ISSN 2524-0374

УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2025-8/70

ДЕЯКІ ПИТАННЯ УДОСКОНАЛЕННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ СУБ'ЄКТІВ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ

SOME ISSUES OF IMPROVING THE LEGAL RESPONSIBILITY OF SUBJECTS OF INFORMATION AND LEGAL SUPPORT OF THE ACTIVITIES OF PROSECUTOR'S OFFICES

Білозьорова Л.В.
здобувач
Науково-дослідний інститут публічного права
ORCID ID: 0009-0002-0822-8715

Статтю присвячено комплексному аналізу юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури в адміністративно-правовому вимірі. Розкрито поняття, сутність і особливості відповідальності в інформаційній сфері, визначено систему її елементів (суб'єкти, об'єкти, підстави, види), теоретично обґрунтовано правовий статус «загальних» та «спеціальних» суб'єктів із урахуванням чотириланкової організаційної побудови прокуратури та особливого режиму Спеціалізованої антикорупційної прокуратури. Показано, що нормативно-правові засади відповідальності формуються у взаємодії зовнішнього законодавства й внутрішніх організаційних актів, які детально регламентують процедури роботи з відомчими інформаційними системами (ЄРДР, система електронного документообігу, аналітичні підсистеми). Обґрунтовано видову палітру відповідальності (дисциплінарна, адміністративна, цивільно-правова, кримінальна) та її кореляцію з інституційним статусом суб'єктів. Запропоновано модель «норма – організація – інформаційно-правова технологія – відповідальність», що забезпечує персоніфікацію обов'язків і доказоспроможність правопорушень через процесуальну фіксацію дій у реєстрах та прозоре оприлюднення внутрішніх актів. Практичне значення визначається системою реалістичних напрямів удосконалення: нормативним вдосконаленням існуючих юридичних актів, розмежуванням критичних функцій і доступів, посиленням методичного нагляду, спеціальним процедурним режимом для САП, а також «доказоспроможними» вимогами до роботи в ЄРДР, системі електронного документообігу й аналітичних підсистемах. Додатково запропоновано операціоналізовані механізми внутрішнього контролю, що уможливлюють уніфікацію дисциплінарної практики та зниження деліктних ризиків. Результати можуть бути використані для вдосконалення відомчих регламентів, підготовки методичних матеріалів і підвищення кваліфікації працівників органів прокуратури, а також для подальших доктринальних досліджень у сфері адміністративного права та інформаційної безпеки публічної влади.

Ключові слова: адміністративне право, юридична відповідальність, органи прокуратури, інформаційно-правове забезпечення, суб'єкти інформаційного забезпечення, ЄРДР, електронний документообіг, внутрішні організаційні акти, Спеціалізована антикорупційна прокуратура.

The article is devoted to a comprehensive analysis of the legal responsibility of the subjects of information and legal support of the activities of the prosecutor's office in the administrative-legal dimension. The concept, essence and features of responsibility in the information sphere are revealed, the system of its elements (subjects, objects, grounds, types) is determined, the legal status of «general» and «special» subjects is theoretically substantiated, taking into account the four-level organizational structure of the prosecutor's office and the special regime of the Specialized Anti-Corruption Prosecutor's Office. It is shown that the regulatory and legal principles of responsibility are formed in the interaction of external legislation and internal organizational acts, which regulate in detail the procedures for working with departmental information systems (ERDR, electronic document management system, analytical subsystems). The specific palette of responsibility (disciplinary, administrative, civil law, criminal) and its correlation with the institutional status of subjects are substantiated. The model "norm – organization – information and legal technology – responsibility" is proposed, which ensures the personification of duties and the provability of offenses through procedural recording of actions in registers and transparent publication of internal acts. The practical significance is determined by a system of realistic directions for improvement: regulatory improvement of existing legal acts, delimitation of critical functions and accesses, strengthening of methodological supervision, a special procedural regime for the SAP, as well as "provable" requirements for work in the ERDR, the electronic document management system and analytical subsystems. Additionally, operationalized internal control mechanisms are proposed, which enable the unification of disciplinary practice and reduction of tort risks. The results can be used to improve departmental regulations, prepare methodological materials and improve the skills of prosecutors, as well as for further doctrinal research in the field of administrative law and information security of public authorities.

Key words: administrative law, legal liability, prosecutor's offices, information and legal support, subjects of information support, ERDR, electronic document flow, internal organizational acts, Specialized Anti-Corruption Prosecutor's Office.

У сучасному інформаційному суспільстві, коли інформація виступає одним із ключових ресурсів держави, суспільства й особи, виникає нагальна потреба у чіткому правовому регулюванні інформаційної діяльності, захисті інформаційних прав, свобод і законних інтересів. Паралельно з цим стає все більш актуальною проблема юридичної відповідальності за порушення в інформаційно-правовій сфері, тобто за дії чи бездіяльність, що пов'язані із створенням, обробкою, зберіганням, поширенням або захистом інформації. Інформаційно-правова відповідальність (інколи вживаний термін «інформаційно-правова відповідальність» як окремий різновид юридичної відповідальності) є складовою системи адміністративно-правового, забезпечення державної політики у сфері інформаційної безпеки, правового режиму інформації та діяльності публічних органів. У контексті діяльності органів прокуратури, органів публічного управління й контролю це завдання набуває особливої ваги, оскільки забезпечення інформаційно-правового супроводу таких органів передбачає високі стандарти професійної поведінки, охорони службової інформації, доступу до публічної інформації, захисту персональних даних та інших складових інформаційного права.

У загальному розумінні юридична відповідальність – це належно встановлена нормами права публічна реакція держави на протиправну поведінку суб'єкта, яка порушує правовий порядок, права й законні інтереси інших осіб або держави, супроводжується заходами державно-примусового характеру й має на меті відновлення порушеного стану або попередження нових правопорушень [1, с. 79].

Сутність юридичної відповідальності можна розглядати як соціально-правове явище, яке має кілька ключо-

вих функцій: каральну (реагування на правопорушення), превентивну (запобігання майбутнім порушенням), відновлювальну (відновлення порушених прав або стану), навчально-виховну (формування правосвідомості).

У сфері інформаційних відносин юридична відповідальність набуває спеціалізованих рис, особливо в контексті дисциплінарної та адміністративної відповідальності, вона стосується правопорушень в інформаційній сфері зокрема неправомірного використання, розголошення, спотворення, втрати або несанкціонованого доступу до інформації [2, с. 83].

Так, під терміном «інформаційно-правова відповідальність» більшість дослідників розуміють особливий вид юридичної відповідальності, що виникає саме внаслідок порушень у сфері інформаційно-правового регулювання. З погляду К. Ю. Ісмайлова, інформаційно-правова відповідальність розкривається як «система заходів примусового характеру, передбачених чинним законодавством, що призводять до притягнення порушника інформаційного законодавства до певних обмежень в інформаційних правах і свободах» [3, с. 88].

