

УДК 342.9

DOI <https://doi.org/10.32782/ln.2025.26.43>

Білозьорова Л.В.

здобувач Науково-дослідного інституту публічного права

ВДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ З ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Нормативно-правова база діяльності органів прокуратури, що здійснюють інформаційно-правове забезпечення, є сукупністю чинних нормативно-правових актів та інших правових джерел, які регламентують створення, збирання, обробку, використання, зберігання та розкриття інформації в процесі здійснення діяльності органів прокуратури. Теоретично вона виконує функції систематизації правовідносин, встановлення правових режимів інформації та визначення відповідальності за їх порушення.

У межах адміністративного права важливим є те, що інформаційно-правове забезпечення органів прокуратури охоплює як діяльність із внутрішнього адміністрування (адміністративно-правове забезпечення їхньої функції), так і здійснення ними процесуальних, наглядових, контрольно-правових функцій. Отже, нормативно-правова база виступає не лише як суто «інформаційне» регулювання, але й як елемент адміністративної організації органів прокуратури.

Правова природа такої бази має подвійний характер, з одного боку це галузеве регулювання інформаційно-правових відносин у публічному секторі, а з іншого це організаційне регулювання діяльності органів прокуратури як суб'єкта публічної влади. У цьому сенсі нормативно-правова база виступає як частина системи адміністративного права, оскільки встановлює правила поведінки посадових і службових осіб, регламентує їхню відповідальність у адміністративному процесі, формує правовід-

носини «органи прокуратури – інформація – суспільство».

На нашу думку, в контексті даного дослідження нормативно-правова база характеризується такими ознаками: 1) Обов'язковість – акти мають нормативний характер, встановлюють загальнообов'язкові правила для органів прокуратури та їх працівників; 2) Ієрархічність – акти розташовані в системі права за юридичною силою та рівнем підпорядкованості (що важливо для уточнення питань пріоритету норм); 3) Системність і комплексність – вона повинна бути таким чином структурована, щоб регулювати всі стадії інформаційного циклу (збирання, обробка, захист, зберігання, доступ) саме для органів прокуратури [1, с. 88]; 4) Динамічність – у зв'язку з розвитком технологій (цифровізація, big data, кібербезпека) нормативно-правова база повинна постійно адаптуватись. Наприклад, у контексті України йдеться про забезпечення інформаційної безпеки в органах прокуратури; 5) Взаємозв'язок із правами людини і публічними інтересами – оскільки інформаційно-правове забезпечення органів прокуратури стосується доступу до інформації, захисту інформації, конфіденційності, державної таємниці тощо. Це підкреслюється у наукових дослідженнях інформаційного права [2, с. 44].

Що стосується поняття нормативно-правової бази, то її слід розуміти, як сукупність нормативно-правових актів та інших юридичних джерел, які регулюють певну сферу публічного управління, а у нашому випадку

це діяльність органів прокуратури у сфері інформаційно-правового забезпечення. У змісті цього поняття виділяються такі складові: джерело права, суб'єкт видачі, юридична сила акта, предмет регулювання (наприклад: доступ до інформації, зберігання службової інформації, захист конфіденційної інформації, реалізація технологічних процедур) та механізм забезпечення контролю і відповідальності.

Щодо структури нормативно-правової бази слід виокремити ієрархію актів та внутрішню логічну побудову. Згідно з адміністративно-правовою доктриною, джерела адміністративного права України включають: Конституцію України, закони України, міжнародні договори, підзаконні акти Кабінету Міністрів України, міністерств, відомчі нормативно-правові акти (наприклад, накази, інструкції), а також рішення Конституційного Суду України та інші джерела (наприклад, підзаконні акти) [3, с 115].

Ми вважаємо, що зв'язок нормативно-правової бази з адміністративною відповідальністю та службовою дисципліною проявляється так: нормативно-правові акти встановлюють обов'язки посадових осіб органів прокуратури щодо інформаційно-правового забезпечення. Одночасно передбачають правові наслідки – дисциплінарна відповідальність за порушення посадового обов'язку чи процедури, адміністративна відповідальність за правопорушення, пов'язані з інформацією, а також можуть містити підстави для звільнення чи інших організаційно-правових заходів. У цьому сенсі нормативно-правова база виступає як підґрунтя, на якому реалізуються механізми державного примусу та контролю в адміністративній площині.

Структура бази має бути сформована за модульним принципом: а) модуль «доступ і розкриття»; б) модуль «захист і зберігання»; в) модуль «контроль і аудит»; г) модуль «відповідальність». Кожен модуль включає відповідні акти різного рівня, від закону до внутрішньої інструкції. Такий підхід забезпечує

системність і прозорість діяльності органів прокуратури у сфері інформаційно-правового забезпечення.

Крім того, варто відзначити, що вдосконалення нормативно-правової бази органів прокуратури у сфері інформаційно-правового забезпечення невід'ємно пов'язане з інституційно-правовими передумовами, які формують контекст і можливості правотворчості та правозастосування. До основних передумов належать:

1. Статус органів прокуратури – виходячи із положень ст. 2 Закону України «Про прокуратуру», як суб'єктів публічної влади, які здійснюють функцію державного нагляду за додержанням законодавства, а також функцію інформаційно-правового забезпечення [4]. У цьому контексті їхній правовий статус має бути чітко закріплений законодавчо, із визначенням компетенцій, прав і обов'язків, включно з інформаційно-правовою діяльністю.

2. Система управління інформаційною безпекою – органи прокуратури мають мати відповідні структурні підрозділи (наприклад, департаменти, управління, служба кібербезпеки) й внутрішні процедури. Наприклад, існує положення про Департамент інформаційно-аналітичного та організаційного забезпечення, контролю виконання та перевірок стану організації прокурорської роботи Генеральної прокуратури України [5].

