Адміністративне право і процес

УДК 342.9:343.353]:004(091)

DOI https://doi.org/10.5281/zenodo.20441101

Класифікація службових зловживань у цифровому середовищі та форми їх прояву

Панечко Ю. В.,

аспірант ЗВО «Львівський університет бізнесу та права»

https://orcid.org/0009-0003-8901-6781

Прийнято: 02.05.2025 | Опубліковано: 25.05.2025

Анотація. Стаття присвячена побудові матричної класифікації службових зловживань у цифровому середовищі та виявленню типології їх конкретних форм прояву на емпіричному матеріалі українських державних реєстрів та інформаційних систем. Обґрунтовано тезу про те, що цифрова трансформація державного управління, прискорена воєнним станом і євроінтеграційними зобов'язаннями за Угодою про асоціацію Україна–ЄС, модифікує всі три ключові ознаки складу службових злочинів за статтями 364–367 Кримінального кодексу України та адміністративних правопорушень, пов'язаних з корупцією (глава 13-А КУпАП), розширюючи коло суб'єктів за рахунок адміністраторів інформаційних систем та операторів реєстрів, переносячи об'єктивну сторону в площину дії через електронні інтерфейси й роблячи предметом посягання електронні дані, метадані та цифрові ідентичності. Сформульовано матрицю класифікації за п'ятьма взаємодоповнюваними підставами – суб'єктом, об'єктом посягання, способом учинення, використаним цифровим інструментарієм і сферою публічного управління – та обґрунтовано необхідність такого підходу

замість одновимірних класифікацій. На прикладах рейдерських перереєстрацій у Державному реєстрі речових прав, схем у Prozorro, фіктивних записів у ЄДЕБО, маніпуляцій з автоматизованим розподілом справ розгорнуто типологію форм прояву, що еволюціонували від електронних аналогів офлайн-зловживань до якісно нових складів. Зіставлено українську доктрину з європейськими стандартами (GDPR, NIS2, eIDAS 2.0, Будапештська конвенція з Другим додатковим протоколом, практика Суду ЄС у справах C-37/20 і C-601/20 та ЄСПЛ у справі Big Brother Watch v. UK). Сформульовано рекомендації щодо доктринального відмежування статей 364 і 366 КК у цифровому контексті за критерієм мети дії, переосмислення статті 367 у режимі реального часу, введення кваліфікуючої ознаки «масштабованості», повної імплементації Директиви NIS2 з персональною підзвітністю керівників державних реєстраторів та завершення транспозиції GDPR через оновлений Закон «Про захист персональних даних».

Ключові слова: службові зловживання; цифрове середовище; державні реєстри; класифікація; електронні докази; е-урядування; адміністративна відповідальність; кібербезпека критичної інфраструктури.

Classification of official abuses in the digital environment and forms of their manifestation

Panechko Yu. V.,
PhD student, Lviv University of Business and Law
https://orcid.org/0009-0003-8901-6781

Abstract. The article develops a matrix classification of official abuses in the digital environment and identifies a typology of their forms of manifestation on the empirical material of Ukrainian state registers and information systems. The thesis is

substantiated that the digital transformation of public administration, accelerated by martial law and European integration commitments under the Ukraine–EU Association Agreement, modifies all three key elements of the corpus delicti under Articles 364–367 of the Criminal Code of Ukraine and corruption-related administrative offences: it expands the range of subjects to administrators of information systems and operators of registers, shifts the actus reus into the plane of action through electronic interfaces, and makes electronic data, metadata, and digital identities the object of encroachment. A classification matrix is formulated across five complementary criteria – subject, object, method of commission, digital instrumentation, and sphere of public administration – and the necessity of this approach instead of one-dimensional classifications is substantiated. The typology of forms of manifestation is developed through examples of raider re-registrations in the State Register of Property Rights, schemes in Prozorro, fictitious entries in the Unified State Electronic Database on Education, and manipulations with the automated distribution of court cases – forms that have evolved from electronic analogues of offline abuses to qualitatively new corpora delicti. The Ukrainian doctrine is juxtaposed with European standards (GDPR, NIS2, eIDAS 2.0, the Budapest Convention with its Second Additional Protocol, the case law of the CJEU in cases C-37/20 and C-601/20 and of the ECtHR in Big Brother Watch v. UK). Recommendations are formulated on the doctrinal demarcation of Articles 364 and 366 in the digital context, the rethinking of Article 367 in real-time mode, the introduction of the qualifying feature of "scalability", the full implementation of NIS2 with personal accountability of heads of state registrars, and the completion of GDPR transposition through the updated Law on Personal Data Protection.

Keywords: official abuses; digital environment; state registers; classification; electronic evidence; e-government; administrative liability; critical infrastructure cybersecurity.

