вимог КПК [3; 5; 7; 9].

Важливим є і *операційний зв'язок* способу з інститутами ОРД та НСРД. Монографічні й статейні напрацювання показали, що результативність негласних заходів у службових справах істотно зростає, коли вони підпорядковані моделі способу (цілеспрямований добір тактичних комбінацій, синхронізація у «вікнах можливостей», мінімізація втручання) та одразу «вшиті» у процесуальний контур належності/допустимості [10; 11; 14]. Це вимагає чіткої маршрутизації: від *виявлення ознаки способу* → до *збору інформації відповідним інструментом* → до *процесуальної фіксації* із дотриманням ланцюга збереження і стандартів судового контролю [3; 7; 9–11; 14].

Насамкінець, історично вироблені криміналістичні підходи до способів у фінансово-банківській сфері (безтоварні операції, «прокладки», завищення вартості, підміна первинних документів) стали «матрицею» для сучасних службових технологій і демонструють, як саме ознаки способу транслюються у *практичні алгоритми* виявлення та документування [12; 18]. Запропонована далі операційна матриця покликана інституалізувати цей зв'язок у стандартизований інструментарій слідства й судового контролю.

Класифікація способів учинення службових правопорушень ґрунтується на поєднанні форм використання чи спотворення владних повноважень, статусних характеристик суб'єкта та галузево-інституційного контексту здійснення службових функцій. У вимірі форм владної поведінки домінують чотири базові моделі: зловживання повноваженнями (ухвалення управлінських рішень всупереч інтересам служби або з відступом від процедур), перевищення повноважень (вчинення дій поза межами компетенції, у тому числі з опорою на фальсифіковані документи), умисна службова бездіяльність (невжиття визначених законом заходів за наявності реальної можливості) та одержання неправомірної вигоди чи зловживання впливом як інструменти монетизації службового становища [17; 16; 14]. Статусна призма розмежовує службових осіб юридичних осіб публічного права та приватного права: у першому випадку спосіб тісно пов'язаний із регламентованими процедурами погодження, доступом до державних реєстрів і формалізованими ланцюгами ухвалення рішень, тоді як у приватному секторі вирішальним стає внутрішній комплаєнс та архітектура корпоративних систем обліку, що задають іншу природу цифрових слідів і точок контролю [16;

18]. Галузево-інституційний контекст уточнює профіль ризиків: державна цивільна служба, військова та правоохоронна служби, державні й муніципальні заклади, а також приватні комерційні та некомерційні структури демонструють різні «екосистеми» документообігу та аудиту, що безпосередньо впливає на вибір першочергових дій і предмет доказування [18]. У межах цієї рамки виокремлюються типові «технології злочинної діяльності» як стійкі комбінації дій і документальних схем. По-перше, технології розкрадань із використанням посади, що спираються на безтоварні операції, «прокладкові» контракти, завищення вартості та підміну первинної документації; такі моделі історично докладно описані на банківсько-фінансовому матеріалі й сьогодні відтворюються у службових кейсах із цифровими модифікаціями (версійність файлів, заднє погодження, маніпуляції в EDMS/ERP) [12; 18]. По-друге, технології заволодіння майном шляхом обману, включно з самовільним привласненням владних повноважень, використанням фальшивих реквізитів доступу до реєстрів і внесенням недостовірних відомостей, що створюють «правдоподібну» легальну оболонку протиправних рішень [17; 16]. По-третє, технології збагачення у сфері служби, де неправомірна вигода маскується під консультаційні чи маркетингові послуги, грантові чи благодійні виплати, «виграші» або інші офіційні виплати; у корупційно ємних секторах до ланцюгів додаються ринки грального бізнесу та суміжні посередницькі мережі, що забезпечують легалізацію коштів і розрив зв'язку між рішенням і бенефіціаром [14; 15; 20–22]. Спільним знаменником цих технологій є модуль службового підроблення, який функціонує і як елемент способу, і як засіб приховування, забезпечуючи синхронізацію фальсифікованих документів із реєстровими слідами та платіжними маршрутами [14; 16–17]. Класифікація не є самоціллю: її прикладна функція полягає в операціоналізації для версійного моделювання, визначення предмета доказування та побудови «карти» цифрових слідів. Для кожної з названих моделей спосіб задає очікувані джерела відомостей (первинка і метадані, журнали погоджень, логи доступів, банківські виписки, внутрішні політики), тактичні кроки їх виявлення й консервації (синхронні тимчасові доступи, огляди EDMS/ERP, інвентаризації, допити розпорядників даних) і форму процесуальної фіксації, придатної для перевірки допустимості під судовим контролем згідно з вимогами КПК і сучасної доктрини доказування щодо необхідності, пропорційності, відтворюваності та мотивованості рішень [3; 4; 7–9; 18]. У подальшому ця класифікаційна рамка трансформується в операційну матрицю, де кожна ознака способу пов'язується з конкретним джерелом, тактичною дією та процесуальною формою фіксації, а також зі стандартизованими переліками питань для слідчого, прокурора, слідчого судді та захисника, що уможливлює відтворювану й перевірювану роботу з цифровими і документальними артефактами [1; 18; 19].