3. Цифрова трансформація та технологічна інфраструктура – для інформаційно-правового забезпечення необхідна сучасна IT-інфраструктура, механізми журналювання, резервування, захисту від витоку даних тощо. Нормативно-правова база має передбачати ці засоби. У науковій літературі наголошується на потребі системного інформатизаційного підходу в діяльності органів прокуратур [6].

4. Взаємодія з іншими суб'єктами публічної влади та міжнародними інститутами – оскільки інформаційно-правове забезпечення органів прокуратури часто пов'язане з іншими державними органами (наприклад, правоохо-

ронними, антикорупційними, кібербезпеки) та міжнародними стандартами. Нормативно-правова база має враховувати ці взаємодії (наприклад, обмін інформацією, взаємне визнання доказів, доступ до міжнародних реєстрів).

5. Контроль і відповідальність – інституційна передумова полягає у встановленні чіткої системи контролю за дотриманням інформаційно-правового законодавства органами прокуратури, визначенні відповідальних осіб, процедури дисциплінарної, адміністративної відповідальності.

6. Підготовка персоналу та розвиток правосвідомості – інституційно-правова передумова полягає в тому, що працівники органів прокуратури повинні мати відповідну підготовку.

Тобто, оновлення нормативно-правової бази в інформаційно-правовому забезпеченні органів прокуратури має відбуватись не лише через текст акта, але й через створення відповідної інституційної екосистеми, яка дозволяє запровадити ці норми в практику, забезпечити їх виконання, оцінити ефективність і реагувати на виклики.

У свою чергу, в сучасних умовах цифровізації публічного управління особливого значення набуває якісне та структуроване нормативне регулювання інформаційно-правового забезпечення діяльності органів прокуратури. Адже саме нормативно-правова база визначає межі, форми та засоби обробки інформації, захисту службових і конфіденційних даних, встановлює порядок доступу, відповідальність за порушення та гарантії дотримання прав людини.

Конституційний рівень задає первинні межі для публічного управління інформацією, закріплюючи право кожного «вільно збирати, зберігати, використовувати і поширювати інформацію» та одночасно дозволяючи його обмеження на підставі закону в інтересах національної безпеки, територіальної цілісності, громадського порядку тощо. Це системно впливає на регламентацію доступу до інфор-

мації в органах прокуратури, оскільки будь-який режим обмеження (службова, конфіденційна інформація, персональні дані) має впливати з закону та відповідати критеріям необхідності і пропорційності. Таким чином, стаття 34 Конституції України виконує роль конституційного «якоря» для всієї системи вторинних норм у сфері обробки та захисту інформації прокурорськими установами [7].

Закон України «Про прокуратуру» (№1697-VII) визначає правовий статус органів прокуратури, їхні завдання та обов'язки, у тому числі вимоги до службової поведінки прокурора стосовно збереження охоронюваної законом інформації. У межах інформаційно-правового забезпечення значення мають норми щодо організації діяльності, повноважень і процесуальних гарантій, які опосередковано задають очікувані стандарти поведінки з відомостями, що містяться в матеріалах проваджень, внутрішніх інформаційних системах тощо. По суті, закон формує «рамку компетенції», у межах якої підзаконні акти деталізують процедури доступу, зберігання, захисту, обліку й розкриття інформації. Зокрема, цей закон прямо передбачає у ст. 19, що прокурор зобов'язаний не розголошувати відомості, які становлять таємницю, що охороняється законом [4].

Крім того, галузеві інформаційні закони забезпечують режимну «начинку» цієї рамки. Закон України «Про інформацію» [8], встановлює дефініції, класифікацію інформації та загальні правила доступу/обмеження; Закон України «Про захист персональних даних» [9] – принципи і підстави обробки, обов'язки володільців/розпорядників і права суб'єктів даних; ці вимоги безпосередньо поширюються на органи публічної влади, включно з органами прокуратури. Унаслідок цього виникає обов'язок вибудувати внутрішні процедури так, щоб забезпечити мінімізацію доступу, журналювання, правові підстави обробки й коректні механізми обмеження доступу.

На рівні підзаконних актів та відомчих нормативно-правових документів форму-

ється низка правил, які безпосередньо реалізують норми законодавства, адаптуючи їх до внутрішньої організації та специфіки органів прокуратури. Це включає накази, інструкції, положення про службу інформаційного забезпечення, внутрішні політики захисту інформації, процедури доступу до публічної інформації, журнали обліку доступу, резервного копіювання та інші технічні й організаційні заходи.

Базовим документом сьогодні є Наказ Генерального прокурора від 06.08.2020 №363 «Про організацію роботи органів прокуратури з особистого прийому, розгляду звернень і запитів та забезпечення доступу до публічної інформації», яким затверджено, зокрема, Інструкцію про порядок забезпечення доступу до публічної інформації в органах прокуратури України [10]. Цим наказом також визнано такими, що втратили чинність, попередні інструкції, зокрема наказ від 18.04.2018 №75, – тобто відбулася консолідація і оновлення процедур доступу до публічної інформації на єдиній платформі.

Важливим елементом відомчого рівня є Кодекс професійної етики та поведінки прокурорів, який, попри етико-деонтологічну природу, містить імперативи належної поведінки щодо збереження та нерозголошення охоронюваної законом інформації й поваги до прав людини у сфері обробки даних; на практиці він слугує орієнтиром для оцінки дисциплінарної відповідальності, коли відсутні більш детальні технологічні стандарти у відомчих інструкціях [11].