На нашу думку, вона вирізняється з інших видів юридичної відповідальності такими ознаками: а) спеціалізований предмет-об'єкт правового регулювання – інформаційна діяльність, інформаційні правовідносини, інформація як ресурс, інформаційні системи; б) тісний зв'язок із технологіями обробки, зберігання та передачі інформації; в) високий динамізм змін у нормативно-технологічному середовищі, що ставить нові передумови і ризики порушень; г) значна суспільна значущість – інформація є засобом управління, контролю, комунікації, тому порушення прав і обов'язків у цій сфері може мати суттєві наслідки для держави, суспільства та особи. Отже, інформаційно-правова відповідальність є похідним, але самостійним елементом юридичної відповідальності, яка враховує особливості інформаційного простору.

Крім того, ми вважаємо, що у розумінні юридичної відповідальності в інформаційно-правовій сфері сутність формується через такі складові:

1. Підстава відповідальності – це настання протиправної поведінки, а саме порушення зобов'язання, здійснення неправомірної дії чи бездіяльності, що заподіяло або могло заподіяти шкоду чи ризик інформаційним правам, інформаційній безпеці або ресурсам. Наприклад, в інформаційній сфері це може бути несанкціонований доступ до бази даних, виток або порушення порядку обробки персональних даних, обіг службової інформації без дозволу [4, с. 44].

2. Умови застосування відповідальності – це наявність правової норми, відповідної процедурної можливості притягнення до відповідальності, встановлення винної поведінки (винуватість суб'єкта), причинного зв'язку між дією/бездіяльністю та наслідком. У інформаційній сфері це ускладнюється технологічною природою інформаційних систем, складністю доказування зв'язку між порушенням та шкодою, а також мультиаспектністю інформаційних правовідносин.

3. Ефект відповідальності – це санкції та наслідки, що наступають для порушника (штраф, обмеження доступу, адміністративні стягнення, дисциплінарні заходи, цивільно-правове відшкодування тощо). У сфері інформаційної діяльності ефект також може включати заборону здійснювати певну інформаційну діяльність, відключення від інформаційної системи, позбавлення права доступу до службової інформації.

Відтак, сутність юридичної відповідальності в інформаційно-правовій сфері полягає у тому, що вона становить інституціоналізований спосіб реагування держави і системи публічного управління на порушення інформаційно-правових норм, із метою відновлення правового порядку, захисту інформаційних прав і безпеки та попередження нових порушень.

Крім того, серед основних особливостей юридичної відповідальності в інформаційно-правовій сфері можна виокремити:

1 Динаміка інформаційного середовища і ризики – це розвиток інформаційних технологій, цифровізації, глобалізації обігу інформації, активне використання електронних комунікацій, що породжує нові форми правопорушень. Ця динаміка створює такі юридично-правові виклики: а) складність ідентифікації порушення та винуватої особи; б) необхідність адаптації законодавства та правозастосування до нових технологій; в) ризик значних масштабів шкоди або потенційної шкоди. Відтак, юридична відповідальність має бути передбачливою, гнучкою, зорієнтованою на технологічні реалії.

2. Мультигалузевий характер і спеціалізація – полягає в тому, що інформаційно-правова відповідальність охоплює правопорушення, які можуть бути предметом адміністративного, кримінального, цивільного, дисциплінарного права, вона має мультигалузевий характер.

3. Превентивна спрямованість та адміністративно-правова форма – оскільки наслідки інформаційних порушень можуть бути значними і складними для відновлення, важливо використовувати відповідальність не лише як каральний механізм, але як стимул до дотримання норм, вдосконалення інформаційної політики, управління ризиками. Таким чином, адміністративно-правова форма відповідальності (штраф, попередження, обмеження доступу) часто є пріоритетною для оперативного реагування. У цьому сенсі вона служить засобом публічного управління.

4. Врахування інформаційної безпеки та права на інформацію – оскільки інформаційно-правова діяльність має подвійний характер, забезпечення права на інформацію та одночасно захист інформаційної безпеки, юридична відповідальність в цій сфері повинна враховувати баланс між відкритістю і захистом. Відповідальність може бути застосована як за утиск права на доступ до публічної інформації, так і за порушення вимог захисту інформації чи персональних даних.

На сьогоднішній день на нормативному рівні чинний Дисциплінарний статут прокуратури України (Постанова ВРУ № 1796-XII від 06.11.1991) врегульовує лише загальні підстави заохочення і дисциплінарної відповідальності працівників органів прокуратури, порядок провадження та види стягнень, але фактично не містить спеціалізованих норм щодо відповідальності саме за порушення у сфері інформаційно-правового забезпечення (неналежне ведення ЄРДР, збої в електронному документообігу, порушення режимно-секретних вимог, роботи з персональними даними тощо). Статут окреслює загальний «процедурний каркас» дисциплінарної практики (порядок заохочень і притягнення до відповідальності), однак не прив'язує склад проступків і санкції до конкретних інформаційних процесів і ролей, що відповідає реаліям 1991 року, але не відбиває сучасної цифрової інфраструктури прокуратури. Показово, що навіть у пізніших редакціях спеціальних інформаційних деліктів не виокремлено, а окремі норми визнавалися неконституційними (ч. 2 ст. 16) без оновлення змісту з урахуванням нових інформаційних режимів. Це створює регуляторний розрив між загальним дисциплінарним інструментарієм Статуту та фактичними ризиками цифрових процесів у прокуратурі, що й зумовлює потребу у детальному нормуванні інформаційних обов'язків і відповідальності у відомчих актах або оновленій редакції Статут) [5].

У контексті діяльності органів прокуратури інформаційно-правове забезпечення охоплює такі аспекти: збір, обробка та аналіз інформації у межах оперативно-аналітичної, правозастосовної, процесуальної діяльності; організація інформаційних систем і баз даних; забезпечення правового режиму доступу, збереження, передачі інфор-

мації. У цьому сенсі правопорушення можуть виникати на етапах створення, обробки, передачі або зберігання інформації, що прямо стосується діяльності органів прокуратури [6, с. 93].

У свою чергу варто відзначити, що в класичному розумінні юридична відповідальність містить такі складові правопорушення: суб'єкт відповідальності, об'єкт відповідальності, підстава настання відповідальності, санкція (наслідок) та процедура її застосування. Розглянемо базові компоненти системи юридичної відповідальності у досліджуваній сфері.

Суб'єкти відповідальності – це ті особи (фізичні чи юридичні), які здійснюють інформаційно-правове забезпечення діяльності органів прокуратури або беруть участь у такій діяльності. Це можуть бути працівники органів прокуратури, інформаційні служби, оператори інформаційних систем, адміністратори баз даних, зовнішні підрядники. Як правило, суб'єктами є посадові особи або інші уповноважені особи, які мають доступ до інформаційних ресурсів і здійснюють відповідні дії [7, с. 90].

Об'єктом відповідальності – є порушення встановлених правових норм у сфері інформаційно-правового забезпечення, наприклад: несанкціонований доступ до даних, недотримання вимог щодо захисту інформації, порушення порядку обробки чи передачі інформації, виток інформації, розголошення службової чи допрофільної інформації, порушення процедур аудиту чи контролю інформаційно-аналітичної діяльності.

