

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ВИННИЧЕНКА**

*Кваліфікаційна наукова праця
на правах рукопису*

БІЛОЗЬОРОВА ЛЮДМИЛА ВОЛОДИМИРІВНА

УДК 342.9

ДИСЕРТАЦІЯ

**ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ
ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ**

12.00.07 - адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Л. В. Білозьорова

АНОТАЦІЯ

Білозьорова Л. В. Інформаційно-правове забезпечення діяльності органів прокуратури України. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Науково-дослідний інститут публічного права, Центральноукраїнський державний університет імені Володимира Винниченка, Кропивницький, 2025.

У дисертаційному дослідженні проведено комплексний адміністративно-правовий аналіз та запропоновано вирішення наукових і практичних проблем, пов'язаних із формуванням та реалізацією інформаційно-правового забезпечення діяльності органів прокуратури України в умовах трансформації публічного управління та цифровізації правосуддя. Перший розділ присвячено методологічним засадам такого забезпечення, що дало змогу розкрити його зміст як самостійного, багаторівневого й функціонально орієнтованого правового інституту у структурі адміністративного права та системи органів публічної влади. На основі системного, функціонального, структурно-логічного й формально-юридичного підходів уточнено базові наукові категорії та закладено теоретичну основу для подальшого дослідження спеціальних адміністративно-правових механізмів інформаційної діяльності органів прокуратури.

Здійснено поглиблений аналіз сутності та особливостей інформаційно-правового забезпечення діяльності органів прокуратури України. Розкрито теоретико-правові засади цього феномену, простежено генезис і становлення інформаційно-правового забезпечення в системі публічного управління, показано еволюцію уявлень про роль інформації та правових режимів її обігу в діяльності органів, наділених владними повноваженнями. Уточнено зміст категорії «інформаційно-правове забезпечення» у тісному зв'язку з конституційно визначеними функціями органів прокуратури, їх процесуальними, адміністративними та позапроцесуальними повноваженнями, що дозволило

тракувати інформаційно-правове забезпечення не як допоміжний, а як системоутворюючий компонент організації й реалізації прокурорської діяльності. Розроблено типологію інформаційних потоків у межах адміністративно-правової діяльності органів прокуратури, виділено нормативно-регулятивний, процесуально-кримінальний, управлінсько-організаційний, аналітико-статистичний, комунікаційний та безпековий сегменти, показано їх взаємозумовленість та вплив на якість реалізації публічних функцій.

Окремий акцент зроблено на інформаційній безпеці в системі органів прокуратури та правових запобіжниках витоку, маніпулювання чи спотворення відомостей, що циркулюють у службовому інформаційному просторі. Проаналізовано підходи до оцінювання ризиків, пов'язаних з обігом службової, конфіденційної та персональної інформації, узагальнено наявні правові інструменти їх зниження, зокрема дисциплінарно-правові, адміністративно-деліктні, організаційно-правові та техніко-юридичні засоби. Показано, що забезпечення інформаційної безпеки є інтегративною складовою інформаційно-правового забезпечення, оскільки поєднує в собі вимоги законності, дотримання прав людини, умов конфіденційності, збереження службової таємниці та стійкість електронної інфраструктури органів прокуратури.

Досліджено мету, принципи та завдання інформаційно-правового забезпечення діяльності органів прокуратури України як ключові системоутворюючі категорії, що визначають характер адміністративно-правового режиму цієї діяльності. Окреслено понятійно-категоріальну характеристику термінів «мета», «принцип», «завдання» в теорії права та адміністративно-правовій доктрині, розкрито їхню роль у конструюванні ефективної моделі публічного управління в прокурорській сфері. Сформульовано мету інформаційно-правового забезпечення як створення цілісної, узгодженої та прозорої системи правових, організаційних і технологічних засобів, які гарантують законний, безпечний та результативний обіг інформації в органах прокуратури. Систематизовано принципи інформаційно-правового забезпечення (законність, верховенство права, відкритість і прозорість, пропорційність

обмежень, захист персональних даних, технологічна надійність, підзвітність службових осіб), а також окреслено завдання, що конкретизують ці принципи у практичній площині (нормативне регулювання, організація інформаційних процесів, забезпечення доступу до публічної інформації, захист інформаційних прав людини, протидія інформаційним загрозам, розвиток цифрових сервісів тощо).