Постановка проблеми. Цифрова трансформація державного управління України, прискорена повномасштабною війною, ставить перед адміністративним і кримінальним правом виклик нової природи. Чотири класичні склади службових злочинів – зловживання владою або службовим становищем (ст. 364), перевищення влади або службових повноважень (ст. 365), службове підроблення (ст. 366), службова недбалість (ст. 367) Кримінального кодексу України [1] – та блок адміністративних правопорушень, пов'язаних з корупцією (глава 13-А КУпАП України [2]), формувалися тоді, коли документ існував переважно на паперовому носії, повноваження здійснювала безпосередньо посадова особа, а доказом службового рішення слугував підпис чорнилом. Коли публічні послуги перенесли в середовище єдиної державної електронної системи «Дія», електронних публічних закупівель Prozorro, Державного реєстру речових прав на нерухоме майно, Єдиної державної електронної бази з питань освіти, Єдиного реєстру досудових розслідувань, системи eHealth, мобільного застосунку Резерв+ і десятків інших юридично значущих платформ, виник простір, у якому одне натискання кнопки реєстратора має такі самі наслідки, як підписання паперового документа, а одне зловмисне рішення адміністратора інформаційної системи здатне автоматично породжувати сотні неправомірних записів.

Цифровий перехід трансформує всі три ознаки складу: суб'єкта (поряд із класичними посадовими особами з'являються адміністратори інформаційних систем і реєстратори, частина з яких виконує делеговані публічні функції на приватноправовій основі), об'єктивну сторону (дія через електронний інтерфейс, бездіяльність щодо обов'язкових записів у реальному часі, маніпуляція з метаданими), предмет посягання (електронні дані, цифрові ідентичності, алгоритми автоматизованого прийняття рішень). Українська доктрина адміністративного й кримінального права, разом із узагальненням Верховного Суду України про офіційний документ у цифровій формі на матеріальному носії як предмет службового підроблення [3], не пропонує систематизованої

класифікації службових зловживань саме в цифровому середовищі, а наявні класифікації корупційних і службових деліктів зорієнтовані переважно на паперову модель публічного управління.

Матрична класифікація, яка одночасно враховувала б суб'єкта, об'єкт, спосіб, цифровий інструментарій і сферу публічного управління, потрібна особливо гостро з огляду на євроінтеграційні зобов'язання України за Угодою про асоціацію та необхідність гармонізації з acquis (GDPR, NIS2, eIDAS 2.0, Будапештська конвенція з Другим додатковим протоколом). Без матричної моделі правозастосовним органам бракує інструменту диференціації відповідальності, а законодавцеві – підстав для введення кваліфікуючих ознак, що адекватно відображали б масштабованість, асинхронність та автоматизованість цифрових службових зловживань.

Аналіз останніх досліджень і публікацій. Класифікацію службових і корупційних правопорушень у цифровому середовищі досліджує низка українських авторів. Габорець О.А. у журналі «Українська поліцеїстика: теорія, законодавство, практика» розгортає кіберзлочини як об'єкт правової класифікації, виокремлюючи критерії диференціації за способом учинення та інструментарієм [4]. Гужва Ю.С. у виданні «Право та державне управління» досліджує службове підроблення зі статті 366 Кримінального кодексу України в частині проблем кваліфікації та запобігання, що дотикається до цифрових форм створення офіційних документів [5]. Зубок В.Ю. і Давидюк А.В. у журналі «Електронне моделювання» зіставляють вимоги Директиви (ЄС) 2022/2555 (NIS2) щодо кібербезпеки критичної інфраструктури з українським законодавством, окреслюючи нормативний вакуум у частині відповідальності операторів державних реєстрів [6].

Електронні (цифрові) докази та їх допустимість формують доказову основу для притягнення посадовців до відповідальності за цифрові зловживання й

утворюють окремий смисловий блок літератури. Козицька О.Г. у «Юридичному науковому електронному журналі» розглядає поняття електронних доказів у кримінальному провадженні [7]. Романюк В.В. і Абламський С.Є. у журналі «Право і безпека» систематизують критерії допустимості цифрових доказів через автентичність, цілісність, верифіковність джерела, фіксацію метаданих [8]. Погорецький М.А. в «Аналітично-порівняльному правознавстві» розгортає цифрові технології як інструмент і предмет розслідування злочинів проти основ національної безпеки України, де службові зловживання посідають окреме місце [9]. Колеснікова І.А. у «Юридичному науковому електронному журналі» досліджує цифрові сліди як категорію та їх значення при розслідуванні кримінальних правопорушень [10]. Фігурський В.М. у «Галицьких студіях: юридичні науки» аналізує специфіку доказів в електронній формі у кримінальному провадженні [11]. Цехан Д.М. у «Науковому віснику Міжнародного гуманітарного університету» пропонує одне з ранніх в українській літературі визначень цифрових доказів та їх місця в системі доказування, що зберігає методологічну цінність [12].

Зарубіжна наукова література розкриває взаємозв'язок цифровізації публічного управління з корупційними ризиками. Невядомська Е. в «EBRD Law in Transition Journal» оцінює вплив системи Prozorro на українську економіку та її роль в обмеженні корупційних схем [13]. Нижніков Р. у журналі «Problems of Post-Communism» реконструює інституційну еволюцію Prozorro після Революції Гідності та фактори її стійкості [14]. Юкінс К. і Келман С. в «NCMA Contract Management Magazine» формулюють уроки воєнного періоду Prozorro для подолання корупції в публічних закупівлях [15]. Калеснікайте В., Нешкова М. та Фредеріксон М. у журналі «Governance» на основі крос-країнового аналізу досліджують вплив е-урядування на бюрократичну корупцію [16]. Адам І. і Фазекаш М. у «Technology in Society» оцінюють емпіричну спроможність нових цифрових технологій (open data, big data, blockchain) у протидії корупції [17].