Також неможливо не згадати дисциплінарний статут прокуратури України (Постанова ВРУ №1796-ХІІ від 06.11.1991) визначає загальні засади заохочень і дисциплінарної відповідальності прокурорських працівників і застосовується, зокрема, до порушень правил поведінки з інформацією, якщо такі порушення виражаються в недодержанні службових обов'язків або розголошенні охоронюваних відомостей. Статут має лаконічну структуру (18 статей) і відсилає до законодав-

ства та відомчих актів, що підкреслює потребу саме у деталізації інформаційних стандартів у внутрішніх регламентах прокуратури (інструкціях, порядках, політиках) [12].

Поза цими документами, сфера інформаційної взаємодії з іншими органами державної влади інституціоналізується окремими міжвідомчими актами. Показовим є спільний наказ Державної судової адміністрації України та Офісу Генерального прокурора від 02.05.2024 №189/98, яким затверджено порядок електронної інформаційної взаємодії (реєстрація електронних кабінетів органів прокуратури, обмін процесуальними документами в Єдиній судовій інформаційно-телекомунікаційній системі) [13].

Також необхідно зазначити, що важливим орієнтиром для модернізації нормативно-правової бази України є міжнародно-правові джерела. До таких джерел належать конвенції, рекомендації й стандарти (наприклад, Конвенція Ради Європи про кіберзлочинність – «Будапештська конвенція», директиви Європейського Союзу з кібербезпеки, стандарти Організації Об'єднаних Націй). Впровадження їх положень сприяє приведенню українського правового регулювання до міжнародних вимог, зокрема у сфері обробки електронних доказів, реагування на кіберінциденти та забезпечення доступу до інформації в умовах воєнного стану. Для органів прокуратури це означає імперативи щодо належного оформлення доступу до даних, фіксації ланцюга збереження і процесуальних гарантій [14].

Окремі проекти Ради Європи для України (CyberEast/CyberEast+) фокусують увагу на узгодженості національних норм із Будапештською конвенцією та практиках обміну даними, що прямо стосується інформаційно-правового забезпечення прокуратури (збереження трафікових даних, оперативне надання інформації, транскордонні запити). Практична цінність таких ініціатив у виробленні типових процедур і доказових стандартів, які далі інтегруються у відомчі акти [15].

Проте аналіз чинної нормативно-правової бази України вказує на численні системні проблеми інформаційно-правового забезпечення діяльності органів прокуратури, що стримують розвиток та імплементацію якісних механізмів захисту інформації, належного регулювання доступу, відповідальності посадових осіб, а також наявності ефективного контролю. Ці недоліки набувають особливої ваги в умовах воєнного стану, зростання кіберзагроз і необхідності взаємодії прокуратури з іншими структурами в режимі реального часу. На нашу думку, серед найбільш актуальних та таких, що потребують першочергового вирішення є:

1. Фрагментарність та відсутність єдиної системи – чинне правове регулювання інформаційно-правового забезпечення у прокуратурі базується на окремих, часто неузгоджених нормативно-правових актах, від Конституції України і Закону «Про прокуратуру» до інструкцій Генерального прокурора, наказів та внутрішніх положень. Відсутність системного акта або уніфікованого підходу створює прогалини, дублювання норм і правову невизначеність, особливо щодо службової інформації, електронних доказів, правил обробки даних тощо.

2. Колізії між загальним інформаційним законодавством і спеціальними актами – закони «Про інформацію» та «Про захист персональних даних» регулюють обіг інформації загалом, однак не враховують специфіку функціонування прокуратури. З іншого боку, Закон «Про прокуратуру» не має чітких норм, які визначають обов'язки та відповідальність працівників прокуратури у сфері інформаційної безпеки. Це створює потенційні колізії, зокрема у випадках визначення меж конфіденційної інформації, порядку її класифікації та механізмів доступу.

3. Проблеми застосування Дисциплінарного статуту прокуратури України: 1) Обмеженість сфери регулювання – Дисциплінарний статут прокуратури України, затверджений Постановою Верховної Ради

України від 06.11.1991 № 1796-ХІІ, містить лише загальні положення щодо дисциплінарної відповідальності. У ньому відсутні спеціальні норми щодо порушень інформаційного характеру, витоку службової або конфіденційної інформації, недотримання правил доступу до інформаційних реєстрів, недотримання правил ведення інформаційних систем, ігнорування режиму збереження електронних документів тощо; 2) Відсутність механізму «ескалації» стягнень за повторні порушення – поточна редакція Статуту не враховує принцип прогресивної відповідальності. Повторні порушення, пов'язані з інформацією, не мають чітко прописаного наслідку, наприклад: перше порушення – дисциплінарне стягнення, друге – адміністративне, далі – переведення на іншу посаду/звільнення. Це створює прогалини у запобіганні системним порушенням інформаційної безпеки; 3) Відсутність процедурних норм щодо цифрових інцидентів – статут не регламентує порядок фіксації фактів несанкціонованого доступу, втрати даних, цифрових інцидентів, що унеможлиблює їх кваліфікацію як дисциплінарні проступки в умовах сучасної цифрової інфраструктури прокуратури.

4. Невизначені моменти у Кодексі України про адміністративні правопорушення (КУпАП) щодо відсутності окремих складів правопорушень, які стосуються інформаційних проступків, а також відсутність нормативного закріплення адміністративної відповідальності за порушення у сфері інформаційної безпеки у сфері публічної служби. Це створює ситуацію, коли працівники правоохоронних органів (БЕБ, ДБР, Нацполіції, СБУ, НАБУ), працівники прокуратури можуть грубо порушити режим інформаційного поводження без наслідків у публічному правовому полі. Окрім того, відсутність норми про «повторне правопорушення» у сфері інформаційної дисципліни – КУпАП не містить положень, які кваліфікують повторне правопорушення, пов'язане з інформацією, як обтяжуючу обставину або окремий склад, що

зменшує превентивну силу правового регулювання.