Операційна матриця виявлення та документування способів учинення вибудовується як послідовний ланцюг «ознака способу → джерела відомостей → тактична дія → процесуальна фіксація → контрольні переліки питань» і виконує функцію практичного інтерфейсу між криміналістичною моделлю та процесуальною формою. На рівні «ознаки» фіксуються маркери способу: посередницькі ланцюги і нетипові платіжні маршрути, версійні конфлікти документів, «задні» погодження в електронних системах, використання регуляторних прогалин, а також «офіційні обгортки» неправомірної вигоди (консалтинг, гранти, подарунки, виграші), властиві корупційно ємним сегментам і суміжним ринкам [14; 15; 20–22]. Для кожної ознаки наперед визначаються релевантні джерела відомостей: первинні бухгалтерські документи та виписки, договори з додатками, електронні історії версій і журнали погоджень у EDMS/ERP, логи доступу до реєстрів, листування та календарі, журнали пропускних систем; тактичні дії синхронізуються в часі для запобігання «підчисткам» і включають одночасні тимчасові доступи, огляди електронних середовищ, інвентаризації матеріальних і цифрових активів, допити розпорядників даних і адміністраторів [1; 18; 19]. Процесуальна фіксація задається вимогами належності, допустимості та відтворюваності: опис середовища і часових налаштувань, read-only копіювання, створення контрольних сум (хешів) для кожного цифрового об'єкта, протоколи з відображенням маршрутів доступу і правок, відсилки до ухвал слідчого судді з мотивованим обґрунтуванням необхідності й пропорційності втручань [3; 4; 7–9]. Завершальною ланкою є стандартизовані контрольні переліки питань для слідчого, прокурора й слідчого судді, що переводять методичні вимоги у форму перевірюваних критеріїв: хто саме створив/змінив документ і коли; чи мав відповідні повноваження; чи узгоджені часові мітки документа з ланцюгом управлінських рішень і платіжних транзакцій; чи існувала менш обтяжлива законна альтернатива доступу до даних; чи доведено ризик втрати або спотворення доказів у разі зволікання [1; 3; 7–9; 18].

Цифровий вимір цієї матриці вимагає строгої дисципліни ланцюга збереження доказів, адже будь-який розрив між моментом виявлення артефакта та його судовим дослідженням компрометує допустимість і доказову вагу. Практичний алгоритм включає картографування джерел даних (EDMS/ERP/CRM, поштові сервери, резервні копії, реєстри, пропускні системи), негайну консерва-

цію стану систем (заморожування журналів, зняття «снапшотів», фіксацію часових налаштувань), створення верифікованих копій із хешами та ведення безперервної документації про походження, переміщення і доступи до кожного об'єкта; ці дії повинні бути «прив'язані» до процесуальних рішень і мотивовані з позицій необхідності та пропорційності [3; 5; 7–9]. Саме у справах про службові правопорушення, де спосіб учинення часто інтегрує документальні маніпуляції, «задні» узгодження і легалізаційні етапи, відтворюваність процедур фіксації стає ключовим критерієм якості: суд очікує не лише логічної версії механізму події, а й технічної можливості повторити кроки вилучення та перевірити цілісність цифрового доказу, що випливає з сучасної доктрини доказування і практики судового контролю [4; 5; 7–9]. На цьому тлі результати ОРД і НСРД набувають процесуальної вартості лише за умови їх первинної підпорядкованості версії способу (цілеспрямований добір засобів, мінімізація втручань) і коректного «вшивання» у процесуальний контур із дотриманням вимог КПК, адже саме модель способу визначає, які негласні комбінації і коли дадуть максимальний індикативний ефект без втрати допустимості [3; 10; 11; 14].

Вершинним елементом застосування матриці є версійне моделювання способу та похідне від нього структурування предмета доказування. Первинно формуються альтернативні версії механізму події з фіксацією ролей кожного учасника, маршрутів документів і коштів, а також «вузлів» виникнення цифрових слідів; далі для кожної версії визначаються перевірювані факти, що підлягають доведенню: мотив і вигода, коло та межі повноважень, конкретні дії на стадіях підготовки, реалізації та приховування, участь посередників, використання регуляторних прогалин, відповідність управлінських рішень економічній доцільності й часовим кореляціям у журналах погоджень та платіжних транзакціях [1; 18–19]. Такий підхід синхронізується з процесуальною доктриною належності й допустимості: доказова інформація має бути отримана у формах, що забезпечують її відтворюваність і перевірність (опис середовища, хеші, журнали доступів, фіксація часових налаштувань), а судовий контроль – мотивовано обґрунтований критеріями необхідності й пропорційності втручань у приватність чи господарську діяльність [3; 4; 7–9].

Першочергові дії в службових провадженнях мають проводитися синхронно і за принципом «замороження» найуразливіших носіїв відомостей. Йдеться про одночасні тимчасові доступи та огляди електронних середовищ (EDMS/ERP/CRM, поштові сервери, резервні копії), інвентаризації матеріальних і цифрових активів, витребування журналів погоджень та історій версій, а також допити розпорядників даних і адміністраторів з фокусом на процеси, а не лише на факти [1; 18–19]. У корупційно ємних сегментах додатково ініціюються ланцюгові перевірки платіжних маршрутів і контрагентів, що маскують неправомірну вигоду під «офіційні обгортки» (консалтинг, гранти, «виграші», благодійність), з паралельною верифікацією ринкової еквівалентності й фактичної реальності наданих послуг [14; 15; 20–22]. Негласні комбінації і результати ОРД застосовуються точково – лише там, де цього вимагає версія способу і де очікується максимальний індикативний ефект за мінімального втручання; подальше «вшивання» таких матеріалів у процесуальну тканину здійснюється з дотриманням вимог КПК до допустимості [3; 10–11; 14].