Розкрито нормативно-правові засади інформаційно-правового забезпечення діяльності органів прокуратури України. Обґрунтовано теоретико-правову природу інформаційного забезпечення як правового інституту, визначено його місце в системі адміністративного законодавства та спеціального прокурорського регулювання. Сформульовано методологічні підходи до розуміння категорії «нормативно-правові засади» у контексті інформаційної діяльності органів прокуратури, показано їх зв'язок із функціональними особливостями інформації як елемента управлінської дії. Визначено інституційно-правові та організаційні засади регламентації інформаційних процесів: статус органів прокуратури, їх повноваження у сфері доступу до інформації, обміну даними з іншими органами, ведення реєстрів і баз даних, забезпечення захисту інформації й персональних даних.

Проаналізовано систему нормативно-правових актів, що закріплюють основні засади інформаційного забезпечення діяльності органів прокуратури, з виокремленням конституційно-правового, законодавчого, підзаконного та міжнародно-правового рівнів. У цьому контексті визначено основні проблеми та напрями вдосконалення нормативно-правового регулювання відносин з питань інформаційно-правового забезпечення діяльності органів прокуратури України.

У другому розділі дисертаційного дослідження здійснено комплексне обґрунтування адміністративно-правового механізму інформаційно-правового забезпечення діяльності органів прокуратури України, у межах якого було здійснено розкриття його внутрішньої структури, видового наповнення, рівневої організації та суб'єктного складу. На основі узагальнення чинного законодавства, підзаконних нормативних актів та практики функціонування

органів прокуратури запропоновано цілісну наукову модель інформаційно-правового забезпечення як особливого різновиду адміністративно-правового регулювання, що охоплює класифікацію його видів, визначення рівнів та напрямів, характеристику адміністративно-правових форм і методів, а також адміністративно-правового статусу суб'єктів, які забезпечують організацію та реалізацію інформаційних процесів у зазначеній сфері діяльності.

Обґрунтовано підхід до видового розмежування інформаційно-правового забезпечення діяльності органів прокуратури України. Аналіз показав, що без науково вивіреної класифікації видів інформаційно-правового забезпечення неможливо ані адекватно описати, ані ефективно модернізувати відповідні управлінські процеси. На цій основі сформульовано й розкрито декілька взаємопов'язаних класифікацій: функціональну, за джерелом і походженням інформації, за правовим режимом і рівнем доступу та за формою реалізації й ступенем стандартизації. Показано, що така багатовимірна класифікація дозволяє систематизувати інформаційно-правові інструменти, зменшити хаотичність інформаційних потоків і закласти підґрунтя для їх подальшої цифрової стандартизації.

Досліджено рівні та напрями інформаційно-правового забезпечення діяльності органів прокуратури України як ключові параметри адміністративно-правового механізму. З'ясовано методологічне підґрунтя розмежування категорій «рівень» і «напрямок» та запропоновано їх адаптацію до специфіки прокурорської організації. Обґрунтовано, що системний розподіл рівнів та напрямів підвищує керованість, дозволяє більш раціонально розподіляти ресурси, уникати дублювання функцій та чіткіше визначати відповідальність конкретних посадових осіб за стан інформаційних процесів.

Досліджено адміністративно-правові форми і методи інформаційно-правового забезпечення діяльності органів прокуратури України. У роботі запропоновано уточнені визначення понять «форма» і «метод» в інформаційно-правовому забезпеченні та показано, що жодна форма діяльності органів прокуратури не є нейтральною з правової точки зору, оскільки завжди втілює

певний метод адміністративно-правового впливу. Виокремлено основні адміністративно-правові форми інформаційно-правового забезпечення та основні методи. Показано, як взаємодія форм і методів структурує інформаційний простір органів прокуратури, впливає на прозорість, передбачуваність і підзвітність їх діяльності та забезпечує баланс між відкритістю інформації і необхідними правовими обмеженнями.