Підстави відповідальності – це протиправні дії або бездіяльність суб'єкта, який мав/має виконати обов'язок щодо забезпечення інформаційної діяльності органів прокуратури, і настання юридично визначених наслідків (санкцій). Наприклад, в Україні Дисциплінарний статут прокуратури України та чинне законодавство у сфері доступу до публічної інформації, захисту персональних даних, правил роботи інформаційно-аналітичних підрозділів органів прокуратури створюють правове підґрунтя для відповідальності [8, с. 75].

Види відповідальності – у межах адміністративно-правового спрямування це дисциплінарна чи адміністративна відповідальність, а у деяких випадках матеріальна відповідальність, а за умови тяжких порушень, кримінальна. Водночас важливо окремо розглядати адміністративну відповідальність за порушення інформаційного законодавства, наприклад, ст. 172-8 Кодексу України про адміністративні правопорушення (КУпАП) – «Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень» [9].

Отже, система юридичної відповідальності в сфері інформаційно-правового забезпечення органів прокуратури формується за загальними засадничими принципами юридичної відповідальності, але також має свою спеціалізовану підсистему з урахуванням характеру інформаційних правовідносин.

У свою чергу, в контексті функціонування органів прокуратури України інформаційно-правове забезпечення поступово набуває рис автономного організаційно-правового напряму, що перетинається із ключовими сферами публічного управління, цифрової трансформації та забезпечення верховенства права. Особливу увагу в цьому зв'язку заслуговує розкриття теоретико-правового змісту та структурної побудови правового статусу суб'єктів інформаційного забезпечення діяльності органів прокуратури як важливої складової їх функціонального потенціалу.

З огляду на завдання, закріплені у внутрішніх положеннях і наказах, суб'єктів інформаційного забезпечення доцільно розмежувати на загальних і спеціальних.

Загальні суб'єкти – це усі прокурори та державні службовці органів прокуратури, які у щоденній роботі створюють, обробляють і використовують інформацію та працюють із відомчими інформаційними системами.

Спеціальні суб'єкти – це працівники підрозділів, на яких покладено організацію, адміністрування, методичний супровід і контроль інформаційних систем та діловодних процесів: Департамент інформаційних технологій Офісу Генерального прокурора, Департамент документального забезпечення Офісу Генерального прокурора, а також управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи (разом із відповідними структурними одиницями в обласних прокуратурах) [10]. Саме ці підрозділи формують «ядро» спеціальної інформаційної компетенції системи.

Що стосується компетенції загальних суб'єктів, то правовий статус прокурорів усіх рівнів є єдиним, незалежно від посади чи місця роботи в системі. У площині інформаційного забезпечення це означає правомірне створення, фіксацію, використання, захист і передачу даних із дотриманням спеціальних режимів доступу, установлених законами та внутрішніми актами (зокрема щодо електронного документообігу та роботи з державними інформаційними ресурсами). Для державних службовців органів прокуратури компетенція визначається законодавством про державну службу та внутрішніми положеннями, що деталізують діловодні, архівні, комунікаційні та технічні операції в межах ІС «СЕД», ІАС «ОСОП» та інших систем.

Тоді, як на рівні спеціальних суб'єктів, а саме: 1) Департамент інформаційних технологій – забезпечує інформатизацію всіх напрямів діяльності органів прокуратури, впровадження та супроводження відомчих інформаційних систем, технічний захист інформації, експлуатацію програмно-апаратних комплексів, IP-телефонію, відеоконференцзв'язок, адміністрування мереж, функціонування центрів обробки даних, а також організаційне та методичне супроводження електронних довірчих послуг (кваліфікований електронний підпис, печатка); 2) Департамент документального забезпечення – визначає єдиний порядок документування управлінської інформації та ведення діловодства в органах прокуратури: правила підготовки документів, облік, зберігання, використання і знищення носіїв, організація електронного документообігу (ІС «СЕД»), взаємодія в системі електронної взаємодії органів виконавчої влади, а також філологічне редагування службових документів, у т.ч. з обмежувальними грифами. На рівні областей ці функції реалізують відділи документального забезпечення; 3) Управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи – виконує завдання з організації ведення ЄРДР, формування та аналізу статистики кримінальної протиправності, розроблення спільно з органами досудового розслідування системи та методики обліку кримінальних правопорушень і руху проваджень, інтеграції ЄРДР з іншими державними реєстрами, гармонізації статистики з європейськими стандартами, а також забезпечує надання відомостей із Реєстру у визначених законом випадках. Вони не лише виконують власні дії, а й задають обов'язкові правила та забезпечують їх дотримання іншими підрозділами, що підсилює вимір юридичної відповідальності за неналежну організацію процесів. Це утворює центр відповідальності за достовірність і повноту даних, які прямо впливають на здійснення прокурорських функцій.

Адміністративно-правовий статус суб'єктів інформаційно-правового забезпечення є невід'ємною складовою режиму функціонування відомчих інформаційних систем. Центральне місце посідає ЄРДР (адміністрування, доступ, наповнення, надання відомостей), а також ІС «СЕД» (електронний документообіг), ІАС «ОСОП» (звітність та аналітика), «Кадри-WEB» (кадрові процеси) та інші системи. Визначальними є: а) регламентований доступ (на підставі службових документів і ролей); б) технічний і криптогра-

фічний захист (у тому числі в сегменті кваліфікованих електронних довірчих послуг); в) процедури тестування, впровадження, супроводження та навчання користувачів; г) інтеграція з іншими державними реєстрами та міжнародними платформами (у межах визначених повноважень).

Крім того, варто відзначити, адміністративно-правовий статус суб'єктів інформаційного забезпечення конкретизується на кожному рівні:

1. Офіс Генерального прокурора – це нормотворчі (внутрішні) і координаційні повноваження, затвердження актів із питань внутрішньої організації, у т.ч. електронного документообігу, а також оприлюднення наказів та набрання ними чинності за процедурою, що гарантує публічність і правову визначеність.

2. Спеціалізована антикорупційна прокуратура (САП) – це інституційна самостійність і функціональна незалежність у межах єдиної системи, а саме власні підрозділи документообігу, режимно-секретної роботи, управління персоналом, внутрішнього контролю; окреме розміщення та особливий режим погодження адміністративних наказів, що стосуються організації діяльності САП.

3. Обласні прокуратури – це управління й відділи, компетенція та штат у межах повноважень, а саме керівник області реалізує представницькі, організаційні, кадрові та контрольні повноваження, у т.ч. щодо інформаційно-аналітичного забезпечення.

4. Окружні прокуратури – це первинна ланка, де функції інформаційного забезпечення зосереджені на веденні статистики, діловодстві, роботі в системах, а також взаємодії з обласним рівнем.