Правові обмеження доступу до даних у державних реєстрах та обробки цифрової інформації аналізують окремі публікації. Сімс М. у «Common Market Law Review» розглядає наслідки рішення Суду ЄС у справі WM and Sovim SA для співвідношення приватності та прозорості реєстрів бенефіціарних власників [18]. Зіго Д. у «Bratislava Law Review» переосмислює прозорість реєстрів кінцевих бенефіціарних власників у світлі того самого рішення [19]. Туранянін В. в «International Cybersecurity Law Review» формулює критерії того, коли масове перехоплення комунікацій порушує право на приватність – питання, безпосередньо релевантне для оцінки логів доступу до державних реєстрів як доказів [20].

Наведені дослідження формують надійний фундамент для аналізу окремих сторін проблеми, проте жодне з них не пропонує цілісної матричної класифікації службових зловживань у цифровому середовищі, що поєднувала б виміри суб'єкта, об'єкта, способу, цифрового інструментарію та сфери публічного управління й одночасно враховувала контекст воєнного стану та євроінтеграційних зобов'язань України. Цей розрив у літературі визначає простір авторського доробку.

Формулювання цілей статті. Стаття має на меті побудувати матричну класифікацію службових зловживань у цифровому середовищі, що дозволяє диференціювати юридичну відповідальність за критеріями суб'єкта, об'єкта посягання, способу учинення, використаного цифрового інструментарію та сфери публічного управління. Друга ціль – виявити типологію конкретних форм прояву цих зловживань на емпіричному матеріалі українських державних реєстрів та інформаційних систем, у тому числі рейдерських перереєстрацій у Державному реєстрі речових прав, маніпуляцій у Prozorro, фіктивних записів у ЄДЕБО, маніпуляцій з автоматизованим розподілом справ. Третя ціль – зіставити українську доктрину з європейськими стандартами (GDPR, NIS2, eIDAS 2.0,

Будапештська конвенція, практика Суду ЄС та ЄСПЛ) і сформулювати рекомендації щодо законодавчого, підзаконного, інституційного, гармонізаційного й судового вдосконалення відповідної правової архітектури.

Виклад основного матеріалу. Понятійно-категоріальний апарат службових зловживань у цифровому контексті природно розгортається довкола чотирьох норм Кримінального кодексу України, з якими взаємодіють адміністративні корупційні правопорушення та склад корупційного правопорушення в розумінні Закону «Про запобігання корупції» [21]. Зловживання владою або службовим становищем (ст. 364) утворює умисне використання повноважень всупереч інтересам служби з корисливих мотивів; перевищення влади (ст. 365) передбачає вихід за межі повноважень; службове підроблення (ст. 366) охоплює складання, видачу завідомо неправдивих офіційних документів або внесення до них неправдивих відомостей; службова недбалість (ст. 367) виступає необережною формою тієї самої онтологічної категорії, якою є порушення відносин публічної довіри [1]. Цифрова трансформація модифікує всі три ознаки складу одночасно, причому модифікація має не кількісний, а якісний характер. Суб'єкт розширюється за рахунок адміністраторів інформаційних систем та операторів реєстрів, а також третіх осіб, які отримують делегований електронний доступ і фактично розпоряджаються службовою владою без класичних інституційних рамок. Об'єктивна сторона переходить у площину дії або бездіяльності через електронні інтерфейси: одне натискання кнопки реєстратора має такі самі правові наслідки, як підписання паперового документа, а відсутність обов'язкового запису в режимі реального часу автоматично породжує негативні правові наслідки, що руйнує класичну презумпцію бездіяльності як нейтрального стану. Предметом посягання дедалі частіше стають електронні дані, метадані та цифрові ідентичності, які раніше відігравали роль лише засобу учинення, а сьогодні

ISSN: 3041-2110

набувають самостійної онтологічної ваги, оскільки їхнє існування чи неіснування безпосередньо породжує юридичні наслідки.

Українська доктрина спирається на визначення офіційного документа у цифровій формі на матеріальному носії, закріплене Верховним Судом України [3] та подальше розвинуте у дослідженнях щодо проблем кваліфікації службового підроблення [5]. Такий підхід наближає український правовий стиль до континентально-європейського поняття Amtsmissbrauch і французького abus d'autorité, що так само концентрують смислове ядро складу довкола умисного використання посадою наданих повноважень всупереч її телеологічному призначенню. Водночас зберігається смисловий розрив із англомовним концептом misconduct in public office, у якому акцент зміщений на порушення публічного довір'я як самостійний делікт без вимоги завідомої неправдивості, тобто на підхід, що дозволяв би кваліфікувати і ті форми цифрових зловживань, які не вкладаються у вузький склад фальсифікації. Гіпотетично можна припустити, що зближення української доктрини з англо-американською рамкою публічного довір'я відкрило б ширші можливості реагування на цифрові форми службової неналежності, проте така рецепція потребувала б ґрунтовного теоретичного опрацювання, далекого від простого імпорту чужої категорії.