Проаналізовано адміністративно-правовий статус суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України, що дозволило перейти від абстрактної моделі механізму до його персоніфікації в межах реальної інституційної структури. Розкрито поняття, сутність і правову природу суб'єктів інформаційно-правового забезпечення, виокремлено основні теоретико-методологічні підходи до їх визначення. Сформовано систему суб'єктів, до якої віднесено Офіс Генерального прокурора, Спеціалізовану антикорупційну прокуратуру, обласні й окружні прокуратури, їх структурні підрозділи та окремих посадових осіб, наділених спеціальними повноваженнями у сфері організації, ведення й захисту інформаційних ресурсів. Проаналізовано адміністративно-правовий статус кожної ланки суб'єктів. Охарактеризовано нормативно-правове регулювання та структурно-функціональну організацію інформаційно-правового забезпечення в Офісі Генерального прокурора.

У третьому розділі дисертаційного дослідження обґрунтовано напрями вдосконалення інформаційно-правового забезпечення діяльності органів прокуратури України як складового елемента сучасного адміністративно-правового механізму публічного управління у сфері правосуддя. Здійснено комплексний аналіз зарубіжного досвіду інформаційно-правового забезпечення діяльності прокуратури країн Європейського Союзу з акцентом на французьку та польську моделі. Розкрито методологічні підходи до дослідження європейського досвіду та окреслено європейську модель інформаційно-правового регулювання діяльності органів прокуратури, яка ґрунтується на поєднанні принципів верховенства права, захисту прав людини, прозорості діяльності та високих стандартів інформаційної безпеки. Охарактеризовано джерела європейського

інформаційного права у сфері діяльності прокуратури, проаналізовано організацію прокуратури у Франції та Польщі, висвітлено особливості їх інформаційно-правового забезпечення (регламентація доступу до інформації, ведення електронних реєстрів, стандарти розкриття відомостей, гарантії конфіденційності). Проведено порівняльний аналіз французького й польського досвіду та сформульовано напрями його адаптації до українських реалій.

Розглянуто перспективи формування інформаційно-правових технологій діяльності органів прокуратури України в контексті цифровізації публічного управління. З'ясовано вплив цифрової трансформації на зміну змісту та форм реалізації повноважень органів прокуратури, показано, що сучасні електронні платформи, реєстри, аналітичні системи й сервіси електронної взаємодії стають не лише технічними засобами, а й елементами адміністративно-правового режиму. Уточнено категоріально-понятійний апарат, пов'язаний із інформаційно-правовими технологіями, та запропоновано авторське бачення їх структури й функціонального призначення в органах прокуратури. Сформульовано систему авторських перспектив, серед яких: розвиток єдиних інтегрованих інформаційно-аналітичних платформ, удосконалення електронного документообігу, впровадження інструментів автоматизованого моніторингу дотримання строків і процедур, розширення відкритих даних, посилення кіберзахисту та запровадження внутрішніх комплаєнс-механізмів щодо обігу службової та конфіденційної інформації.

На теоретико-правовому рівні визначено поняття, зміст і структуру нормативно-правової бази у цій сфері, окреслено методологічні підходи до її аналізу та модернізації. Досліджено сучасний стан законодавчого, підзаконного та відомчого регулювання інформаційних процесів в органах прокуратури, а також роль міжнародно-правових джерел та механізмів їх імплементації. У роботі запропоновано «карту процесів і ролей», яка відображає, які саме суб'єкти й на яких етапах обробляють інформацію, де розташовані ключові точки ризику витоків або спотворення відомостей, які запобіжники вже існують та які потребують додаткового нормативного закріплення. Виокремлено основні

проблеми нормативно-правової бази (фрагментарність, колізійність, нечіткість процедур, недостатня регламентація електронних форм взаємодії), а також сформульовано напрями й механізми її вдосконалення: систематизація й гармонізація актів, уточнення повноважень органів прокуратури в інформаційній сфері, посилення стандартів захисту персональних даних, унормування електронного документообігу та міжвідомчого обміну даними, закріплення більш деталізованих процедур доступу до публічної інформації.