5. Проблеми інформаційного законодавства: 1) Відсутність спеціального закону про службову або конфіденційну інформацію – попри наявність Закону України «Про інформацію», класифікація відомостей як службових або конфіденційних має загальний характер. У реальному обігу в органах прокуратури застосовуються внутрішні класифікації, які не мають законодавчого закріплення, що породжує правову невизначеність. Працівники часто не мають чіткого орієнтира, які саме категорії інформації потребують спеціального режиму обігу; 2) Неврегульованість поводження з інформацією, отриманою в цифровій формі – законодавство не визначає належні способи фіксації, зберігання, передавання й архівування електронної інформації в межах кримінального або іншого провадження. Це породжує практичні проблеми в доказуванні, формуванні цифрових слідів, верифікації джерел даних тощо; 3) Відсутність механізмів «технічного обов'язку» (організаційно-технічні заходи) – інформаційне законодавство не містить прямих приписів для органів прокуратури щодо застосування багатофакторної автентифікації, журналювання доступу, резервного копіювання – що є загальноприйнятими в міжнародній практиці (зокрема відповідно до стандартів ISO/IEC 27001) [16].

Саме тому, виходячи із наведених проблем та необхідності того, що у сучасних умовах цифровізації державного управління та зростання кіберзагроз інформаційно-правове забезпечення діяльності органів прокуратури потребує не лише адаптації до технологічного прогресу, але й глибинного нормативно-правового переосмислення. Де структурна фрагментарність, відсутність спеціалізованих механізмів відповідальності за порушення в обігу інформації та в роботі з інформаційними системами, а також недостатність процедурних гарантій фіксації та реагування на інциденти, об'єктивно вимагають системного

оновлення відповідних законодавчих і відомчих актів. А тому, першочерговими напрямками вдосконалення нормативно-правової бази діяльності органів прокуратури з інформаційно-правового забезпечення мають бути:

1. Зміни до Дисциплінарного статуту прокуратури України, зокрема це:

1) Створення окремого розділу Статуту № IV «Дисциплінарна відповідальність за проступки у сфері обігу інформації, а також під час роботи в інформаційних системах» – у якому чітко визначити види проступків, пов'язаних із порушенням режиму поводження з інформацією, зокрема: а) неналежне зберігання документів, що містять службову або конфіденційну інформацію; б) розголошення службової інформації в будь-якій формі (усній, письмовій, цифровій); в) недотримання процедури доступу до електронних реєстрів; г) порушення порядку класифікації або декласифікації документів; ґ) невиконання внутрішніх політик інформаційної безпеки; д) ігнорування правил зберігання цифрових носіїв та резервного копіювання; е) несвоєчасне внесення відомостей до ЄРДР; ж) незабезпечення повного, всебічного та достовірного обліку обов'язкових до внесення відомостей про кримінальне правопорушення до ЄРДР.

На наш погляд, новий розділ Статуту має містити в собі: 1) Поняття інформаційного дисциплінарного проступку; 2) Типологію проступків; 3) Категорії тяжкості; 4) Процедури фіксації інциденту; 5) Докази; 6) Ескаляційну шкалу стягнень.

Як результат, запровадження спеціального розділу дозволить уніфікувати підхід до визначення дисциплінарних порушень в інформаційній сфері, посилить правову визначеність для прокурорсько-слідчих працівників і створить основу для практичного застосування заходів реагування у цифрову епоху.

2) Доповнення статті 9 Статуту новим видом дисциплінарного стягнення – заборона доступу до службової інформації на певний

строк. Так, до переліку дисциплінарних стягнень необхідно внести новий захід: «заборона доступу до окремих категорій службової інформації на певний строк». Такий захід буде альтернативою для випадків, коли прокурора не слід звільняти, але він проявив недбалість у поводженні з інформацією. З ним необхідно провести додаткове навчання з метою запобігання повторення подібних порушень. Це дозволить поєднати принцип відповідальності із принципом інституційної доцільності. Як результат, це створить інструмент гнучкої відповідальності, підвищить рівень персональної обачності при роботі з інформацією, а також мінімізує ризики повторного витоку або маніпулювання даними.

2. Зміни до Кодексу України про адміністративні правопорушення, зокрема це:

1) Доповнення статті 172-8 КУпАП (Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень). Суть змін: а) уточнити, що інформація може бути як в електронній, так і в матеріальній формі; б) ввести кваліфікуючу ознаку – «якщо такі дії вчинені особою, яка раніше була притягнена до дисциплінарної відповідальності за порушення режиму поводження з інформацією»; в) передбачити одночасно з накладенням штрафу можливість накладення санкції у вигляді тимчасового позбавлення права доступу до інформаційних систем органів державної влади на певний строк. Як результат, поєднання дисциплінарного та адміністративного впливу сформує механізм «ескалації» відповідальності, що є загальновизнаним принципом у міжнародній правовій практиці.

2) Оновлення статті 212-5 КУпАП (Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію). А також внесення змін до статті 255 КУпАП (Особи, які мають право складати протоколи про адміністративні правопорушення).

Крім того, в межах змін до КУпАП, а саме для техніко-юридичної бездоганності запропонованої моделі посилення відповідальності необхідно на рівні Загальної частини КУпАП уніфікувати сам предмет адміністративного стягнення, пов'язаний із інформаційною сферою. Йдеться про запровадження узагальненого конструкта «спеціальне право доступу до охоронюваної інформації» як легальну категорію, котра може бути об'єктом адміністративного позбавлення на визначений строк. Таке «спеціальне право» слід розуміти як службово зумовлену, персоніфіковану можливість посадової чи службової особи виконувати операції з інформацією, що має спеціальний правовий режим (службова, конфіденційна, інша охоронювана законом інформація), у тому числі доступ у відповідні інформаційні системи, реєстри та сховища даних у межах посадової компетенції.