Визначивши категоріальний апарат, доцільно перейти до інституційного контуру, в якому склади службових зловживань набувають конкретного змісту. Єдина державна електронна система «Дія» станом на початок 2024 року надає доступ до понад тридцяти електронних послуг і чотирнадцяти цифрових документів та обслуговує близько двадцяти мільйонів унікальних користувачів, утворюючи нову точку концентрації службової влади у вигляді єдиної цифрової платформи [22]. Prozorro у 2023 році провела близько 3,6 мільйона процедур публічних закупівель з обсягом близько 480 мільярдів гривень, що втричі перевищило показник 2022 року, перетворюючи прозорість на технологічну норму ринку [13]. Державний реєстр речових прав на нерухоме майно зберігає

юридично значущі записи, що водночас слугують і свідченням права, і об'єктом рейдерських перереєстрацій, поєднуючи в собі онтологічну подвійність юридичного факту та технологічного запису [23]. ЄДЕБО, ЄРДР, електронні кабінети платника податків, eHealth і нещодавно запущений мобільний застосунок Резерв+ розширюють контур цифрової інфраструктури публічного управління, причому кожна з цих систем формує власну логіку доступу, делегування і відповідальності, що відкриває окремі простори потенційного зловживання.

Описана архітектура реєстрів становить організаційну рамку, проте сама вона породжує специфічні ризики, які класична доктрина службових злочинів не могла передбачити. Першим таким ризиком є асинхронність зловживання і його виявлення: запис, внесений у нічну годину неправомірним адміністратором, виявляється через тижні, і вже самий цей часовий розрив руйнує класичну презумпцію миттєвої доступності правової реакції. Другим виступає можливість масштабування, коли один скрипт здатний здійснити сотні перереєстрацій, і одиничне зловживання набуває характеру масового делікту без потреби в окремих діяннях. Третім є складність атрибуції в розподілених системах із делегованими ключами, де між волею суб'єкта і правовим наслідком стоїть проміжний шар технологічної опосередкованості, який ускладнює встановлення суб'єктивної сторони. Четвертим виявляється парадоксальна роль цифрових слідів як одночасно інструменту виявлення та об'єкта фальсифікації [10], що ставить під сумнів саму епістемологічну рамку доказування у цифровому контексті. Режим воєнного стану додав ще один ризиковий шар: за повідомленням AWS, у межах термінової міграції Україна перемістила до хмари 161 державний реєстр і 356 організацій разом із приблизно 15 петабайтами критичних урядових даних, серед яких реєстри речових прав, податкова інформація та система «Дія». Міграція не лише змінила технологічну архітектуру, а й перенесла частину юридично значущих записів за межі

національної юрисдикції, відкриваючи питання про застосовне право, доступ до даних та контроль над логами в умовах транскордонної інфраструктури [24].

Критерії класифікації службових зловживань у цифровому середовищі видається доцільним вибудовувати не одновимірно, а як матрицю взаємодоповнюваних підстав, що розгортається в кількох вимірах одночасно. За суб'єктом необхідно виокремлювати чотири позиції: посадові особи органів публічної влади у класичному розумінні, працівники державних підприємств, установ та організацій, адміністратори інформаційних систем і реєстратори (зокрема приватні нотаріуси, що виконують делеговані публічні функції), треті особи, які виступають співучасниками або фактичними бенефіціарами. За об'єктом посягання виокремлюються права і свободи громадян, державний бюджет, інформаційна безпека, конкурентне середовище. За способом учинення фігурують неправомірний доступ, маніпуляції з даними, бездіяльність щодо обов'язкових записів, використання службових облікових записів у приватних інтересах [4]. За використаним цифровим інструментарієм диференціюються адміністративний доступ до реєстру, інсайдерська обробка персональних даних, маніпуляції з електронним підписом у режимі eIDAS 2.0 [25], втручання в алгоритми автоматизованого прийняття рішень. За сферою публічного управління відкриваються земельні відносини, публічні закупівлі, освіта, охорона здоров'я, оподаткування, судочинство. У такій конструкції кожен з вимірів окреслює власну координату, а конкретне зловживання локалізується одночасно в кількох з них, що дає змогу описувати його не як точку, а як вектор у багатовимірному просторі юридичної кваліфікації.

Одновимірна класифікація недостатня тому, що та сама поведінка одночасно належить до кількох категорій і потребує комбінованого опису для диференціації відповідальності. Маніпуляція з електронним підписом адміністратора реєстру, наприклад, є водночас неправомірним доступом за способом, посяганням на інформаційну безпеку за об'єктом, втручанням в

електронний документообіг за інструментарієм і, залежно від конкретного реєстру, зловживанням у сфері земельних відносин, освіти або судочинства; саме одночасна локалізація в усіх цих вимірах визначає її правову характеристику. Емпіричні дослідження впливу е-урядування на бюрократичну корупцію [16] підтверджують, що цифровізація сама собою корупційного ризику не знижує, бо вона перерозподіляє його, концентруючи в нових точках, серед яких адміністратори реєстрів, точки агрегації даних та алгоритми прийняття рішень. У тому самому смисловому ключі Адам І. і Фазекаш М. [17] спостерігають, що технології забезпечують прозорість лише за умови інституційної здатності верифікувати дані та реагувати на аномалії, без чого вони перетворюються на форму технологічного видовища без правової субстанції. Видається обґрунтованим інтерпретувати ці спостереження як підставу для нової концептуалізації службової влади у цифровому середовищі: вона переходить від матеріальної до диспозитивної форми, де владним актом стає не дія з матеріальним носієм, а налаштування доступу до інформаційної системи.