Проаналізовано особливості юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України. Сформовано поняття та розкрито сутність юридичної відповідальності в інформаційно-правовій сфері, визначено її об'єкти, суб'єкти, підстави та види. На основі теоретичного обґрунтування правового статусу суб'єктів інформаційного забезпечення органів прокуратури систематизовано види юридичної відповідальності (дисциплінарна, адміністративна, цивільно-правова, у визначених випадках – кримінальна) та їх нормативні підстави. Проаналізовано співвідношення статусу та відповідальності «загальних» і «спеціальних» суб'єктів, зокрема посадових осіб, які мають розширений доступ до інформаційних ресурсів і несуть підвищений рівень обов'язків щодо їх належного використання й захисту. Окрему увагу приділено судовій та квазісудовій (дисциплінарній) практиці у сфері порушення правил обігу інформації, що дало змогу виявити характерні тенденції правозастосування, типові порушення та прогалини в правовому регулюванні, а також окреслити потребу в уточненні складів інформаційних проступків і вдосконаленні процедур притягнення до відповідальності.

Ключові слова: інформаційно-правове забезпечення, органи прокуратури України, адміністративно-правовий механізм, публічне управління, інформаційна діяльність, адміністративно-правовий режим, суб'єкти, інформація, відповідальність, електронні реєстри, електронний документообіг, цифровізація, інформаційно-правові технології, міжнародні стандарти, кіберзахис, інформаційні ресурст.

SUMMARY

Bilozorova L. V. Information and legal support for the activities of the prosecutor's office of Ukraine. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Candidate of Legal Sciences in the specialty 12.00.07 "Administrative law and process; financial law; information law". Scientific Institute of Public Law, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, 2025.

The dissertation research conducted a comprehensive administrative and legal analysis and proposed solutions to scientific and practical problems related to the formation and implementation of information and legal support for the activities of the prosecutor's office of Ukraine in the context of the transformation of public administration and the digitalization of justice. The first section is devoted to the methodological principles of such support, which made it possible to reveal its content as an independent, multi-level and functionally oriented legal institution in the structure of administrative law and the system of public authorities. Based on the systemic, functional, structural-logical and formal-legal approaches, the basic scientific categories were clarified and a theoretical basis was laid for further research into special administrative and legal mechanisms for the information activities of the prosecutor's office.

An in-depth analysis of the essence and features of the information and legal support for the activities of the prosecutor's office of Ukraine was carried out. The theoretical and legal foundations of this phenomenon are revealed, the genesis and formation of information and legal support in the public administration system are traced, the evolution of ideas about the role of information and legal regimes of its circulation in the activities of bodies vested with power is shown. The content of the category "information and legal support" is specified in close connection with the constitutionally defined functions of prosecutorial bodies, their procedural, administrative and extra-procedural powers, which allowed to interpret information

and legal support not as an auxiliary, but as a system-forming component of the organization and implementation of prosecutorial activities. A typology of information flows within the administrative and legal activities of prosecutorial bodies is developed, the normative and regulatory, procedural and criminal, managerial and organizational, analytical and statistical, communication and security segments are highlighted, their interdependence and impact on the quality of the implementation of public functions are shown.