У свою чергу варто відзначити, що оскільки інформаційно-правове забезпечення реалізується через юридично значущі дії з даними (створення, внесення до ЄРДР, оприлюднення відкритих даних, ведення діловодства, збереження носіїв, застосування КЕП тощо), міра відповідальності є органічною частиною правового статусу. Вона випливає з: 1) посадових інструкцій і положень про підрозділи (визначають персональну й колективну відповідальність за процеси); 2) наказів (установлюють стандарти та процедури); 3) режимних вимог (державна таємниця, службова інформація, захист персональних даних); 4) обов'язків користувача (доступ, збереження ключів, коректність внесення даних, дотримання строків і повноти звітності).

Проте, для «спеціальних» суб'єктів підстави юридичної відповідальності посилюються їх адміністративно-організаційною роллю: вони несуть відповідальність не лише за власні дії, а й за методичне керівництво, контроль і супровід інформаційних процесів у системі. Така конструкція унеможливлює розмивання відповідальності та забезпечує простежуваність управлінських рішень.

Підсумовуючи, адміністративно-правовий статус суб'єктів інформаційного забезпечення органів прокуратури доцільно моделювати як інтегральну систему чотирьох взаємопов'язаних блоків: 1) Норма – зовнішні (закон) та внутрішні (накази, положення) регулятори, що визначають завдання і процедури; 2) Організація – структурні рівні й підрозділи, посадові ролі, підпорядкованість, координація; 3) Інформаційно-правова технологія – як засіб захисту від витоків інформації; 4) Відповідальність – персоніфікована (посадова), організаційна (підрозділу), процедурна (дотримання регламентів), режимна (таємниця, персональні дані). Саме поєднання цих блоків забезпечує правову визначеність, керованість і відповідальність інформаційної діяльності на всіх рівнях – від Офісу до окружної ланки та САП.

Так наприклад до інформаційно-правових технологій, як засобів захисту від витоків інформації можна віднести такі способи, як: 1. Системи запобігання витокам (DLP) – це інструмент реалізації внутрішніх приписів (наказів, положень) щодо обмеження виведення службових відомостей за периметр, наприклад: автоматичне виявлення і блокування передачі даних, контроль каналів (електронна пошта, веб, носії), перевірка вмісту на ознаки конфіденційності/таємниці; 2. Шифрування даних – виконує роль правового режиму збереженості, навіть у разі несанкціонованого доступу вміст захищається, а ключі/сертифікати закріплюються за посадовими особами. Для відомчих систем (ЄРДР, СЕД, ІАС «ОСОП») це означає окремі процедури керування ключами, обов'язок негайного повідомлення про компрометацію, а також можливість визначити вид відповідальності при порушенні правил зберігання/використання крипто засобів; 3. Автентифікація та контроль доступу – мінімізує ризик зловживань обліковими записами, а рольовий доступ (за посадою/функцією) забезпечує принцип необхідного мінімуму і розмежування критичних операцій (створення – перевірка – затвердження запису). Такі механізми легко вбудовуються у посадові інструкції та внутрішні процедури, утворюючи чіткий зв'язок між обсягом прав доступу та мірою юридичної відповідальності; 4. Моніторинг і аналіз активності користувачів – спрямований на превенцію та фіксацію інцидентів, зокрема, відстеження нетипових дій, масових вивантажень, спроб обійти політики доступу, фіксація часу, місця та суб'єкта дії. У правовому вимірі це забезпечує доказоспроможність дисциплінарних проваджень і можливість індивідуалізувати вину; 5. Політики безпеки це організаційні заходи для всіх наведених технологій, наприклад, навчання, інструктажі, тестування доступів, стандарти обігу документів у СЕД, правила класифікації/маркування й архівації, порядок реагування на інциденти. Саме такі політики переводять технічні вимоги у сферу службових обов'язків і дисциплінарної відповідальності, забезпечуючи єдність практики між Офісом, областями, округами та САП і надаючи керівникам легітимні підстави для управлінських рішень у разі загрози витоку.

У свою чергу варто відзначити, що юридична відповідальність суб'єктів, що забезпечують інформаційно-правову діяльність органів прокуратури, формується на основі визначеного комплексу нормативно-правових актів, що встановлюють їх правовий статус, повноваження, обов'язки, а також порядок притягнення до відповідальності у разі порушення встановлених вимог.

Базовий рівень становлять норми Закону України «Про прокуратуру» № 1697-VII, які визначають систему органів (Офіс Генерального прокурора; обласні; окружні; САП), єдність організаційних засад та єдиний статус прокурорів [11]. Саме через цю інституційну рамку конкретизуються повноваження посадових осіб і встановлюються формальні процедури видання внутрішніх актів (наказів), їх оприлюднення й набрання чинності, як загальні передумови правомірної діяльності та подальшої юридичної відповідальності у разі відхилення від стандартів.

До блоку зовнішнього регулювання, на який прямо орієнтовано внутрішні положення та інструкції органів прокуратури, належать: Кримінальний процесуальний кодекс України; Закон України «Про інформацію»; Закон України «Про доступ до публічної інформації»; Закон України «Про захист персональних даних»; Закон України «Про державну таємницю»; Закон України «Про електронні документи та електронний документообіг». Їх приписи інтегруються у відомчі процедури (робота в ЄРДР; електронний документообіг у СЕД; застосування кваліфікованих електронних довірчих послуг; захист інформації), задаючи нормативні межі поведінки та види можливих порушень.

Окреме місце у зовнішньому регулюванні посідає Дисциплінарний статут прокуратури України, затверджений Постановою Верховної Ради України № 1796-XII від 06.11.1991, який визначає загальні підстави дисци-

плінарної відповідальності прокурорських працівників, види дисциплінарних стягнень, порядок їх застосування та процедури провадження. Хоча Статут виконує функцію «процедурного каркасу» дисциплінарної практики, він переважно не містить спеціалізованих норм щодо складів проступків, пов'язаних із порушенням правил роботи у відомчих інформаційних системах (ЄРДР, система електронного документообігу, аналітичні підсистеми), режимно-секретних вимог чи використання електронних довірчих послуг. Відтак деталізація відповідальності за такі порушення логічно переноситься до внутрішньоорганізаційних актів (наказів і положень), що конкретизують обов'язки на рівні посад і підрозділів.

Другий, внутрішній блок – становить система організаційно-розпорядчих актів Генерального прокурора (накази про затвердження положень про самостійні структурні підрозділи) і підпорядкованих керівників (обласного, окружного рівня, керівника САП). Ці акти деталізують завдання, функції, процедури доступу й адміністрування інформаційних систем (ЄРДР, ІС «СЕД», ІАС «ОСОП», «Кадри-WEB»), правила документообігу, режимно-секретної роботи, статистичного обліку та звітності і є прямими «носіями» юридичних обов'язків працівників. Невиконання або неналежне виконання таких обов'язків утворює підставу юридичної відповідальності відповідно до закону й внутрішніх актів.