Абстрактна матриця наповнюється емпіричним змістом через конкретні форми прояву, які доцільно розгорнути в порядку зростання їхньої цифрової специфічності, рухаючись від таких, що мають паперові прототипи, до якісно нових складів, які поза цифровою інфраструктурою неможливі. Неправомірний доступ посадовців до персональних даних громадян у реєстрах МВС, ДРАЦС та інших базах став одним із найпоширеніших проявів, коли інсайдер за гроші формує довідки про осіб, які використовують для шахрайства або тиску [4]; ця форма має очевидний паперовий прототип у вигляді витоку службової інформації, проте її масштаб і швидкість у цифровому середовищі якісно відмінні. Маніпуляції з записами в Державному реєстрі речових прав на нерухоме майно набули форми рейдерських перереєстрацій, коли рейдери отримують віддалений доступ до робочого місця реєстратора або вступають у змову з нотаріусом, який вносить фіктивні підстави переходу права власності

[23], причому первинність цифрового запису перед матеріальним документом тут досягає того рівня, на якому сам реєстр стає об'єктом юридичної реальності. Зловживання в системі Prozorro формалізуються через змову замовника з учасником, технічне маніпулювання критеріями оцінки, штучне обмеження конкуренції через специфікації, що лише на перший погляд є нейтральними; ілюстративним зразком такої практики став епізод закупівлі швабр (як «пристрою з насадкою та утримувачем» за ціною близько ста доларів США за одиницю) онкологічним центром у Києві [13]. Інституційна історія Prozorro [14] разом з уроками воєнного періоду її роботи [15] показують, що технічна архітектура прозорості сама собою не усуває корупційний інтерес, а лише змінює технологічний контекст, у якому він реалізується, переносячи його з кулуарних домовленостей у простір технічних специфікацій і алгоритмічних обхідних маневрів.

Якісно нові форми, не редуковані до паперових прототипів, проявляються там, де цифрова інфраструктура породжує юридичні можливості, недоступні поза нею. Несанкціонована видача документів через електронні кабінети охоплює фіктивні дипломи в ЄДЕБО, безпідставне зняття з військового обліку через Резерв+, зловживання інсайдерською інформацією з податкових і митних систем, використання службового цифрового підпису поза службовими завданнями. Особливою рисою режиму воєнного стану стає можливість оформлювати відстрочки від мобілізації через внесення до бази неправдивих даних про фіктивне студентство осіб, які реально не навчаються; саме оперативність цифрового запису та автоматизована верифікація відстрочок через довідку з ЄДЕБО роблять такий обхід військового обліку особливо привабливим для зловмисників. Бездіяльність щодо обов'язкового внесення відомостей у ЄРДР і маніпуляції алгоритмами автоматизованого розподілу справ у судах належать до тих форм, які класична доктрина не могла передбачити. Особливо показовим є приклад автоматизованого розподілу: судді після відпустки

протягом перших днів мають підвищену ймовірність вибору при авторозподілі, і апаратний працівник, який володіє цією інсайдерською інформацією про коефіцієнти навантаження, здатен скоординувати момент подання справи через «Електронний суд» так, щоб справа потрапила до бажаного судді без жодних слідів втручання в саму систему [26]. Зловживання тут не залишає традиційного матеріального сліду, бо воно існує лише в логіці взаємодії з алгоритмом, і саме ця обставина ставить перед доктриною питання про можливість юридичної кваліфікації того, що технічно є коректним користуванням системою.

Описана типологія була б неповною без міжнародного контексту, який задає рамки гармонізації і формує телеологічний горизонт для національної моделі. Конвенція Ради Європи про кіберзлочинність 2001 року разом із Другим додатковим протоколом про посилене співробітництво та розкриття електронних доказів, відкритим до підписання 12 травня 2022 року і підписаним Україною того ж року [27], формує процесуальну архітектуру транскордонного збирання цифрових доказів у справах про службові зловживання. Регламент GDPR [28] встановлює відповідальність публічних органів за неправомірну обробку даних, передбачає адміністративні штрафи та закладає підставу для відповідальності посадових осіб, виходячи з принципу, що сама посада ще не легітимізує обробку. Директива NIS2 поширює зобов'язання щодо кібербезпеки на критичну інфраструктуру публічного сектору, запроваджуючи персональну підзвітність керівництва та диференційовані санкції: для essential entities передбачено щонайменше 10 мільйонів євро або 2 відсотки світового обороту, для important entities – щонайменше 7 мільйонів євро або 1,4 відсотка [29]. Регламент eIDAS 2.0 встановлює загальноєвропейську рамку цифрової ідентифікації та електронних довірчих послуг, зобов'язуючи держави-члени забезпечити цифрові гаманці до грудня 2026 року [25], і тим самим уніфікує саму онтологію цифрової ідентичності, яка набуває центрального значення в цифровому контексті службових зловживань. Конвенція ООН проти корупції 2003 року в статтях 7, 9

і 13 прямо адресує електронні форми корупції та прозорість урядування, утворюючи глобальний контур, у який вписуються національні та регіональні зусилля [30].