Нормативно це потребує трьох взаємопов'язаних кроків. По-перше, необхідно доповнити Загальну частину визначенням самого поняття «спеціального права доступу» як правового статусу, що виникає не автоматично, а через сукупність умов: проходження спеціальних перевірок/атестації, наявність службової потреби та оформлені адміністратором доступи до інформаційних ресурсів.

По-друге, у Загальній частині КУпАП, у статті 24 (види адміністративних стягнень) слід визначити новий різновид адміністративного стягнення – «позбавлення спеціального права доступу до охоронюваної інформації».

По-третє, у Загальній частині доцільно встановити кореляційне правило: якщо особа піддана дисциплінарному стягненню за інформаційний проступок, то при вчиненні повторного (аналогічного за характером) порушення протягом визначеного строку це становить кваліфікуючу підставу для застосування адміністративного стягнення у вигляді позбавлення спеціального права доступу (або адміністративної заборони провадити діяльність, пов'язану з обробкою охоронюваної інформації). Такий підхід унеможливить роз-

рив між відповідальністю у дисциплінарній та адміністративній площинах, забезпечить логіку «ескалації» та водночас утримує правозастосувача в межах принципів необхідності й пропорційності.

Крім того, у Загальній частині КУпАП доцільно передбачити статтю у якій визначити загальні процесуальні наслідки для роботодавця/органу державної влади, а саме покладення обов'язку на адміністраторів безпеки органу державної влади після набрання чинності постанови суду про позбавлення правопорушника спеціального права доступу до інформації, невідкладно виконати рішення (блокувати особисті ключі доступу, деактивувати облікові записи, анулювати токени/сертифікати, переглянути матриці доступів), а сам факт застосування такого стягнення підлягає внесенню кадровим підрозділом до відомчого реєстру для контролю повторності. У сукупності це формує чіткий, технологічно дружній до правозастосування механізм, який узгоджує перелік стягнень у КУпАП із реальними режимами роботи з даними у правоохоронній та суміжній сферах.

3. Вдосконалення інформаційного законодавства, зокрема доповнити Закон України «Про інформацію» новим розділом щодо службових осіб «Особливості використання службової та конфіденційної інформації посадовими та службовими особами публічних органів». У ньому визначити: а) обов'язки щодо зберігання, недопущення витоку, дотримання політик доступу; б) обмеження на повторне використання інформації (особливо після звільнення з посади); в) права громадян на захист від незаконного обігу їхніх даних через недбалість посадових осіб. Як результат, усунення прогалин між загальними нормами інформаційного права та специфікою публічного сектору, а також зменшення рівня корупційних ризиків.

4. Вдосконалення інституту дисциплінарної відповідальності – необхідно створити окремий підінститут у межах загального інституту дисциплінарної відповідальності

«інформаційна дисциплінарна відповідальність», що: а) базується на характеристиці службової інформації як об'єкта особливого захисту; б) передбачає стандарти обов'язкової поведінки; в) формує спеціальні види стягнень (обмеження доступу, тимчасове блокування акаунтів, тимчасова заборона виконання повноважень). Як результат, гнучка система реагування на порушення без вдавання до звільнення, чітка кореляція між видом порушення й видом стягнення, а також запобігання «перевантаженню» системи звільнень і судових позовів.

5. Пропонується офіційно впровадити в нормативно-правову базу прокуратури механізм обліку повторності інформаційних проступків з відповідною градацією стягнень: 1) Перше порушення (легке) – тягне дисциплінарне зауваження, запис в особову справу; 2) Друге порушення (аналогічне або інше впродовж року) – тягне адміністративне стягнення, позбавлення доступу; 3) Третє порушення (системне або з наслідками) – тягне довгострокову заборону займати відповідні посади, переведення до іншого структурного підрозділу або звільнення.

Ця модель має бути відображена у: 1) Дисциплінарному статуті прокуратури України, як окрема стаття запропонованого вище розділу № IV «Дисциплінарна відповідальність за інформаційні проступки» або таблиця ескалації; 2) КУпАП – як підстава для кваліфікації повторності; 3) відомчих інструкціях прокуратури, як обов'язкова процедура обліку порушень та ведення реєстру.

Як результат, забезпечення системності покарання, створення мотиваційного бар'єру для повторних порушень, а також зменшення зловживань та підвищення безпеки обігу інформації в органах прокуратури.

6. Запровадити рамковий «мінімальний технічний профіль безпеки» для органів публічної влади. Доцільно ухвалити урядовий акт рамкового характеру, що закріпить мінімальні, обов'язкові для всіх органів критерії технологічної безпеки, а саме багатфакторну

автентифікацію, централізоване журналювання, обов'язкове шифрування на робочих станціях і носіях, сегментацію прав доступу, політику резервування та регулярну перевірку відновлюваності, а також періодичні аудити доступів. Такий документ, маючи загальнодержавний статус, стане «парасолькою», під якою відомчі інструкції прокуратури зможуть деталізувати власні регламенти без ризику суперечностей або технологічних «прогалин». Як результат, єдність мінімальних стандартів, чіткий зв'язок між технічними вимогами і юридичною відповідальністю.

7. Запровадження уніфікованих форм документування інцидентів (акт виявлення; чек-лист первинних дій; шаблон технічного звіту; матриця оцінки впливу; фінальний висновок) та стандартного таймлайна (повідомлення протягом 24 годин; первинний технічний звіт – до 72 годин; фінальний висновок – до 10 днів) забезпечить швидкість і якість реагування. Уніфікація дозволить порівнювати інциденти між регіонами, створити спільну «мову» для взаємодії ІТ-фахівців, юристів та керівництва, а також зменшить ризики процесуальних помилок у дисциплінарних і адміністративних справах.