Типові помилки, що призводять до втрати доказової переконливості, повторювані: несвоєчасна фіксація цифрових слідів і журналів змін; розрив ланцюга збереження доказів через неідентифіковані копії або відсутність контрольних сум; формальний аналіз документів без темпоральної та авторської атрибуції (не визначено, хто і коли створив або змінив файл, чи мав доступ і повноваження); нехтування підготовчою та приховувальною фазами способу; клопотання до слідчого судді без належного обґрунтування необхідності й пропорційності [3; 5; 7–9; 18]. Запобігають цим ризикам стандартизовані контрольні переліки питань для слідчого, прокурора та судового контролю: чи існує менш обтяжлива альтернатива доступу до даних; чи узгоджені часові мітки документів із ланцюгом управлінських рішень; чи підтверджена економічна доцільність угод; чи зафіксовано повний маршрут доступів; чи забезпечено відтворюваність процедури вилучення [1; 3; 7–9; 18].

Трансфер результатів у нормативно-методичну площину передбачає закріплення у відомчих актах класифікації ідентифікаційних ознак способу та індикаторів «злочинних технологій», мінімальних технічних вимог до роботи з цифровими артефактами (ідентифікація джерел, консервація, хешування, опис середовища, ведення ланцюга збереження), а також впровадження уніфікованих шаблонів процесуальної фіксації та переліків питань для судового контролю [1; 3; 7–9; 18–19]. У підсумку поєднання криміналістичної типології способів із процесуальною операціоналізацією через матрицю, цифрову форензіку та ланцюг збереження забезпечує відтворюваний і перевірюваний механізм виявлення й документування службових правопорушень, сумісний з актуальною доктриною доказування та практикою судового контролю [4; 5; 7–9].

Подальше розгортання основного матеріалу доцільно сконцентрувати на прикладних модулях матриці, які переводять класифікаційну рамку у відтворювані алгоритми дій. Перший модуль охоплює ситуації маскування неправомірної вигоди під легальні виплати, зокрема «консалтинг»,

«грантову підтримку», «виграші» та благодійні внески. Практична перевірка починається з відновлення ланцюга формування управлінського рішення та синхронного одержання первинної і цифрової документації: договорів і актів із супровідними листами, журналами погоджень у системах EDMS, журналами доступів до відповідних реєстрів, історіями версій файлів і поштовими треками; далі зіставляються часові мітки документів і подій, ринкова еквівалентність заявлених послуг та наявність реальних результатів робіт, а також кореляція з внутрішніми політиками комплаєнсу [14; 15; 18–22]. Релевантні негласні комбінації застосовуються лише тоді, коли очікується максимальний індикативний ефект за мінімального втручання й забезпечена процесуальна «вшивка» у контур допустимості та судового контролю; критеріями успіху є відтворюваність цифрових процедур фіксації та безперервність ланцюга збереження доказів від моменту виявлення артефактів до представлення у суді [3; 5; 7–9; 10–11; 14].

Другий модуль стосується документальної фальсифікації та «задніх» погоджень у електронному документообігу. Відправною точкою є темпорально-порівняльний аналіз версій документів і маршрутів узгодження, який дозволяє ідентифікувати розриви у логіці змін, невідповідності авторства, а також підміни дат створення чи підписання. Процесуально значущим є детальний опис середовища, версій програмного забезпечення і часових налаштувань, read-only копіювання та створення контрольних сум для кожного цифрового об’єкта, фіксація ланцюга доступів до файлів і реєстрів, а також своєчасне звернення під судовий контроль із мотивованим обґрунтуванням необхідності і пропорційності втручань [1; 3; 5; 7–9; 18–19]. У межах предмета доказування окремо перевіряється узгодженість «офіційної легенди» зі слідами у журналах погоджень та історіях версій: якщо заявлена послуга виконана, вона мусить залишити цифровий «слід процесу» у вигляді листування, проміжних артефактів, календарів та проміжних версій документів, що підтверджується метаданими і журналами доступів [18–19; 21–22].

Третій модуль охоплює експлуатацію регуляторних прогалин і відступи від процедур комплаєнсу. Тут ключовим є порівняльний аналіз «як має бути» та «як було» з опорою на норми права і внутрішні регламенти, який виявляє, чи існувала менш обтяжлива законна альтернатива, чи були свідомо обійдені контрольні механізми, а також хто фактично ініціював і просував рішення у ланцюзі узгоджень [2; 3; 16–18]. У цьому модулі особливою є роль версійного моделювання способу: саме воно задає черговість дій, визначає «вузли» для невідкладної консервації слідів і підказує, де розміщені критичні цифрові артефакти, від вмісту EDMS/ERP до резервних копій і реєстрових логів [1; 18–19]. Усі процедури повинні відповідати сучасній процесуальній доктрині доказування щодо належності, допустимості, відтворюваності і мотивованості клопотань під судовим контролем; недотримання будь-якої з цих вимог з великою ймовірністю призведе до процесуальних втрат у суді по суті [4; 5; 7–9].