A special emphasis is placed on information security in the system of prosecutors' offices and legal safeguards against leakage, manipulation or distortion of information circulating in the official information space. Approaches to assessing risks associated with the circulation of official, confidential and personal information are analyzed, and the available legal instruments for their reduction are summarized, in particular disciplinary and legal, administrative and tortious, organizational and legal and technical and legal means. It is shown that ensuring information security is an integrative component of information and legal support, since it combines the requirements of legality, observance of human rights, confidentiality conditions, preservation of official secrets and the stability of the electronic infrastructure of prosecutors' offices. The purpose, principles and tasks of information and legal support for the activities of prosecutors' offices of Ukraine are studied as key system-forming categories that determine the nature of the administrative and legal regime of this activity. The conceptual and categorical characteristics of the terms "goal", "principle", "task" in legal theory and administrative law doctrine are outlined, their role in constructing an effective model of public administration in the prosecutor's office is revealed. The goal of information and legal support is formulated as the creation of a holistic, coordinated and transparent system of legal, organizational and technological means that guarantee the legal, safe and effective circulation of information in prosecutor's offices. The principles of information and legal support are systematized (legality, rule of law, openness and transparency, proportionality of restrictions, protection of personal data, technological reliability, accountability of officials), and the tasks that specify these principles in the practical plane are outlined (regulatory

regulation, organization of information processes, ensuring access to public information, protection of human information rights, counteraction to information threats, development of digital services, etc.).

The normative and legal principles of information and legal support for the activities of the prosecutor's office of Ukraine are revealed. The theoretical and legal nature of information support as a legal institution is substantiated, its place in the system of administrative legislation and special prosecutorial regulation is determined. Methodological approaches to understanding the category of "normative and legal principles" in the context of the information activities of the prosecutor's office are formulated, their connection with the functional features of information as an element of managerial action is shown. The institutional and legal and organizational principles of regulating information processes are determined: the status of the prosecutor's office as subjects of power, their powers in the field of access to information, data exchange with other bodies, maintaining registers and databases, ensuring the protection of information and personal data. The system of normative and legal acts that establish the basic principles of information support for the activities of the prosecutor's office is analyzed, with the separation of the constitutional and legal, legislative, subordinate and international legal levels. In this context, the main problems and directions for improving the regulatory and legal regulation of relations on the issues of information and legal support of the activities of the prosecutor's office of Ukraine are identified.

In the second section of the dissertation research, a comprehensive justification of the administrative and legal mechanism of information and legal support of the activities of the prosecutor's office of Ukraine is carried out, within the framework of which its internal structure, specific content, level organization and subject composition were disclosed. Based on the generalization of current legislation, subordinate regulations and the practice of functioning of the prosecutor's office, a holistic scientific model of information and legal support as a special type of administrative and legal regulation is proposed, which includes the classification of its types, the definition of levels and directions, the characteristics of administrative and legal forms and methods, as well as the administrative and legal status of subjects that

ensure the organization and implementation of information processes in the specified field of activity.

An approach to the specific delimitation of information and legal support of the activities of the prosecutor's office of Ukraine is substantiated. The analysis showed that without a scientifically verified classification of types of information and legal support, it is impossible to adequately describe or effectively modernize the relevant management processes. On this basis, several interrelated classifications were formulated and revealed: functional, by source and origin of information, by legal regime and level of access, and by form of implementation and degree of standardization. It was shown that such a multidimensional classification allows systematizing information and legal tools, reducing the chaos of information flows and laying the foundation for their further digital standardization. The levels and directions of information and legal support of the activities of the prosecutor's office of Ukraine as key parameters of the administrative and legal mechanism were studied. The methodological basis for the distinction between the categories "level" and "direction" was clarified and their adaptation to the specifics of the prosecutor's organization was proposed. It is substantiated that the systematic distribution of levels and directions increases manageability, allows for a more rational allocation of resources, avoids duplication of functions and more clearly defines the responsibility of specific officials for the state of information processes.