Залежно від характеру порушення суб'єкти інформаційного забезпечення можуть нести такі види відповідальності, зокрема:

1. Дисциплінарна відповідальність – це порушення внутрішніх регламентів, наказів і посадових інструкцій щодо інформаційної діяльності (неналежне внесення даних до ЄРДР; порушення строків і правил реєстрації/руху документів у СЕД; невиконання вимог режимно-секретної роботи; недотримання політик доступу; неналежне використання кваліфікованого електронного підпису/печатки). Нормативно ця відповідальність випливає із поєднання Закону України «Про прокуратуру» та конкретизується наказами про підрозділи й відповідними положеннями [12, с. 11].

2. Адміністративна відповідальність – виникає у випадках порушення загальнообов'язкових правил інформаційної діяльності поза межами суто службової підлеглості, наприклад, у ст. 212-5 Кодексу України про адміністративні правопорушення за порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв, що містять службову інформацію [9]. Такі проступки охоплюють, зокрема, неналежну реєстрацію/маршрутизацію документів, порушення строків архівації, неправильне проставлення грифів, самовільне копіювання чи винесення носіїв. Підстави та межі визначаються законами про інформацію, державну таємницю, електронні документи, а також відомчими регламентами, що конкретизують порядок доступу, обліку і зберігання.

3. Матеріальна відповідальність – як окремий вид в межах адміністративної відповідальності, можлива у разі спричинення шкоди внаслідок протиправних дій з інформацією (наприклад, розголошення інформації з обмеженим доступом, що спричинило збитки, або несвоєчасне/неналежне внесення даних, яке призвело до негативних майнових наслідків). Фактичні обов'язки й стандарти належної поведінки формалізовані у внутрішніх положеннях і наказах, вони слугують критеріями належної професійної діяльності.

4. Кримінальна відповідальність – настає за порушення режиму державної таємниці, несанкціоноване втручання в роботу інформаційних систем, підроблення електронних підписів/документів чи інші діяння, що криміналізовані загальним законодавством та становлять окрему категорію деліктів (статті 361, 361-1, 361-2, 362, 363, 363-1, 364 КК України) [13]. Відомчі акти, що регулюють ЄРДР, СЕД, ІАС «ОСОП», роботу КЕП і режимні вимоги, виконують превентивну роль, а також слугують доказовою базою щодо наявності/відсутності службових обов'язків та їх порушення.

5. Інформаційно-правова відповідальність – хоча в чинному законодавстві України вона прямо не виокремлена, як самостійний інститут, проте дедалі частіше розглядається у доктринальному контексті як міждисциплінарний вид відповідальності, що охоплює специфіку регулювання відносин щодо захисту інформації в цифровому середовищі.

У практичному вимірі такої діяльності органів прокуратури вона реалізується у правовідносинах між: а) володільцями/розпорядниками службової інформації (Офіс Генерального прокурора, обласні та окружні прокуратури, САП; адміністратори відомчих систем) і користувачами цієї інформації (прокурори, державні службовці, уповноважені працівники); б) між розпорядниками персональних даних і суб'єктами персональних даних; в) між керівниками підрозділів і підлеглими, які зобов'язані дотримуватися встановлених режимів доступу, зберігання, передачі та архівації відомостей. Саме в цих точках контакту, виникають підстави притягнення до відповідальності за порушення внутрішніх регламентів, режимно-секретних вимог, вимог щодо персональних даних та правил експлуатації ЄРДР/СЕД/ІАС «ОСОП», що знаходить нормативну опору у зовнішніх актах (закони про інформацію, доступ, персональні дані, держтаємницю, електронні документи) та у внутрішніх організаційних актах органів прокуратури.

У межах практичного функціонування органів прокуратури юридична відповідальність реалізується, насамперед, через внутрішні процедури контролю за діяльністю підрозділів – на підставі щорічних звітів, перевірок, службових розслідувань. Зокрема, невиконання норм щодо збереження конфіденційності інформації у Департаменті документального забезпечення або в управлінні ЄРДР, у разі настання шкідливих наслідків, тягне за собою дисциплінарні або інші санкції.

До того ж варто відзначити, що система наказів Генерального прокурора про затвердження положень самостійних структурних підрозділів Офісу (зокрема: про Департамент інформаційних технологій; Департамент документального забезпечення; Управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи; підрозділи з охорони державної таємниці; комунікацій з громадськістю; міжнародного співробітництва; тощо) виконує три ключові функції: 1) нормативізує обов'язки (хто, що і як зобов'язаний робити з даними та системами); 2) розмежовує повноваження і відповідальність (адміністратор, користувач, контролер, методист); 3) забезпечує контрольованість (встановлює звітність, моніторинг, аудит, статистичні процедури, погодження). Порушення кожного з цих елементів може бути кваліфіковано за відповідним видом юридичної відповідальності залежно від тяжкості і наслідків. Адже належне дотримання стандартів юридичної відповідальності є критично важливим в умовах воєнного стану, коли значна частина оброблюваної інформації має обмежений доступ або стосується досудових розслідувань у справах державної безпеки.

Крім того, з огляду на структуру компетенцій і технологічні контури діяльності, підвищений ризик утворення деліктів найбільше може спостерігатися у таких структурних елементах:

1. ЄРДР – це: а) несвоєчасне, неповне або недостовірне внесення відомостей; б) порушення методики обліку та правил надання інформації; в) несанкціоновані дії з реєстром; г) неналежне адміністрування доступів. Об'єктивна сторона пов'язана з відступом від єдиних стандартів обліку/звітності, а суб'єктивна з недбалістю,

перевищенням доступу чи свідомим спотворенням даних. Норми щодо організації ведення ЄРДР, визначення єдиного порядку звітності, розвитку ІАС «ОСОП» і впровадження нових цифрових продуктів (як складників екосистеми обліку) окреслюють критерії належної поведінки та, відповідно, підстави відповідальності у випадку їх порушення;

2. СЕД – це: а) порушення строків реєстрації та маршрутизації документів; б) відсутність належної реєстрації; в) недотримання правил оформлення; г) втрата/псування електронних та матеріальних носіїв; ґ) порушення архівування та знищення документів. Оскільки порядок електронного документообігу закріплюється внутрішніми актами Генерального прокурора (із обов'язковим оприлюдненням і набранням чинності у визначеному порядку), будь-який відступ від цих вимог має правову значущість і тягне персональну відповідальність відповідного суб'єкта

3. ІАС «ОСОП» і статистика – це: а) виробництво недостовірної статистики; б) відступ від методики; в) порушення принципу статистичної конфіденційності; г) невідповідність єдиному порядку формування звітності. Відповідальність активується в разі, коли процедурно визначені правила формування адміністративних даних і аналітики не виконані, що спотворює інформаційні підстави рішень керівництва Офісу та регіональних ланок;

4. КЕП і електронні довірчі послуги – це: а) неналежне зберігання особистих ключів; б) передання засобів підпису третім особам; в) використання підпису поза межами повноважень; г) компрометація ключів. Хоч технологічний супровід екосистеми забезпечується профільними підрозділами (у межах загальної ІТ-інфраструктури системи прокуратури), персоніфікований обов'язок використовувати КЕП належним чином лежить на кожному користувачеві, а відтак і персональна відповідальність за порушення;

5. Режимно-секретна діяльність і персональні дані – це: а) неправомірний доступ; б) розголошення; в) неналежне зберігання й облік носіїв; г) порушення класифікації; ґ) несанкціонований обмін інформацією між рівнями системи. Зміст режимно-секретних і кадрових функцій закріплено у структурі САП та інших ланок (окремі підрозділи, окремі приміщення, внутрішній контроль, управління персоналом), що посилює обов'язок дотримання режимів і підвищує відповідальність у разі порушення (включно з кримінально-правовою оцінкою найтяжчих випадків);

Сукупно окреслені структурні елементи показують, що доказова база для притягнення до відповідальності формується «зсередини» процесу, через журналювання операцій у ЄРДР/СЕД/аналітичних системах, офіційне оприлюднення і чинність наказів, документовані регламенти доступів і процедурні карти процесів, які детермінують як належну, так і протиправну поведінку.