Четвертий модуль присвячено відтворенню ланцюгів платежів і зв’язків із контрагентами як «нервовій системі» способу. Алгоритм починається з інвентаризації фінансових документів (платіжні доручення, виписки, договори, акти, рахунки), синхронного доступу до бухгалтерських підсистем та журналів змін, а також запиту політик комплаєнсу й кошторисних лімітів. Далі вибудовується граф переказів і залежностей: бенефіціар–посередник–одержувач, з маркуванням «вузлів» підвищеного ризику (нетипові MCC-коди, «кругові» перекази, короткі інтервали між рішенням і оплатою, непомірна ціна без ринкового обґрунтування). Перевіряється реальність наданих послуг (звітність/листи/проміжні результати), ідентифікуються «офіційні обгортки» для неправомірної вигоди (консалтинг, гранти, благодійність, «виграші»), а також канали легалізації, характерні для суміжних ринків, у т. ч. грального [14; 15; 20–22]. Процесуально значущим є повний опис середовища і часових налаштувань, read-only копіювання, фіксація хешів та ведення безперервного ланцюга збереження доказів для кожного цифрового об’єкта; звернення до слідчого судді має бути мотивоване критеріями необхідності та пропорційності з огляду на ризик «підчисток» [3; 5; 7–9]. У предметі доказування цей модуль підтверджує мотив, вигоду, причинно-наслідковий зв’язок між управлінським рішенням і грошовими потоками та роль посередників [1; 18–19].

П’ятий модуль – тактика допитів «носіїв процесу»: адміністратори систем, бухгалтерія, юристи, особи, що «погоджували» документи, а також захисник і підозрюваний у межах їхніх прав. Фокус зміщується від суто фактичних свідчень до опису процесів: «як реально ухвалювалися рішення», «якою була послідовність і мета погоджень», «хто створював та редагував електронні версії і за чиїм дорученням», «чи існувала альтернативна законна процедура». Тактика допиту вибудовується на зіставленні показань із цифровими журналами, метаданими, календарями та листуванням, що дає змогу швидко виявляти суперечності та ініціювати додаткові процесуальні дії [1; 18–19; 24–25]. Для справ, де захисник відіграє активну роль у формуванні «офіційної легенди», використовується блок питань про реальність правничої допомоги та кореляцію її змісту з документальними артефактами (відповідно до процесуальної доктрини належності/допустимості й судово-

го контролю) [4; 7–9; 13]. Будь-які результати НСРД/ОРЗ інкорпоруються лише після перевірки їхнього походження, цілісності та співвіднесення з версією способу, з урахуванням меж втручання у приватність [3; 10–11; 14].

Шостий модуль – стандарти пакування та представлення цифрових і документальних артефактів. Для кожного об'єкта формується «паспорт доказу», який включає: ідентифікацію джерела, опис середовища і ПЗ, часові пояси/налаштування, спосіб одержання (ухвала/доручення), метод копіювання (read-only), контрольні суми, журнал доступів/переміщень, місце зберігання, перелік похідних копій і перевірок хешів на етапах досудового і судового розгляду [5; 7–9]. Для документів – історія версій, авторство, маршрути погоджень, відповідність часових міток управлінським подіям; для транзакцій – мапа платіжних ланцюгів і ознаки ринкової еквівалентності; для реєстрових дій – логи доступу та службові ролі користувачів [1; 18–19]. Такий «паспорт» забезпечує відтворюваність і перевірність доказового ланцюга згідно з вимогами КПК і сучасної доктрини [3; 4; 7–9].

З урахуванням класифікації та модульного підходу покажемо застосування матриці на типових ситуаціях. Кейс закупівель без конкуренції і «прокладкових» контрактів передбачає первинне картографування процесу ухвалення рішення (ініціатор, погоджувачі, підписанти), синхронне отримання договорів із додатками, технічних завдань, актів, кошторисів і звітів, а також витребування історій версій і журналів погоджень у EDMS, логів доступу до реєстрів і корпоративних бухгалтерських підсистем. Далі зіставляються часові мітки документів із платіжними подіями та внутрішніми лімітами комплаєнсу; тестується ринкова еквівалентність (цінові бенчмарки, альтернативні комерційні пропозиції), перевіряється реальність наданих послуг через проміжні артефакти (листи, протоколи, календарі, чернетки). Типові індикатори способу тут: появи «прокладок», безтоварні операції, задні дати в погодженнях, швидкі інтервали «рішення → оплата», а також зміни авторства у фінальних файлах порівняно з чернетками [12; 14; 18–19]. Процесуально критичними є опис середовища, read-only копіювання, створення контрольних сум і ведення ланцюга збереження для кожного цифрового об'єкта; клопотання до слідчого судді мотивуються необхідністю, пропорційністю та ризиком «підчисток» у системах [3; 7–9].