Практика Суду ЄС у справах WM and Sovim SA проти Luxembourg Business Registers (об'єднані справи C-37/20 і C-601/20 від 22 листопада 2022 року) визнала недійсним положення Директиви 2018/843 про відкритий доступ публіки до даних бенефіціарних власників як таке, що становить серйозне втручання у статті 7 і 8 Хартії основних прав ЄС [31]. Аналітика цього рішення [18; 19] доводить його значущість для архітектури українських реєстрів, що рухаються до публічної прозорості бенефіціарів, і ставить перед законодавцем питання про межі цієї прозорості та її співвідношення з приватністю. ЄСПЛ у справі Big Brother Watch and Others v. UK 25 травня 2021 року встановив, що британський режим масового перехоплення комунікацій не містив достатніх «end-to-end» гарантій і порушив статті 8 і 10 Конвенції [32]; критерії, що випливають з цієї практики [20], мають пряме значення для оцінки логів доступу до державних реєстрів як доказів. Підходи Венеційської комісії, GRECO та Європейської прокуратури сходяться у вимозі персональної підзвітності за дії з цифровими інструментами, що зачіпають фінансові інтереси ЄС, і в обов'язку держав забезпечити аудиторський слід для кожного юридично значущого електронного запису, що корелює з Рекомендацією Ради ОЕСР щодо стратегій цифрового уряду [33], яка від 2014 року окреслює базові принципи доброчесності цифрового урядування. Якщо припустити, що ефективна імплементація цих стандартів у національну правову систему можлива лише за умови концептуальної готовності доктрини до сприйняття цифрової специфіки, то роль теоретичної підготовки (зокрема через матричну класифікацію) виявляється не допоміжною, а структурно необхідною.

Механізми протидії та доказування мають інституційний, нормативний і технологічний виміри, які доцільно розглядати у їх взаємозв'язку, а не як

паралельні треки. Інституційний контур охоплює НАЗК, НАБУ, САП, Кіберполіцію, Держспецзв'язку та Державне бюро розслідувань, кожен із яких займає окремий сегмент у поділі юрисдикцій щодо цифрових службових зловживань. Нормативний інструментарій включає електронне декларування з автоматизованою перевіркою через зіставлення з понад двадцятьма реєстрами та банками даних [34], що саме собою є прикладом використання матричної логіки в правозастосовній практиці, бо перевірка одного факту відбувається через кілька координат одночасно. Технологічні рішення сягають систем виявлення аномалій у логах доступу, блокчейн-фіксації юридично значущих дій, штучного інтелекту для виявлення схем у Prozorro, і їхня ефективність зростає пропорційно інтеграції з нормативною та інституційною рамками. Доказовий аспект залишається найвразливішим: за чинною редакцією Кримінального процесуального кодексу України [35] дублікат документа та копія комп'ютерних даних, виготовлені слідчим із залученням спеціаліста, визнаються оригіналом, що породжує проблему дуальної природи електронного доказу. Інформація, носій та метадані, які формуються пристроєм створення інформації, утворюють триєдину структуру, у якій кожен компонент окремо є невід'ємною частиною доказу [36]. Українська доктрина обґрунтовує критерії допустимості цифрових доказів через автентичність, цілісність, можливість верифікації джерела та фіксацію метаданих хешуванням [7; 8; 9; 10; 11; 12], і саме така багатокритеріальна структура виявляється практичним відображенням матричного підходу на доказовому рівні. Проблема отруйних плодів постає особливо гостро, коли логи доступу до реєстру отримано в порядку, що порушує гарантії статті 8 ЄКПЛ і стандарт, закріплений у справі Big Brother Watch [32]: такі докази треба визнавати недопустимими навіть за наявності матеріальної істини у справі, бо інакше сам процес доказування втрачає той телеологічний горизонт законності, заради якого він існує.

Авторська позиція щодо вдосконалення класифікаційної моделі розгортається у трьох взаємопов'язаних тезах, що випливають із попереднього аналізу. Доктринальне відмежування статті 364 від статті 366 КК у цифровому контексті, як видається обґрунтованим, варто проводити за критерієм мети дії: коли посадова особа використовує службові електронні повноваження для отримання неправомірної вигоди без створення неправдивого запису, кваліфікація йде за статтею 364, а коли створюється або змінюється запис, що містить завідомо неправдиві відомості, належить застосовувати статтю 366. Склад службової недбалості (стаття 367) у цифровому середовищі потребує переосмислення, оскільки бездіяльність щодо обов'язкового внесення відомостей у реєстр у режимі реального часу є якісно іншою формою порівняно з паперовою недбалістю, бо реєстр генерує юридично значущі дії автоматично, і відсутність запису безпосередньо породжує правові наслідки без будь-якого окремого делікту посадової особи. Видається обґрунтованим запровадити матричний класифікатор з обтяжуючою ознакою масштабованості: коли одне діяння автоматично породжує сотні неправомірних реєстраційних дій, ступінь суспільної небезпеки якісно зростає й має знаходити відображення у санкції, інакше класична правова реакція виявляється структурно непропорційною новій онтології цифрового зловживання. Найближчий горизонт нормативної дії становить поглиблення інтеграції з європейською рамкою через повну імплементацію NIS2 [29] у національне законодавство про критичну інфраструктуру з персональною підзвітністю керівників державних реєстраторів, завершення транспозиції GDPR через оновлений Закон «Про захист персональних даних» і ратифікацію Другого додаткового протоколу до Будапештської конвенції з імплементацією прискорених процедур отримання даних від провайдерів послуг [27]. Відсутність цих кроків здатна затягнути моніторинг виконання Угоди про асоціацію і одночасно залишити українську доктрину в позиції відстаючої адаптації, тоді як цифровий перехід уже сьогодні

формує нові форми службових зловживань швидше, ніж право встигає їх кваліфікувати.