Виходячи із всього вище сказаного, можна з упевненістю констатувати, що загальні суб'єкти (усі прокурори, державні службовці) несуть відповідальність за коректність, повноту, своєчасність і правомірність інформаційних операцій, від внесення даних у ЄРДР до реєстрації документів у СЕД і роботи зі статистикою в ІАС «ОСОП». Вони діють у межах єдиного статусу прокурора (незалежно від адміністративної посади) і підпорядковуються уніфікованим внутрішнім актам.

Тоді, як спеціальні суб'єкти додатково відповідають за організацію та методичне керівництво процесами, а саме: впровадження та супроводження інформаційних систем; адміністрування доступів; технічний і криптографічний захист; виробництво та гармонізацію статистики; підготовку і навчання користувачів; інтеграцію з іншими державними реєстрами; відповідність європейським стандартам звітності; забезпечення функціонування центрів обробки даних і каналів зв'язку; дотримання процедур оприлюднення відкритих даних. Відтак їхній обсяг юридичної відповідальності включає організаційний компонент – за належну архітектуру, стабільність і контрольованість інформаційних процесів у всій системі.

Крім того варто відзначити, система документування (СЕД), регламентований доступ і логування операцій у ЄРДР, стандарти формування звітності в ІАС «ОСОП», правила зберігання та знищення носіїв, політики застосування КЕП, а також офіційне оприлюднення наказів та їх набрання чинності – це ключові процесуальні гарантії, що слугують як превенції, так і доказовій базі при вирішенні питань притягнення до відповідальності (дисциплінарної, адміністративної, цивільно-правової або кримінальної). Вони забезпечують трасованість управлінських рішень, перевірюваність дій користувачів і адміністраторів та відтворюваність процедур, що є необхідними ознаками належного врядування у публічній адміністрації.

Виходячи із цього ми з упевненістю можемо визначити, що юридична відповідальність суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури – це закріплений у законодавстві та внутрішніх нормативно-правових актах інститут державного примусу, що передбачає застосування до працівників (прокурорів, державних службовців та інших осіб), які здійснюють інформаційно-правове та технічне забезпечення діяльності органів прокуратури, правових санкцій (адміністративного, дисциплінарного, матеріальна або кримінального характеру) у випадку порушення ними встановлених правил обігу інформації, регламентів роботи з інформаційними системами, стандартів захисту службової, персональної та іншої захищеної інформації, з метою відновлення законності, забезпечення належного функціонування інформаційної інфраструктури прокуратури, запобігання правопорушенням та підтримки інформаційної безпеки у межах виконання повноважень.

У свою чергу, що стосується основного питання досліджуваної проблематики то ми вважаємо, що формування дієвого механізму юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України становить важливий аспект розвитку інформаційної безпеки, цифрового управління та належного правозастосування в умовах гібридних викликів. Особливої актуальності це питання набуває з огляду на міждисциплінарний характер інформаційно-правового забезпечення, в якому перетинаються інформаційне, адміністративне, кримінальне, дисциплінарне та процесуальне право [14].

На сьогодні в національному законодавстві не закріплено чіткої конструкції юридичної відповідальності саме суб'єктів інформаційно-правового забезпечення органів прокуратури, що породжує прогалини, правову невизначеність і підвищує ризики інформаційних порушень. На нашу думку, ключ до підвищення правової визначеності та підзвітності в інформаційній діяльності органів прокуратури – це послідовне оновлення правил, організації та технологій, через які реалізуються обов'язки «загальних» і «спеціальних» суб'єктів (прокурори, державні службовці. Вихідною базою для такого оновлення є чинна інституційна архітектоніка системи (Офіс Генерального прокурора – область – округ – САП) та перелік внутрішніх положень/наказів, якими вже деталізовано функції, процедури і стандарти роботи з ЄРДР, СЕД, ІАС «ОСОП», «Кадри-WEB».

Першочергово, удосконалення має відбуватися за такими принципами:

1. Принцип «статус – обов'язок – відповідальність»: кожен елемент правового статусу суб'єкта (посада, підрозділ, рівень організаційної ієрархії) повинен бути безпосередньо пов'язаний із визначеним переліком інформаційних обов'язків і відповідною мірою юридичної відповідальності. Такий підхід передбачає чітку відпо-

відність між функціональним місцем суб'єкта в структурі прокуратури й обсягом його відповідальності – дисциплінарної, адміністративної, цивільно-правової чи кримінальної. Особливої уваги потребує забезпечення цієї кореляції з урахуванням єдиного статусу прокурора, визначеного законом, а також спеціалізованих функцій «особливих» суб'єктів – наприклад, аналітиків, працівників служб безпеки інформації або адміністраторів баз даних;

2. Принцип вертикальної узгодженості – система інформаційно-правового забезпечення прокуратури має бути побудована за принципом єдності підходів до тлумачення обов'язків і форм юридичної відповідальності на всіх рівнях організаційної структури – від центрального (Офіс Генерального прокурора) до регіонального (обласні прокуратури), окружного (місцеві прокуратури) та спеціалізованого (Спеціалізована антикорупційна прокуратура). Водночас слід зберігати процесуальну автономію окремих підрозділів, зокрема САП, у частині специфіки інформаційного режиму та організації цифрових процесів.

3. Принцип техніко-юридичної відповідальності – технічні регламенти й інформаційні протоколи (системи логування, порядок надання доступу, кваліфіковані електронні підписи, механізми архівації, внутрішні та міжвідомчі інтеграції) повинні набувати юридичного значення як засобів персоніфікації обов'язків суб'єктів інформаційного забезпечення. У цьому аспекті технічна інфраструктура розглядається не як нейтральне середовище, а як інструмент фіксації правопорушень, встановлення відповідальної особи, юридичної оцінки інформаційної дії або бездіяльності.