8. Щорічне підвищення кваліфікації та атестація з інформаційної безпеки як умова доступу – атестація має складатися з теоретичного тесту та практичних кейсів. Невдале складання – є підстава для тимчасового обмеження доступів і обов'язкового повторного навчання. Поєднання мотивації та санкційної рамки забезпечить реальне підвищення компетентності, а не формальне «підписання інструктажу».

Запропоновані напрями вдосконалення нормативно-правової бази діяльності органів прокуратури з інформаційно-правового забезпечення спрямовані на побудову сучасної системи інформаційної безпеки в органах прокуратури. Вони мають сприяти: а) формуванню чіткої ієрархії відповідальності; б) посиленню правових гарантій конфіденційності даних; в) гармонізації з міжнарод-

ними стандартами; г) формуванню інституційної пам'яті через чітке документування та правове закріплення всіх стадій поводження з інформацією. За належного законодавчого супроводу ці пропозиції здатні трансформувати інституційну поведінку працівників органів прокуратури та сформувати якісно нову інформаційно-правову культуру. Вони мають стати превентивним запобіжником випадкам неналежного поводження з інформацією та підвищити ефективність роботи з інформаційними системами прокуратури.

У свою чергу, розкриття досліджуваної проблематики вважається неповноцінним без аналізу судової практики. Адже судова та квазісудова (дисциплінарна) практика у сфері обігу службової й конфіденційної інформації в органах прокуратури розгортається у трикутнику правових режимів: а) доступ до публічної інформації та межі його обмеження; б) таємниця досудового розслідування і процесуальні особливості обігу даних; в) персоніфікована відповідальність службових осіб (дисциплінарна та адміністративна). Для коректної оцінки кейсів застосовано критеріальний підхід: 1) правовий статус запитуваної/використаної інформації; 2) наявність і якість «трискладового тесту» (законність, легітимна мета, необхідність/пропорційність); 3) фіксація технічної частини (журналювання, збереження цифрових слідів, інцидент-менеджмент); 4) індивідуалізація відповідальності з урахуванням повторності та наслідків. Так прикладами реальних кейсів судової практики можна навести:

1. У справі № 101393078/2021 від 26.11.2021 Одеського окружного адміністративного суду позивач звернувся до Одеської обласної прокуратури із запитом на надання копії розпорядчого акту, який формував групу прокурорів, що здійснювали процесуальне керівництво у кримінальному провадженні. Сторона відповідача вважала, що такий запит стосується процесуального документа і тому розглядається не за Законом «Про доступ до публічної інформації», а за правилами кри-

мінального процесуального кодексу України. Суд встановив, що відповідач діяв з порушеннями: не було належного розгляду запиту як публічної інформації, відмовився мотивовано надати копію акту, і визнав бездіяльність. Суд дійшов висновку, що запитувана інформація вже існувала й була задокументована, а перевірки/оціночні дії не були передбачені Законом «Про доступ до публічної інформації» [17]. Цей приклад ілюструє стандарт щодо публічної інформації: органи прокуратури як суб'єкти владних повноважень зобов'язані надавати задокументовану інформацію, якщо вона не становить таємниці слідства, і не можуть зловживати процедурою посилення строків чи перевірок. Водночас справа фіксує проблему – неоднозначність застосування норм (спеціального процесуального права vs. закону про доступ), що створює правову невизначеність.

2. У рішенні № 640/7688/21 від 21.03.2024, яке публікується в спеціалізованих базах, відображено спор щодо адвокатського запиту до Державного бюро розслідувань про надання відомостей, які містяться у Єдиному реєстрі досудових розслідувань. Відповідач відмовив, мотивуючи, що запитувані відомості належать до таємниці досудового розслідування згідно зі ст. 222 КПК України і що порядок їх отримання має визначатися саме КПК. Суд відзначив, що хоча інформація може містити відомості слідства, проте не кожен такий запит автоматично відноситься до заборонених і що відповідач повинен був обґрунтувати необхідність обмеження саме через закон і наявність пропорційності [18].

З практики видно, що органи прокуратури стикаються з дилемою: з одного боку, захист таємниці слідства; з іншого – вимога загального права на доступ до інформації. Судова практика встановлює, що відмова має бути обґрунтованою, з застосуванням «трискладового» підходу (законність, легітимна мета, пропорційність).

3. У публічному доступі зафіксовано дисциплінарне провадження КДКП щодо витоку

відомостей під час проведення НСРД, пов'язане з прокурором Бадіоном М.О.. За фавбулою, попередження про прослуховування було отримане підозрюваними у месенджері. Службове розслідування з технічною прив'язкою SIM/IMEI вказало на апарат і номер, якими користувався прокурор. КДКП застосувала звільнення з посади як пропорційне стягнення; фавбулу, хід та мотиви рішення викладено у відкритому повідомленні Комісії, а також у фахових медіа-оглядах. Водночас у відкритих судових масивах не виявлено остаточного судового підтвердження цього звільнення (станом на дату підготовки огляду), що важливо для загального висновку про «кінцеві» наслідки [19].

4. У справі щодо Запорізької обласної прокуратури суд визнав протиправною відмову у наданні інформації на адвокатський запит, підкресливши необхідність індивідуалізованого «трискладового тесту» (законність обмеження – легітимна мета – необхідність/пропорційність) і часткового доступу (вилучення чутливих фрагментів). Це рішення відтворює усталений підхід адміністративних судів до мотивації відмови та структури відповіді розпорядника [20].