The administrative-legal forms and methods of information-legal support of the activities of the prosecutor's office of Ukraine are studied. The paper proposes refined definitions of the concepts of "form" and "method" in information-legal support and shows that no form of activity of the prosecutor's office is neutral from a legal point of view, since it always embodies a certain method of administrative-legal influence. The main administrative-legal forms of information-legal support and the main methods are identified. It is shown how the interaction of forms and methods structures the information space of the prosecutor's office, affects the transparency, predictability and accountability of their activities and ensures a balance between the openness of information and the necessary legal restrictions.

The administrative and legal status of the subjects of information and legal support of the activities of the prosecutor's office of Ukraine was analyzed, which allowed us to move from an abstract model of the mechanism to its personification within the framework of a real institutional structure. The concept, essence and legal nature of the subjects of information and legal support were revealed, and the main theoretical and methodological approaches to their definition were identified. A system of subjects was formed, which includes the Prosecutor General's Office, the Specialized Anti-Corruption Prosecutor's Office, regional and district prosecutor's offices, their structural divisions and individual officials endowed with special powers in the field of organization, management and protection of information resources. The administrative and legal status of each level of subjects was analyzed. The regulatory and legal regulation and structural and functional organization of information and legal support in the Prosecutor General's Office were characterized, which allowed us to show how the general models developed in the dissertation are materialized in specific organizational decisions and internal regulations.

The third section of the dissertation research substantiates the directions for improving the information and legal support of the activities of the prosecutor's office of Ukraine as a component of the modern administrative and legal mechanism of public administration in the field of justice. A comprehensive analysis of foreign experience in the information and legal support of the activities of the prosecutor's office of the European Union countries is carried out with an emphasis on the French and Polish models. Methodological approaches to the study of European experience are revealed and a European model of information and legal regulation of the activities of the prosecutor's office is outlined, which is based on a combination of the principles of the rule of law, protection of human rights, transparency of activities and high standards of information security. The sources of European information law in the field of prosecutor's office activities are characterized, the organization of the prosecutor's office in France and Poland is analyzed, and the features of their information and legal support are highlighted (regulation of access to information, maintenance of electronic registers, standards for disclosure of information, guarantees of confidentiality). A

comparative analysis of the French and Polish experience was conducted and directions for its adaptation to Ukrainian realities were formulated.

The prospects for the formation of information and legal technologies for the activities of the prosecutor's office of Ukraine in the context of the digitalization of public administration were considered. The impact of digital transformation on changing the content and forms of implementation of the powers of the prosecutor's office was clarified, it was shown that modern electronic platforms, registers, analytical systems and electronic interaction services are becoming not only technical means, but also elements of the administrative and legal regime. The categorical and conceptual apparatus associated with information and legal technologies was clarified, and the author's vision of their structure and functional purpose in the prosecutor's office was proposed. A system of author's perspectives has been formulated, including: the development of unified integrated information and analytical platforms, improvement of electronic document flow, introduction of automated monitoring tools for compliance with deadlines and procedures, expansion of open data, strengthening of cyber protection and introduction of internal compliance mechanisms for the circulation of official and confidential information.

At the theoretical and legal level, the concept, content and structure of the regulatory framework in this area have been defined, methodological approaches to its analysis and modernization have been outlined. The current state of legislative, by-law and departmental regulation of information processes in prosecutor's offices has been studied, as well as the role of international legal sources and mechanisms for their implementation. The work proposes a "map of processes and roles", which reflects which entities and at what stages process information, where the key points of risk of leaks or distortion of information are located, which safeguards already exist and which require additional regulatory consolidation. The main problems of the regulatory framework are identified (fragmentation, conflict, unclear procedures, insufficient regulation of electronic forms of interaction), and directions and mechanisms for its improvement are formulated: systematization and harmonization of acts, clarification of the powers of prosecutors' offices in the information sphere, strengthening personal

data protection standards, standardization of electronic document flow and interdepartmental data exchange, and consolidation of more detailed procedures for access to public information.