У зв'язку з цим концептуальними напрямками удосконалення юридичної відповідальності суб'єктів інформаційно-правового забезпечення органів прокуратури можуть бути:

1. Нормативне вдосконалення існуючих юридичних актів, які регулюють обов'язки і відповідальність співробітників органів прокуратури:

1) Доцільно доповнити Дисциплінарний статут прокуратури України окремим розділом 4 «Дисциплінарна відповідальність прокурорських і слідчих працівників за інформаційні проступки», у якому: а) закріпити визначення інформаційного проступку (неналежне зберігання, оброблення, передання/розповсюдження, розкриття, знищення службової інформації; порушення режимно-секретних вимог; недотримання правил роботи з ЄРДР, СЕД, ІАС «ОСОП», недбале поводження з носіями криптографічних ключів; використання невстановлених каналів обміну; б) установити типологію проступків за ступенем тяжкості (незначні, істотні, грубі) з прив'язкою до наслідків і повторюваності; в) передбачити процесуальні гарантії (фіксація подій у журналах систем, право на пояснення, перевірка, мотивоване рішення). Одночасно до статті 9 Статуту обґрунтовано додати новий вид дисциплінарного стягнення – тимчасову заборону доступу до окремих видів службової інформації (у т.ч. до сегментів ЄРДР/СЕД/ІАС «ОСОП», до відомостей з обмеженим доступом), із визначенням строків такого обмеження, підстав (ступінь ризику повторного порушення), процесуальних умов (перегляд, дострокове скасування) та технічних наслідків (блокування облікових записів, скасування або реверсія ролей доступу, перевидача засобів підпису).

2) Доцільним видається загальне оновлення положень, що регулюють відповідальність за незаконне використання службової інформації та порушення правил її обліку, зберігання і використання (зокрема у статтях 172-8 та 212-5 КУпАП), у бік чіткішого та уніфікованого охоплення всіх працівників правоохоронних органів і прирівняних до них суб'єктів, а також працівників органів прокуратури.

3) До кожного чинного положення і наказу щодо ЄРДР, ІС «СЕД», ІАС «ОСОП» внести додатки з покроковим описом операцій та закріпленням відповідальної посадової особи на кожній стадії (створення, реєстрація, перевірка, затвердження, надання відомостей, архівація). Це безпосередньо корелює з покладеними на профільні підрозділи функціями організаційного забезпечення ведення Реєстру, єдиного порядку звітності та документування управлінської інформації.

4) У кожному наказі (та його змінах) обов'язково фіксувати спосіб офіційного оприлюднення та момент набрання чинності (з урахуванням вимоги оприлюднення державною мовою наступного робочого дня). Це усуває сумнів у обов'язковості норм і спрощує кваліфікацію відступів як дисциплінарних проступків.

5) Запровадити стислий офіційний виклад змін до внутрішніх правил електронного документообігу з чітким зазначенням, як змінюються обов'язки конкретних посад. Такий «пояснювальний блок» підвищує передбачуваність і доказовість у провадженнях про відповідальність.

2. Укріплення методичного центру та вертикальної узгодженості:

1) Запровадити щоквартальні вибіркові перевірки регіональних практик внесення відомостей до ЄРДР і формування звітності з боку управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи (за ротаційним планом відбору областей/округів), із обов'язковим складанням акта-висновку та пропозицій щодо корекції локальних інструкцій. Такий формат мінімізує навантаження на управління, зберігаючи методичний вплив і відповідність визначеним завданням щодо розвитку ЄРДР/ІАС «ОСОП» та встановлення єдиного порядку звітності.

2) Передбачити щомісячну взаємозвірку даних, внесених до ЄРДР та ІАС «ОСОП», між управлінням організаційного забезпечення ведення ЄРДР та інформаційно-аналітичної роботи й відповідними структурними підрозділами обласного/окружного рівнів як превентивний захід для недопущення порушень (із фіксацією виявлених розбіжностей та наданням рекомендацій для їх оперативного усунення).

3. Доказоспроможність процесів у ЄРДР, ІС «СЕД», ІАС «ОСОП»:

1) Установити мінімальні вимоги до журналів фіксації дій користувачів: незмінність записів, часові позначки, ідентифікація посадової особи, перелік обов'язкових «подій-сигналів» (прострочення, повторні виправлення, нестандартні операції).

2) Для ІАС «ОСОП» затвердити показники своєчасності, повноти та коректності звітності (пороги відхилень; порядок автоматичного формування переліку порушень для службової перевірки), що логічно випливає з централізованої ролі цього підрозділу у виробництві адміністративних даних.

4. Розмежування функцій у критичних операціях:

1) У СЕД заборонити суміщення функцій «реєстрація документа» і «контроль маршруту» однією особою, а в ІАС «ОСОП» розмежувати виробника статистики й внутрішнього перевіряльника. Це унеможливлює конфлікт інтересів та підвищує індивідуалізацію відповідальності.

2) Нормативно закріпити типові профілі доступу (користувач, перевіряльник, адміністратор) до ЄРДР, ІС «СЕД», ІАС «ОСОП» з чіткими обов'язками та відповідальністю, включно з режимом зберігання засобів електронного підпису.

5. Підвищення правової визначеності у застосуванні кваліфікованого електронного підпису:

1) Уточнити в положеннях Департаменту інформаційних технологій та Департаменту документального забезпечення персональні обов'язки щодо зберігання носіїв ключів, негайного повідомлення про втрату/компрометацію, а також підстави обмеження доступу до систем у разі порушення цих вимог.

2) Увести періодичне підтвердження компетентності користувачів (короткий навчальний модуль і тест у відомчих системах), результати якого фіксувати в «КадриWEB» і враховувати при визначенні міри відповідальності.

6. Режимно-секретна діяльність і простежуваність обігу інформації:

1) Оновити внутрішні регламенти щодо обміну матеріалами, які містять службову/таємну інформацію, між ланками системи (Офіс – область – округ – САП), закріпивши точки контролю, відповідальних і строки виконання на кожній стадії.

2) У СЕД і в паперовому діловодстві встановити обов'язкові позначки про місце зберігання, термін тимчасового зберігання, відповідального за видачу/повернення; фіксувати порушення як підставу для дисциплінарної відповідальності з урахуванням наслідків.

3) Уточнити порядок підготовки та передання документів до архівних установ (зокрема ЦДАВО), щоб строковість і комплектність виступали вимірюваними критеріями належної поведінки відповідальних осіб.

7. Внутрішній контроль і реагування на інциденти:

1) Для кожної системи (ЄРДР, ІС «СЕД», ІАС «ОСОП») затвердити внутрішній порядок реагування: виявлення порушення → фіксація події → повідомлення керівника → перевірка → висновок про вид відповідальності → реалізація рішення. Кожну стадію персоніфікувати.

2) Визначити перелік порогових показників (прострочення реєстрації, частка виправлених записів, невідповідність довідникам), при перевищенні яких автоматично ініціюється службова перевірка керівником відповідного підрозділу.

3) Результати перевірок обов'язково відображати у щоквартальних звітах Офісу та обласних прокуратур; звіти мають містити пропозиції щодо корекції локальних інструкцій і посадових обов'язків.