Висновки. Службові зловживання у цифровому середовищі не вкладаються в одновимірну класифікацію за об'єктом, способом чи суб'єктом ізольовано, оскільки сам феномен має багатовимірну онтологію, у якій кожен з елементів складу одночасно зачіпається цифровою специфікою. Запропонована матрична модель враховує суб'єкта в усьому спектрі від класичної посадової особи до адміністратора інформаційної системи й третьої особи зі співучастю, об'єкт посягання, спосіб учинення, використаний цифровий інструментарій і сферу публічного управління в їхньому одночасному застосуванні. Така модель пропонує правозастосовним органам інструмент диференціації відповідальності, а законодавцеві підставу для введення кваліфікуючих ознак, що адекватно відображали б асинхронність, масштабованість і автоматизованість цифрових службових зловживань. Її методологічне значення виходить за межі суто класифікаційної функції, бо матриця водночас задає телеологічну рамку правової реакції, окреслюючи, які саме виміри феномена потребують диференційованого юридичного оформлення, і визначає горизонт подальшого розвитку доктрини.

Аналіз інституційної архітектури українських державних реєстрів (від «Дії» до Prozorro, від ЄДЕБО до ЄРДР, від Резерв+ до eHealth) показує, що цифрова трансформація корупційний ризик автоматично не зменшує, а перерозподіляє, концентруючи в адміністраторах реєстрів, точках агрегації даних і алгоритмах прийняття рішень. Евакуація приблизно 15 петабайтів критичних державних даних до хмарної інфраструктури в умовах воєнного стану додала юрисдикційний вимір, що потребує окремого правового реагування, бо саме питання застосовного права і доступу до доказів у транскордонних архітектурах залишається відкритим. Класичні склади статей 364–367

Кримінального кодексу зберігають чинність як інструменти кваліфікації, проте їх застосування у цифровому контексті вимагає чіткого відмежування за метою дії, переосмислення службової недбалості в режимі реального часу і введення обтяжуючої кваліфікуючої ознаки масштабованості. Без таких доктринальних рухів право залишається структурно непідготовленим до реакції на нові форми зловживань.

Європейський контекст задає три рамкові правила, кожне з яких має пряме відображення в українській правовій реальності. Першим виступають суворі обмеження публічного доступу до даних бенефіціарних власників після рішення Суду ЄС у справах C-37/20 і C-601/20, що актуалізує питання балансу між прозорістю та приватністю в українських реєстрах. Другим стає персональна підзвітність менеджменту критичної інфраструктури за NIS2 з диференційованими адміністративними санкціями, що ставить вимогу переосмислення інституційної архітектури підзвітності операторів державних реєстрів. Третім є високі стандарти процесуальної законності в обробці метаданих за практикою ЄСПЛ, що визначає верхню планку для українського кримінального процесу у справах про цифрові службові зловживання. Гармонізація з європейськими стандартами через повну імплементацію NIS2, завершення транспозиції GDPR і ратифікацію Другого додаткового протоколу до Будапештської конвенції становить обов'язок України за Угодою про асоціацію та одночасно умову збереження довіри міжнародних партнерів до української цифрової інфраструктури.

Перспективи подальших досліджень охоплюють статус автоматизованих рішень як предмета зловживання, відповідальність за бездіяльність у режимі реального часу, транскордонну юрисдикцію щодо хмарних реєстрів, методику експертизи цифрових слідів і доктринальну розробку складу цифрового службового зловживання як можливого окремого підрозділу розділу XVII Особливої частини Кримінального кодексу України. Видається обґрунтованим

стверджувати, що поглиблене вивчення окреслених питань сприятиме формуванню цілісної правової архітектури, здатної адекватно відповісти на виклики, які цифрова трансформація публічного управління ставить перед адміністративним і кримінальним правом. Якщо ж припустити, що темп цифрового переходу й надалі випереджатиме темп доктринального реагування, то структурне зростання правового відставання може стати тривалішою проблемою, ніж окремі складнощі кваліфікації, що особливо актуалізує методологічну роботу над матричними моделями опису службової влади у цифровому контексті.

Список використаних джерел

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

2. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10

3. Узагальнення судової практики Верховного Суду України щодо застосування статті 366 Кримінального кодексу України : постанова Судової палати у кримінальних справах ВСУ від 09.07.2015 № 5-50кс15. URL: https://reyestr.court.gov.ua/

4. Габорець О. А. Кіберзлочини як об'єкт правової класифікації. *Українська поліцеїстика: теорія, законодавство, практика*. 2024. URL: https://www.policeyistika.dnuvs.ukr.education/index.php/policeyistyka/article/view/267

5. Гужва Ю. С. Службове підроблення у кримінальному праві України: проблеми кваліфікації та запобігання. *Право та державне управління*. 2024. № 4. С. 277–283.

6. Зубок В. Ю., Давидюк А. В. Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555 (NIS2). *Електронне моделювання*. 2023. Т. 45, № 5. С. 55–61.

7. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421. DOI: https://doi.org/10.32782/2524-0374/2020-8/103

8. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні. *Право і безпека*. 2024. № 2 (93). URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653

9. Погорецький М. А. Цифрові технології у розслідуванні кримінальних правопорушень. *Вісник кримінального судочинства*. 2023. № 3–4. С. 84–102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf

10. Колеснікова І. А. Цифрові сліди: поняття та значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. № 10. DOI: https://doi.org/10.32782/2524-0374/2023-10/114

11. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: юридичні науки*. 2023. № 4. С. 97–105. DOI: https://doi.org/10.32782/galician_studies/law-2023-4-14

12. Цехан Д. М. Цифрові докази: поняття, особливості та місце в системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260.

13. Підсумки публічних закупівель: у 2023 році обсяги закупівель зросли утричі – до 480 млрд грн. *Кабінет Міністрів України*. 29.12.2023. URL: https://www.kmu.gov.ua/news/pidsumky-publichnykh-zakupivel-u-2023-rotsi-obsiahy-zakupivel-zrosly-utrychi-do-480-mlrd-hrn

14. Nizhnikau R. Love the Tender: ProZorro and Anti-Corruption Reforms after the Euromaidan Revolution. *Problems of Post-Communism*. 2022. Vol. 69, No. 2. P. 192–204.

15. Yukins C., Kelman S. Overcoming Corruption and War – Lessons from Ukraine's ProZorro Procurement System. *NCMA Contract Management Magazine*. 2022. URL: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2887&context=faculty_publications

16. Kalesnikaite V., Neshkova M., Frederickson M. Parsing the impact of E-government on bureaucratic corruption. *Governance*. 2023. Vol. 36, No. 3. P. 827–842. DOI: https://doi.org/10.1111/gove.12707

17. Adam I., Fazekas M. Are emerging technologies helping win the fight against corruption? *Technology in Society*. 2021. Vol. 66. DOI: https://doi.org/10.1016/j.techsoc.2021.101680

18. Siems M. Privacy vs. Shareholder Transparency: Did the ECJ Decision in WM and Sovim SA Impair the Global Fight Against Money Laundering? *Common Market Law Review*. 2023. Vol. 60, No. 4. P. 1137–1152. DOI: https://doi.org/10.2139/ssrn.4540817

19. Zigo D. CJEU: WM and Sovim SA v. Luxembourg Business Registers – Rethinking Transparency of Ultimate Beneficial Owners Registers. *Bratislava Law Review*. 2023. Vol. 7, No. 2. P. 227–240. DOI: https://doi.org/10.46282/blr.2023.7.2.725

20. Turanjanin V. When does bulk interception of communications violate the right to privacy? *International Cybersecurity Law Review*. 2023. Vol. 4, No. 1. P. 115–135.

21. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18

22. Дія: портал державних послуг України. URL: https://diia.gov.ua

23. Рейдерські справи у суді: хто буде відповідачем та до якого суду звертатися? *Адвокатське бюро «Ципін і партнери»*. URL: https://tsypin.partners/rejderski-spravi-u-sudi-hto-bude-vidpovidachem-ta-do-yakogo-sudu-zvertatisya/

24. Robinson F. How a push to the cloud helped a Ukrainian bank keep faith with customers amid war. *Nextgov/FCW*. 2023. URL: https://www.nextgov.com/modernization/2023/11/how-push-cloud-helped-ukrainian-bank-keep-faith-customers-amid-war/392375/

25. Регламент (ЄС) 2024/1183 Європейського Парламенту і Ради від 11.04.2024 (eIDAS 2.0). *Official Journal of the European Union*. 30.04.2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj

26. Автоматизований розподіл справ у судах: чи все гаразд. *Дзеркало тижня*. URL: https://zn.ua/ukr/POLITICS/avtomatizovanij-rozpodil-sprav-u-sudakh-chi-vse-harazd.html

27. Конвенція Ради Європи про кіберзлочинність (ETS № 185), Будапешт, 23.11.2001; Другий додатковий протокол про посилене співробітництво та розкриття електронних доказів (CETS № 224), Страсбург, 12.05.2022. URL: https://www.coe.int/en/web/cybercrime

28. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27.04.2016 про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний обіг таких даних та про скасування Директиви 95/46/ЄС (GDPR). *Official Journal of the European Union*. L 119. 04.05.2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

29. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14.12.2022 про заходи щодо досягнення високого спільного рівня кібербезпеки на території Союзу (NIS2). *Official Journal of the European Union*. L 333. 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

30. Конвенція Організації Об'єднаних Націй проти корупції від 31.10.2003. URL: https://zakon.rada.gov.ua/laws/show/995_c16

31. Court of Justice of the European Union. Joined Cases C-37/20 and C-601/20, WM and Sovim SA v Luxembourg Business Registers, judgment of 22.11.2022, ECLI:EU:C:2022:912. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0037

32. European Court of Human Rights. Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, Grand Chamber judgment of 25.05.2021. URL: https://hudoc.echr.coe.int/eng?i=002-12080

33. OECD. Recommendation of the Council on Digital Government Strategies. OECD/LEGAL/0406. 2014. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

34. НАЗК змінює підхід до відбору та перевірок декларацій. *Національне агентство з питань запобігання корупції*. URL: https://nazk.gov.ua/uk/uk/nazk-zminyue-pidhid-do-vidboru-ta-perevirok-deklaratsiy/

35. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17

36. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. *Юридична газета*. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi-dokazi-pid-chas-vikonannya-vimog-st-290-kpk-ukrayini.html