У кейсі «консалтингова/грантова обгортка» неправомірної вигоди матриця спрямовує на відновлення ланцюга управлінського рішення й платіжних маршрутів, ідентифікацію посередників і пов'язаних осіб, а також тест «процесуальної наявності» послуги: якщо послуга реально виконувалась, у системах мають існувати листування, постановки задач, календарі, чорнові версії матеріалів, трек-ченджі, що корелюють у часі з актами і рахунками. Верифікація ринкової еквівалентності та аналіз контрагентів (у т. ч. їхній профіль на суміжних ринках, пов'язаних із гральним бізнесом або благодійними фондами) дозволяє виявити легалізаційні сегменти «ланцюга виходу» [14–15; 20–22]. Негласні комбінації застосовуються точково під версію способу (напр., фіксація контактів посередника перед платежами), а їх інкорпорація у доказовий масив відбувається з дотриманням вимог належності/допустимості та меж втручання у приватність [3; 10–11; 14].

Ситуації «задніх» погоджень і маніпуляцій в електронному документообігу вирішуються темпорально-порівняльним аналізом: будуються послідовності створення, редагування і погодження документів із прив'язкою до користувачів, ролей і IP/хостів; виявляються аномалії часових міток, розриви логіки змін, невідповідності авторства. Додатково перевіряється, чи відповідають підписи/кваліфіковані електронні підписи маршрутам погодження; чи є в системі «заморожені» копії і резерви, що віддзеркалюють первісний стан файлів. Ці кроки переводяться у процесуальну площину через протоколи огляду електронних систем із зазначенням версій ПЗ, часових налаштувань і створених хешів, а також через фіксацію доступів і прав користувачів, що забезпечує відтворюваність і судову перевірність [1; 3; 5; 7–9; 18–19].

Для кейсів експлуатації регуляторних прогалин матриця вимагає подвійного порівняльного тесту «як має бути/як було»: аналіз норм і внутрішніх регламентів, що визначають належну процедуру, та реконструкція фактичного процесу з джерелами, відповідальними особами і темпоральними зв'язками. Перевіряється, чи існувала менш інвазивна законна альтернатива, чи були свідомо обійдені контрольні механізми і хто фактично просував рішення у ланцюгу узгоджень. На цьому тлі формується обґрунтування необхідності процесуальних втручань і мінімізації даних, придатне до судового контролю [2–3; 16–18].

Окремий вузол матриці стосується допитів «носіїв процесу». Адміністратори систем, бухгалтери, юристи та погоджувачі документів дають не стільки «факти», скільки опис алгоритмів: як реально ухвалювалися рішення, хто ініціював зміни у файлах, чи відповідає задекларована «легенда» цифровим слідам (журнали, метадані, календарі). Тактика допиту будується на зіставленні відповідей із технічними артефактами для швидкого виявлення суперечностей і ініціювання додаткових доступів або експертиз; для справ, де активна роль захисника формує «офіційну легенду», до

переліку питань включаються критерії реальності правничої допомоги та її кореляція з матеріалами справи, відповідно до сучасної доктрини доказування і стандартів судового контролю [4; 7–9; 13; 18–19; 24–25].

Важливо стандартизувати «паспорт доказу» як форму пакування й представлення артефактів. Для кожного цифрового об'єкта він має містити ідентифікацію джерела, опис середовища та версій ПЗ, часові налаштування, спосіб отримання (ухвала/доручення), метод копіювання (*read-only*), контрольні суми, журнал доступів і переміщень, місце зберігання, список похідних копій та акти верифікації хешів на досудовій і судовій стадіях; для документів – історію версій, авторство, маршрути погоджень і узгодженість часових міток із управлінськими подіями; для транзакцій – карту платіжних ланцюгів і тест ринкової еквівалентності; для реєстрових дій – логи доступу та ролі користувачів [3; 5; 7–9; 18–19]. Такий «паспорт» забезпечує відтворюваність і процесуальну перевірність ланцюга збереження, що є центральною вимогою КПК і сучасної доктрини [3–4; 7–9].

Завершально, ризик-орієнтований судовий контроль у нашій моделі реалізується через короткі, але змістовні пакети клопотань: опис ознаки способу, очікувані джерела й конкретні артефакти, чому менш інвазивний інструмент є неефективним, які ризики втрати або спотворення існують, як буде забезпечено мінімізацію персональних даних і безперервний ланцюг збереження. Для оцінки здобутих матеріалів суд застосовує переліки питань щодо відтворюваності процедури, наявності журналів доступів, узгодженості часових міток, авторської атрибуції та повноважень осіб, що вносили зміни [3; 7–9]. Інституціоналізація цих пакетів у відомчих методиках і локальних регламентах мінімізує процесуальні втрати та підвищує керованість розслідувань [1; 18–19].

З урахуванням наведених модулів доцільно формалізувати інтеграцію ОРД і НСРД у доказовий контур через «маршрутизацію за ознакою способу»: кожен індикатор (посередники, «задні» погодження, нетипові платіжні маршрути, експлуатація прогалин) прив'язується до конкретного інструмента одержання відомостей із мінімальним втручанням і максимальною відтворюваністю результату. Практично це означає, що рішення про негласний захід не є «всеохопним», а випливає з логіки способу (напр., короткострокова фіксація контактів перед здійсненням платежу чи перед «узгодженням» у системі), а подальше включення матеріалів у провадження супроводжується повною документацією походження й цілісності та співвіднесенням із вже наявними цифровими слідами (метадані, журнали доступів, історії версій), що знижує ризики недопустимості [3; 10–11; 14]. Установлення причинно-наслідкового зв'язку між управлінським рішенням і вигодою забезпечується «подвійним швом»: документально-цифровою кореляцією (часові мітки погодження ↔ дата платежу ↔ лог доступу до реєстру) і економічним тестом еквівалентності (ринкова ціна ↔ зміст і обсяг заявлених послуг), який унеможливлює легалізацію неправомірної вигоди під «офіційними обгортками» [14–15; 20–22].