Проте варто підкреслити, що Конституційний Суд України стабільно підкреслює, що право на доступ до інформації не є абсолютним і може бути обмежене за умов законності, легітимної мети та необхідності, що задає рамку для адміністративних судів у спорах щодо відповідей прокуратури на запити громадян, журналістів чи адвокатів [21]. Загалом, судова практика виступає важливим індикатором ефективності нормативно-правового регулювання діяльності органів прокуратури в сфері інформаційно-правового забезпечення. Аналіз конкретних рішень дозволяє не лише відобразити рівень правозастосування, але й виявити прогалини в нормотворчій базі, її імплементації, взаємозв'язках із процесуальними стандартами та адміністративною відповідальністю. У контексті діяльності органів прокуратури ключовими є питання:

чи забезпечується належний доступ до інформації, чи дотримуються стандарти обробки службової/конфіденційної інформації, яку відповідальність несуть працівники прокуратури за порушення правил обігу інформації, чи формуються передумови превенції повторних проступків.

Висновки. Проведене дослідження дає підстави стверджувати, що чинна нормативно-правова база, яка регламентує інформаційно-правове забезпечення діяльності органів прокуратури України, є фрагментованою, методологічно розпорошеною та недостатньо адаптованою до сучасних викликів цифрового суспільства. На рівні конституційного та законодавчого регулювання, окремі положення щодо інформаційної функції прокуратури залишаються декларативними та не забезпечують цілісного адміністративно-правового механізму реалізації її повноважень у сфері інформаційних правовідносин. У свою чергу, відомчі та підзаконні акти, попри певну деталізацію процедур, нерідко дублюють або суперечать одне одному, що унеможливує єдність правозастосування.

Інституційно-правові передумови реформування цієї бази мають спиратися на концепцію інтегрованої цифрової прокуратури, яка поєднує прозорість, відповідальність та

безпеку у сфері управління інформаційними потоками. Адміністративно-правові аспекти потребують гармонізації з європейськими стандартами в частині забезпечення балансу між правом на інформацію та обмеженнями, пов'язаними з державною таємницею, службовою інформацією, а також захистом персональних даних. Окремого нормативного переосмислення потребує інститут юридичної відповідальності за інформаційні проступки прокурорських працівників із врахуванням принципу пропорційності та спеціального правового статусу.

Вказані недоліки мають бути усунені шляхом системного перегляду таких актів, як Дисциплінарний статут прокуратури України, Кодекс України про адміністративні правопорушення, а також профільного інформаційного законодавства. Крім того, важливо забезпечити механізми міжвідомчої інтероперабельності, оновлення внутрішніх інформаційних стандартів та адаптацію до новітніх цифрових загроз. Таким чином, вдосконалення нормативно-правової бази діяльності органів прокуратури з інформаційно-правового забезпечення має здійснюватися в межах адміністративно-правової доктрини, орієнтованої на ефективне публічне управління, законність, прозорість та цифрову безпеку.

Агортація

У статті здійснено комплексне дослідження теоретико-правових засад, змісту, структури та актуального стану нормативно-правової бази, що регламентує інформаційно-правове забезпечення діяльності органів прокуратури України. Особлива увага приділена аналізу інституційно-правових передумов оновлення чинного масиву нормативних актів, що регулюють доступ, обробку, обмін та захист інформації в межах повноважень органів прокуратури. Обґрунтовано, що адміністративно-правовий аспект є ключовим для формування ефективного та контрольованого механізму інформаційної взаємодії між органами прокуратури та іншими суб'єктами публічної влади.

У роботі запропоновано систематизовану модель нормативно-правової бази в цій сфері, з виокремленням конституційно-законодавчого рівня, підзаконних і відомчих нормативно-правових актів, а також міжнародно-правових джерел та механізмів їх імплементації. Окреслено проблеми правової невизначеності, колізійності, фрагментарності регулювання та недостатності санкційного потенціалу чинного законодавства. На цій основі сформульовано авторські напрями удосконалення нормативно-правової бази, зокрема в частині оновлення Дисциплінарного статуту прокуратури України, внесення змін до Кодексу України про адміністративні

правопорушення та гармонізації інформаційного законодавства з європейськими стандартами. У контексті практичної реалізації цих підходів проаналізовано судову практику, яка ілюструє наявність прогалин у нормативному регулюванні відповідальності та інформаційної діяльності прокурорських працівників.

Запропоновані положення можуть бути використані для формування концептуальних засад реформування адміністративно-правового забезпечення діяльності органів прокуратури в інформаційній сфері, з урахуванням принципів законності, спеціалізації, пропорційності та підконтрольності. Актуальність порушених питань зростає в умовах цифрової трансформації органів публічної влади та викликів, пов'язаних із захистом персональних даних, службової та іншої охоронюваної інформації.

Ключові слова: органи прокуратури України, інформаційно-правове забезпечення, правове регулювання, підзаконні акти, міжнародно-правові стандарти, інституційна спроможність, цифрова трансформація, дисциплінарна відповідальність, правова імплементація, інформаційна безпека.

Bilozorova L. V. Improving the regulatory framework for the activities of prosecutors' offices in the field of information and legal support

Summary

The article carries out a comprehensive study of the theoretical and legal foundations, content, structure and current state of the regulatory and legal framework that regulates the information and legal support of the activities of the prosecutor's office of Ukraine. Particular attention is paid to the analysis of the institutional and legal prerequisites for updating the current body of regulations that regulate access, processing, exchange and protection of information within the powers of the prosecutor's office. It is substantiated that the administrative and legal aspect is key to the formation of an effective and controlled mechanism for information interaction between prosecutor's offices and other subjects of public power. The work proposes a systematized model of the regulatory and legal framework in this area, with the separation of the constitutional and legislative level, subordinate and departmental regulatory and legal acts, as well as international legal sources and mechanisms for their implementation. The problems of legal uncertainty, conflict, fragmentation of regulation and insufficient sanction potential of the current legislation are outlined. On this basis, the author's directions for improving the regulatory framework have been formulated, in particular in terms of updating the Disciplinary Statute of the Prosecutor's Office of Ukraine, amending the Code of Ukraine on Administrative Offenses and harmonizing information legislation with European standards. In the context of the practical implementation of these approaches, judicial practice has been analyzed, which illustrates the existence of gaps in the regulatory regulation of the responsibility and information activities of prosecutors.