8. Посилення ролі документального забезпечення:

1) Запровадити щомісячні огляди правильності маршрутизації в ІС «СЕД» і складати зведений перелік типових помилок для навчання і запобігання повторенням.

2) Визначити спеціальний електронний порядок редагування службових документів за допомогою цифрових інформаційних сиситем (включно з обмежувальними грифами), де фіксується відповідальність за лінгвістичну точність і коректність посилань на правові акти.

9. Узгодження з організаційними повноваженнями керівників ланок:

1) Для керівників обласних і окружних прокуратур затвердити перелік обов'язків щодо контролю за статистикою, діловодством, інформаційним забезпеченням та строками виконання, що логічно випливає з їхніх управлінських повноважень (організація діяльності, видання актів, призначення і контроль).

2) Встановити, що невжиття керівником заходів реагування на виявлені порушення інформаційної дисципліни розглядається як самостійна підстава для дисциплінарної відповідальності керівника.

Підсумовуючи здійснене обґрунтування, вважаємо, що запропонована система вдосконалення юридичної відповідальності суб'єктів інформаційно-правового забезпечення органів прокуратури являє собою цілісну конструкцію, у якій нормативна детермінація операційних обов'язків, організаційне розмежування ролей і процедурне забезпечення доказовості правопорушень інтегровані в єдину вертикаль управління та контролю. Її наукова новизна полягає у поєднанні «тонкого» персоніфікування відповідальності на рівні конкретних дій у ЄРДР, системі електронного документообігу та аналітичних підсистемах із «грубої» інституційною прив'язкою до повноважень керівників і спеціалізованих підрозділів, включно з особливим режимом САП. Практичний сенс такої моделі полягає в трансформації інформаційних технологій і внутрішніх регламентів на інструменти правової визначеності: кожна дія стає вимірюваною, кожна роль – відповідальною, кожен відступ – юридично кваліфікованим. У підсумку досягається системний ефект: скорочення простору управлінської дискреції без належного обґрунтування, уніфікація правозастосування між рівнями, зростання превентивного потенціалу внутрішнього контролю та, як наслідок, підвищення довіри до прокуратури як до інституту, що діє на засадах законності, публічної підзвітності та належного урядування.

Висновки. Узагальнюючи результати дослідження, слід констатувати, що юридична відповідальність суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури є системним інститутом адміністративного права, який функціонує на перетині нормотворчих (зовнішніх і внутрішніх), організаційно-управлінських і процесуальних механізмів. Її сутність розкривається через поєднання публічно-владного характеру реагування держави на порушення в інформаційній сфері та спеціалізованих режимів роботи з відомчими інформаційними системами (ЄРДР, система електронного документообігу, аналітичні підсистеми), що обумовлює персоніфікацію обов'язків і кореляцію відповідальності з правовим статусом суб'єктів. Сформульована структура (суб'єкти, об'єкти, підстави, види) і теоретично обґрунтований правовий статус «загальних» та «спеціальних» суб'єктів у межах єдиної вертикалі органів прокуратури дають змогу цілісно описати межі належної поведінки й критерії протиправності, а також забезпечити доказоспроможність рішень завдяки офіційно оприлюдненим внутрішнім актам, процедурній фіксації дій у реєстрах та простежуваності управлінських процедур. Такий підхід узгоджує превентивну, відновлювальну та каральну функції відповідальності із завданнями публічного управління, підсилює правову визначеність і уніфікує правозастосування на всіх рівнях – від Офісу Генерального прокурора до базової ланки та САП.

Отже, запропоновані напрями вдосконалення (нормативне вдосконалення існуючих юридичних актів, розмежування ролей і доступів у критичних операціях, підвищення «доказоспроможності» процесів, спеціальний режим для САП, методичний нагляд і внутрішній контроль) трансформують технічні регламенти й інформаційні протоколи у правові інструменти персональної підзвітності. Це мінімізує управлінську дискрецію без належного обґрунтування, знижує ризики деліктів у «вузлах» інформаційної діяльності, забезпечує єдність статистики та діловодства, а відтак підвищує якість адміністративно-процесуального забезпечення функцій прокуратури й довіру до її діяльності як до інституції, що діє за стандартами законності, публічної підзвітності та належного урядування.

ЛІТЕРАТУРА

1. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ: КВІЦ, 2019. 344 с. URL: https://dspace.nlu.edu.ua/handle/123456789/16729

2. Федоренко Т. В., Садковський С. П. Юридична відповідальність в інформаційній сфері: поняття та особливості. *Часопис Київського університету права*. 2022. (2-4) С. 82-85.

3. Ісмайлов К. Ю. Інформаційно-правова відповідальність в Україні. *Правовий часопис Донбасу.* 2018. № 3 (64). С. 87–93. URL: https://ljd.dnuvs.in.ua/wp-content/uploads/2022/01/13-ismajlov.pdf.

4. Катрич Є. О. Відповідальність за правопорушення в інформаційній сфері. Робота на здобуття рівня магістра ; спец. 081 «Право». Миколаїв : НУК. 2020. 87 с. URL: https://eir.nuos.edu.ua/items/c6af05a8-cc37-4fea-a46e-e10ca4ffa5b7

5. 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

6. Савчук Р. М. Інформаційно-аналітична діяльність органів прокуратури у сфері протидії злочинності: теоретичні та організаційно-правові аспекти. *Дніпровський науковий часопис публічного управління, психології, права.* 2022. № 5. С. 90–94. URL: https://www.chasopys-ppp.dp.ua/index.php/chasopys/article/view/309/271

7. 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.

8. Dubynskyy O., Dubynskyi I., Markin, S. Features of financial and legal liability in Ukraine. *Baltic Journal of Economic Studies,* 2024. 10(1). 72-79. URL: http://www.baltijapublishing.lv/index.php/issue/article/view/2313

9. Кодекс України про адміністративні правопорушення (статті 1 – 212-24) : Кодекс України від 07.12.1984 № 8073-X : станом на 1 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text

10. Структура Офісу Генерального прокурора. Головна – Офіс Генерального прокурора. URL: https://gp.gov.ua/ua/posts/struktura-struktura-ofisu-generalnogo-prokurora-zatverdzhena-nakazom-generalnogo-prokurora-vid-21-12-2019-no-99-shc

11. 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

12. Дисциплінарна відповідальність прокурорів в Україні / О. Банчук, М. Каменєв, Є. Крапивін, Б. Малишев, В. Петраковський, М. Цапок. – К.: Москаленко О. М., 2019. 140 с. URL: https://pravo.org.ua/wp-content/uploads/2024/10/1548703302disciplinary-responsibility-of-prosecutors-in-ukraine_ukr.pdf

13. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

14. Костенко С. К. Дисциплінарна відповідальність прокурорів: національна практика та міжнародний досвід. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2025. № 73. С. 112–116. URL: https://vestnik-pravo.mgu.od.ua/archive/juspradenc73/23.pdf.

Дата першого надходження рукопису до видання: 17.08.2025
Дата прийнятого до друку рукопису після рецензування: 20.09.2025
Дата публікації: 26.09.2025