Окремо фіксуються показники якості розслідування, що випливають із доктрини доказування і слугують «контрольною картою» на всіх стадіях: повнота карти процесу (ідентифіковані всі учасники і ролі), відтворюваність цифрових процедур (наявні описи середовищ, хеші, журнали доступів, прив'язка часових поясів), безперервність ланцюга збереження (журнали переміщень і копіювань, верифікації хешів), мотивованість і пропорційність клопотань, узгодженість «офіційної легенди» з технічними артефактами, а також наявність «паспортів доказів» на кожен цифровий і паперовий об'єкт [3–5; 7–9; 18–19]. Недотримання будь-якого з цих показників прямо трансформується у процесуальні ризики в суді по суті; своєю чергою, їх системне виконання підвищує переконливість реконструкції способу та стійкість доказового масиву до спростувань [4; 7–9].

Запропонована модель має і межі застосовності. По-перше, у середовищах із низьким рівнем цифрової зрілості частина очікуваних журналів або метаданих може бути відсутня, що вимагає ширшого використання альтернативних джерел (резерви, зовнішні інфраструктури, контрагентські сліди) та посиленого судового контролю за необхідністю доступів [1; 3; 18–19]. По-друге, у високоавтоматизованих системах ризик «невидимих» змін адмінкористувачами компенсується незалежним технічним аудитом середовища та фіксацією інваріантів (хеші, «снапшоти» на рівні носія, апаратні журнали), що забезпечує відтворюваність і перевірність процедур [5; 7–9]. По-третє, у справах із транскордонним відбитком платіжних або хостингових маршрутів необхідна рання координація із процесуальними інструментами міжнародної правової допомоги й узгодженням форматів цифрової фіксації, аби не допустити «дір» у ланцюзі збереження та колізій стандартів допустимості на етапі судового розгляду [2–3; 18]. У підсумку операційна матриця, дисципліна цифрової форензіки і ризик-орієнтований судовий контроль разом утворюють відтворюваний алгоритм виявлення та документування способів учинення службових правопорушень, узгоджений із сучасною доктриною доказування, що уможливлює переходи до прикладних висновків і нормативно-методичних пропозицій для відомчих актів і локальних регламентів [1; 3–5; 7–9; 18–19; 20–22].

Завершуючи «каркас» розділу, формалізуємо алгоритм «першої доби» та предмет доказування, а також вводимо мінімізаційні й приватнісні фільтри, що забезпечують процесуальну стійкість здобутої інформації. Алгоритм першої доби побудовано за принципом одночасності та невідкладної консервації. Спершу складається карта процесу ухвалення рішення (ініціатор, погоджувачі, підписанти, адміністратори систем), далі синхронно здійснюються тимчасові доступи до EDMS/ERP/CRM, поштових серверів, резервних сховищ, бухгалтерських підсистем і реєстрових логів із read-only копіюванням і створенням контрольних сум; паралельно проводяться інвентаризації матеріальних і цифрових активів та допити «носіїв процесу» з фокусом на алгоритмах, а не лише на фактах. Кожен крок документується описом середовища та часових налаштувань, а для кожного об'єкта заводиться «паспорт доказу» й журнал ланцюга збереження. Звернення під судовий контроль готуються за ризик-орієнтованою схемою: ознака способу → очікувані джерела і конкретні артефакти → чому менш інвазивний інструмент неефективний → які ризики втрати/спотворення → як забезпечується мінімізація даних і ланцюг збереження [1; 3; 5; 7–9; 18–19].

Предмет доказування у справах цієї категорії структуровано за п'ятьма блоками. Перший – мотив і вигода: їх встановлення спирається на часові кореляції між управлінськими подіями та грошовими потоками, тест ринкової еквівалентності заявлених послуг і наявність проміжних артефактів виконання робіт (листи, постановки задач, чернетки з трек-ченджами) [14; 18–19; 20–22]. Другий – повноваження й фактичний вплив: зіставляються формальні ролі та реальні дії у журналах погоджень і доступів; фіксуються ініціативні дії «неформальних» учасників процесу [1; 18–19]. Третій – послідовність «підготовка → реалізація → приховування»: картографуються цифрові сліди кожної фази, виявляються «задні» погодження та темпоральні аномалії версій [1; 3; 5; 18–19]. Четвертий – посередники і пов'язані особи: будується граф зв'язків та платіжних маршрутів із виділенням «вузлів» ризику, характерних для схем легалізації (у т. ч. через «консалтинг», гранти, благодійність, сегменти грального ринку) [14–15; 20–22]. П'ятий – експлуатація регуляторних прогалин: проводиться порівняльний аналіз «як має бути/як було» з фіксацією свідомого обминання контрольних механізмів і наявності менш інвазивних законних альтернатив [2–3; 16–18]. Усі блоки підпорядковано вимогам належності, допустимості та відтворюваності: доказова інформація набуває ваги лише за умови правильної процесуальної форми та можливості технічно повторити процедури її здобуття [4; 7–9].