The proposed provisions can be used to form conceptual principles for reforming the administrative and legal support of the activities of prosecutors' offices in the information sphere, taking into account the principles of legality, specialization, proportionality and control. The relevance of the issues raised is increasing in the context of the digital transformation of public authorities and the challenges associated with the protection of personal data, official and other protected information.

Key words: prosecutor's offices of Ukraine, information and legal support, legal regulation, by-laws, international legal standards, institutional capacity, digital transformation, disciplinary liability, legal implementation, information security.

Список використаних джерел:

1. Гайдай С. Г. Інформація прокуратури: питання правової природи, класифікації та реалізації повноважень по роботі з інформацією. *Наукові праці МАУП. Серія Юридичні науки*. 2018. № 56(2). С. 86–94. URL: <https://journals.maup.com.ua/index.php/law/article/download/840/1358>
2. Кормич Б. А. Інформаційне право : підручник. Харків : Бурун і К, 2011. 334 с. URL: https://www.researchgate.net/publication/369358287_Informacijne_pravo
3. Ludmila Stasiuk, Oleksandr Stasiuk, Serhii Zytsyk, Liubov Sheptytska, Yurii Husiev, Yurii Skrypiuk. *Sources system of asministrative law in Ukraine*. AD ALTA. 12/02-XXIX. 2022. pp. 113-117. URL: http://www.magnanimitas.cz/ADALTA/120229/papers/A_20.pdf
4. Про прокуратуру : Закон України від 14.10.2014 № 1697-VII : станом на 7 верес. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1697-18#Text>
5. Наказ Генеральної прокуратури України 21 жовтня 2019 року № 237. Положення про Департамент інформаційно-аналітичного та організаційного забезпечення, контролю виконання та перевірок стану організації прокурорської роботи Генеральної прокуратури України. URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=207663
6. Цимбалюк В. Правова інформатика в діяльності прокуратури України. *Правова інформатика*. 2007. № 2. С. 18-27. URL: <https://ippi.org.ua/sites/default/files/07tvdpu.pdf>
7. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
8. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14 черв. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
9. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
10. Про організацію роботи органів прокуратури з особистого прийому, розгляду звернень і запитів та забезпечення доступу до публічної інформації : Наказ Офісу Ген. прокурора від 06.08.2020 № 363 : станом на 18 лип. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/v0363905-20#Text>
11. Кодекс професійної етики та поведінки прокурорів : Кодекс Ген. прокуратури України від 27.04.2017. URL: <https://zakon.rada.gov.ua/laws/show/n0001900-17#Text>
12. Про затвердження Дисциплінарного статуту прокуратури України : Постанова Верхов. Ради України від 06.11.1991 № 1796-XII : станом на 15 лип. 2015 р. URL: <https://zakon.rada.gov.ua/laws/show/1796-12#Text>
13. Наказ Державної судової адміністрації України та Офісу Генерального прокурора від 02.05.2024 № 189/98. URL: https://dsa.court.gov.ua/userfiles/media/new_folder_for_uploads/dsa/2024/normativna_pravova_baza/Dod_N_189_98_02-05-2024.pdf
14. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
15. CyberEast+: Ukrainian authorities committed to further strengthen legislation on cybercrime and electronic evidence. URL: <https://www.coe.int/en/web/cybercrime/-/cybereast-ukrainian-authorities-committed-to-further-strengthen-legislation-on-cybercrime-and-electronic-evidence>
16. ISO/IEC 27001:2022, 2013. Система Менеджменту Інформаційної Безпеки. Юнісерт Україна. Міжнародна сертифікація ISO 27001. System Management | Міжнародна сертифікація ISO 9001, ISO 14001, OHSAS 18001, ISO 22000, ISO 50001, ISO 27001, ISO 17100, ISO 13485. URL: https://certification.com.ua/iso27001?gad_source=1&gad_campaigni

d=22638344346&gbraid=0AAAAAo4yQR0tSg1Uy1JC59J1192CR4TJi&gclid=CjwKCAjw04HIBhB8EiwA8jGNbQUHf2q4SYImC4nlmx93YI91SJuxBkqNhr3XCoT7DU-KDRI5MPsmMMhoCJQkQAvD_BwE

17. Рішення № 101393078. 26.11.2021. Одеський окружний адміністративний суд. URL: <https://youcontrol.com.ua/catalog/court-document/101393078/>
18. Постанова суду № 640/7688/21 від 21.03.2024 про визнання протиправною бездіяльності та зобов'язання вчинити дії, провадження у якій відкрито. ipLex Судові рішення. URL: <https://iplex.com.ua/doc.php?regnum=117858879&red=100003cd1e1c2a50c3abd457cd5c19edc73dc&d=5>
19. Кваліфікаційно-дисциплінарна комісія прокурорів. Офіційний сайт. URL: <https://kdkp.gov.ua/decision/2024/08/6/4833>
20. Рішення № 99680763. 16.09.2021. Запорізький окружний адміністративний суд. URL: <https://youcontrol.com.ua/catalog/court-document/99680763/>
21. 4.3.1. Право на інформацію. Конституційний Суд України. Офіційний вебсайт. URL: <https://ccu.gov.ua/storinka-knygy/431-pravo-na-informaciyu>

Дата надходження статті: 18.08.2025

Дата прийняття статті: 20.08.2025

Опубліковано: 29.09.2025