Мінімізаційні та приватнісні фільтри інтегруються в тактику від початку. Для кожного доступу обґрунтовується вузький перелік полів і періодів, які необхідні для перевірки конкретної ознаки способу; запроваджується правило негайного «сепарування» надлишкових персональних даних і протоколювання будь-яких операцій з ними; у клопотаннях до слідчого судді коротко, але чітко пояснюється, чому саме такі обсяги даних є пропорційними заявленій меті та як буде забезпечено їхній захист (обмеження кола доступу, технічні та організаційні бар'єри, політика видалення копій після експертиз) [3; 7–9]. Результати ОРД і НСРД включаються до загального доказового масиву лише після перевірки походження й цілісності та прив'язки до версії способу, аби уникнути недопустимості через «надмірні» або невмотивовані втручання [3; 10–11; 14].

На завершення викладу основного матеріалу окреслюємо метрики якості розслідування, що одночасно є «*чекпоінтами*» для прокурора та суду. Це повнота карти процесу (ідентифіковані учасники, ролі, маршрути документів і коштів), відтворюваність цифрових процедур (описи середовищ, контрольні суми, журнали доступів, часові пояси), безперервність ланцюга збереження (журнали переміщень/копіювань, верифікації хешів), мотивованість і пропорційність клопотань, узгодженість «офіційної легенди» з технічними артефактами, наявність «паспортів доказів» на кожен цифровий і паперовий об'єкт. Сумарно ці показники перетворюють класифікацію способів і модулі матриці на відтворювану процесуальну технологію, сумісну з доктриною доказування та судовим контролем, і створюють надійне підґрунтя для практичних висновків і нормативно-методичних пропозицій, що будуть предметом наступного розділу [1; 3–5; 7–9; 18–19; 20–22].

Висновки з проведеного дослідження зводяться до того, що спосіб учинення службових правопорушень у сучасному цифровому середовищі виступає не лише елементом криміналістичної характеристики, а й конструкцією процесуального управління розслідуванням: через нього формуються версії події, предмет доказування, пріоритети першочергових дій, карта цифрових слідів і рамка судового контролю. Запропонована операційна матриця «*ознака способу → джерела → тактика → процесуальна фіксація → контрольні переліки*» забезпечує відтворюваний перехід від ідентифікації маркерів до одержання й процесуально коректного пакування доказової інформації, сумісної з вимогами належності, допустимості, пропорційності та відтворюваності, закріпленими в КПК та сучасній доктрині доказування [2–4; 7–9]. Ключовим інструментом стійкості доказів є ланцюг збереження, який у службових справах має подвійне навантаження: технічне (*read-only копіювання, хешування, опис середовища, журнали досту-*

пів і змін) та процедурне (мотивованість клопотань, мінімізація даних, документування кожної операції з об'єктом) – будь-який розрив негативно впливає на допустимість і переконливість доказів у суді [3; 5; 7–9; 18–19].

На емпіричному рівні доведено, що типові «технології злочинної діяльності» – розкрадання через безтоварні операції та «прокладки», заволодіння майном шляхом обману з маніпуляціями реєстрами, збагачення у сфері служби під «офіційними обгортками» виплат – зчитуються через сталий набір індикаторів у документах і цифрових журналах; їхня своєчасна консервація і правильна процесуальна фіксація прямо корелюють із успішністю доведення в суді [12; 14–15; 18–22]. Інтеграція ОРД та НСРД у доказовий контур є ефективною лише за умови маршрутизації за ознакою способу, тобто коли кожен індикатор підтягує мінімально інвазивний інструмент збору відомостей, а результати негайно «вшиваються» у процесуальну тканину з підтвердженою цілісністю та походженням [3; 10–11; 14].

Практичний результат моделі – стандартизація «*першої доби*» розслідування: синхронні доступи до EDMS/ERP/CRM, резервів і поштових серверів; темпорально-порівняльний аналіз версій і погоджень; інвентаризації й допити «носіїв процесу» з фокусом на алгоритмах; формування «паспортів доказів» і ризик-орієнтованих пакетів для судового контролю [1; 3; 5; 7–9; 18–19].

У нормативно-методичній площині доцільно закріпити в рубриках відомчих актів класифікацію ознак способів і типових «злочинних технологій», мінімальні технічні вимоги до роботи з цифровими артефактами (ідентифікація джерел, консервація, хеші, описи середовищ, журнали доступів, політика зберігання/видалення), уніфіковані шаблони протоколів огляду електронних систем і «паспортів доказів», а також стандартизовані контрольні переліки питань для слідчого, прокурора та слідчого судді, що віддзеркалюють критерії необхідності, пропорційності, належності та відтворюваності [1; 3; 7–9; 18–19].

Запропонована модель є придатною до масштабування в різних інституційних середовищах – від державної цивільної, військової та правоохоронної служби до державних і приватних закладів – за умови урахування рівня цифрової зрілості та локальних регламентів; у середовищах зі слабкою журналізацією вона компенсується розширеним використанням зовнішніх слідів (контрагенти, резерви, інфраструктури), тоді як у високоавтоматизованих системах – незалежним технічним аудитом і фіксацією інваріантів, що забезпечують повторюваність процедур. Сукупно це дозволяє перевести типологію способів учинення службових правопорушень із площини теоретичних описів у керовану процесуальну й криміналістичну технологію виявлення, документування та доказування, узгоджену з національним процесуальним правом і сучасними уявленнями про якісне доказування у справах цієї категорії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Криміналістична тактика: навчальний посібник / О.В. Бишевець, М.А. Погорецький, Д.Б. Сергєєв та ін. / 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.
2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.
4. Погорецький М. Теорія кримінального процесуального доказування: проблемні питання. *Право України*. 2014. № 10. С. 12–25. URL: https://pravoua.com.ua/uk/store/pravoukr/pravoukr_10_14/Pogoretskyi_10_14.
5. 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.
6. 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.
7. 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.
8. 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.

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.
10. 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.
11. 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.
12. Погорецький М.А., Сухачов О.О. Способи вчинення злочинів у кредитно-банківській сфері та їх значення для оперативно-розшукової діяльності та кримінального процесу. *Кримський юридичний вісник*. 2009. Вип. 2(6). С. 14–22. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A%3D&S21COLORTERMS=1&S21STR=%D0%A1%D1%83%D1%85%D0%B0%D1%87%D0%BE%D0%B2+%D0%9E%24.
13. Погорецький М., Щирук М. Участь захисника у доказуванні у справах про привласнення або розтрату майна службовою особою: проблемні питання та практики. *Knowledge, Education, Law, Management*. 2025. № 3. С. 139–150. DOI: https://doi.org/10.51647/kelm.2025.3.20. URL: https://kelmczasopisma.com/ua/jornal/98.
14. Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою: проблеми доказування стороною обвинувачення у досудовому розслідуванні: монографія / Погорецький М.А., Старенький О.С., Баганець О.В. та ін.; за ред. М.А. Погорецького, С.С. Чернявського. Київ: НАВС, 2017. 250 с.
15. Протидія відмиванню коштів: міжнародні стандарти, зарубіжний досвід, адміністративно-правові, кримінологічні, кримінально-правові, криміналістичні засади та система фінансового моніторингу в Україні: підручник / О.Є. Користін, Л.І. Аркуша, А.С. Беніцький та ін.; за ред. О.Є. Користіна. Одеса: Фенікс, 2015. 984 с. URL: https://nm2.univd.edu.ua/download/113921.
16. Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування кримінальних правопорушень у сфері службової діяльності: дис. … докт. юрид. наук: 12.00.09. Харків, 2017. 575 с. URL: https://dspace.univd.edu.ua/items/71ac104a-9354-4e91-8dc0-4a560b72b1fc.
17. Ромців О.І. Особливості способів вчинення посадових кримінальних правопорушень. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2014. № 8. С. 264–267. URL: http://vestnik-pravo.mgu.od.ua/archive/juspradenc8/72.pdf.
18. Розслідування кримінальних правопорушень у сфері службової діяльності: навч. посібн. / Погорецький М.А., Сергєєва Д.Б., Топорецька З.М., Черняк А.М. та ін.; 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.
19. Салтевський М.В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2008. 588 с. (див. с. 427). URL: https://lib.univer.km.ua/sites/default/files/ Право/Салтевський%20М%20В%20Криміналістика%20у%20сучасному%20викладі.pdf.
20. Топорецька З.М. Виграш у лотерею як спосіб легалізації корупційних доходів. *International scientific and practical conference «New challenges of legal science in Ukraine and EU countries»* (Miskolc, Hungary, 19–20 Apr 2019). Miskolc: Izdevnieciba «Baltija Publishing», 2019. P. 399–402. URL: https://www.navs.edu.ua/files/antykoruptsia/ 2022/materialy_konf_081222.pdf.
21. Топорецька З. М. Легалізація корупційних доходів з використанням грального бізнесу та лотерей. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали VII Міжнар. наук.-практ. конф. (Київ, 8–9 груд. 2022 р.). Київ: НАВС, 2022. С. 291–296. URL: https://www.navs.edu.ua/files/antykoruptsia/2022/materialy_konf_081222.pdf.
22. Toporetska, Z., Pohoretskyi, M., Vazhynskyi, V., Denysenko, G., & Pohoretskyi, M. Institutional risks of organised crime in the gambling business: Structure, mechanisms of influence, and threats to the national security of Ukraine in wartime context based on the analysis of case studies. *Social and Legal Studios*. 2025. 8(2), 200–213. https://doi.org/10.32518/sals2.2025.200. URL: https://sls-journal.com.ua/uk/journals/tom-8-2-2025/institutsiyni-riziki-organizovanoyi-zlochinnosti-v-gralnomu-biznesi-struktura-mekhanizmi-vplivu-ta-zagrozi-natsionalniy-bezpetsi-ukrayini-v-umovakh-viyni-na-osnovi-analizu-materialiv-praktiki.

23. Шумейко Д.О. Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою: проблеми правової кваліфікації. *Юридичний часопис Національної академії внутрішніх справ*. 2015. № 1. С. 39–51. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/9445fa64-2c36-42f6-86c6-2a3d27d715d1/content.
24. 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.
25. Розслідування окремих видів злочинів: навч. посібник / Бишевець О.В., Погорецький М.А., Сергєєва Д.Б. та ін.; за ред. М.А. Погорецького та Д.Б. Сергєєвої. Київ : Алерта, 2015. 536 с. URL: https://alert a.kiev.ua/pravo/463-rozsliduvannya-okremikh-vidiv-zlochiniv.html.