The features of the legal liability of subjects of information and legal support of the activities of the prosecutor's office of Ukraine are analyzed. The concept is formed and the essence of legal liability in the information and legal sphere is revealed, its objects, subjects, grounds and types are determined. Based on the theoretical substantiation of the legal status of subjects of information support of the prosecutor's office, the types of legal liability (disciplinary, administrative, civil law, in certain cases - criminal) and their regulatory grounds are systematized. The correlation of the status and responsibility of "general" and "special" subjects, in particular officials who have expanded access to information resources and bear an increased level of responsibilities for their proper use and protection, is analyzed. Special attention is paid to judicial and quasi-judicial (disciplinary) practice in the field of violations of information circulation rules, which made it possible to identify characteristic trends in law enforcement, typical violations and gaps in legal regulation, as well as to outline the need to clarify the components of information offenses and improve procedures for bringing them to justice.

Key words: information and legal support, prosecutor's offices of Ukraine, administrative and legal mechanism, public administration, information activity, administrative and legal regime, subjects, information, responsibility, electronic registers, electronic document flow, digitalization, information and legal technologies, international standards, cyber security, information resources.

СПИСОК ОПУБЛІКОВАНИЙ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких висвітлено основні наукові результати дисертації:

1. Білозьорова Л. В. Деякі питання щодо особливостей інформаційно-правового забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2023. № 5. С. 513-522. URL: http://pravoisuspilstvo.org.ua/archive/2023/5_2023/74.pdf

2. Білозьорова Л. В. Основні засади нормативно-правового регулювання інформаційного забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2024. № 2. С. 743-755. URL: http://pravoisuspilstvo.org.ua/archive/2024/2_2024/109.pdf

3. Білозьорова Л. В. Досвід Франції та Польщі щодо інформаційно-правового забезпечення діяльності органів прокуратури. *Knowledge, Education, Law, Management*. 2024. № 7 (67). С. 400-412. URL: <https://kelmczasopisma.com/ua/jornal/94>

4. Білозьорова Л. В. Сучасний адміністративно-правовий механізм інформаційно-правового забезпечення діяльності органів прокуратури України. *Правові новели*. 2024. № 23. С. 563-576. URL: http://legalnovels.in.ua/journal/23_2024/78.pdf

5. Білозьорова Л. В. Суб'єкти інформаційно-правового забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2025. № 2. С. 731-743. URL: http://pravoisuspilstvo.org.ua/archive/2025/2_2025/101.pdf

6. Білозьорова Л. В. Деякі питання удосконалення юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури. *Юридичний науковий електронний журнал*. 2025. № 8. С. 338-346. URL: http://lsej.org.ua/8_2025/72.pdf

7. Білозьорова Л. В. Вдосконалення нормативно-правової бази діяльності органів прокуратури з інформаційно-правового забезпечення. *Правові новели*. 2025. № 26. С. 377-390. URL: http://legalnovels.in.ua/journal/26_2025/45.pdf

які засвідчують апробацію матеріалів дисертації:

8. Білозьорова Л. В. Сучасний погляд на використання інформації з єдиних

і державних реєстрів України представниками слідчих та правоохоронних органів. Сектор безпеки України: актуальні питання науки та практики: збірник наукових статей, тез доповідей та повідомлень за матеріалами XIII Міжнародної науково-практичної конференції (27 березня 2025 року, Національний юридичний університет імені Ярослава Мудрого, м. Харків). У 2-х частинах. Частина 1. Серія «Сектор безпеки України». Вип. 54. Упорядник Мех Ю.В. Харків: Друкарня Мадрид, 2025. С. 15-18.

9. Білозьорова Л. В. Щодо інформаційно-правового забезпечення діяльності органів прокуратури України в умовах цифрової трансформації. Актуальні питання адміністративного права та адміністративного судочинства: збірник наукових статей, тез доповідей та повідомлень за матеріалами II Міжнародної науково-практичної конференції (15 травня 2025 року, Національний юридичний університет імені Ярослава Мудрого, м. Харків). Серія «Сектор безпеки України». Вип.55. Упорядник Мех Ю.В. Харків: Друкарня Мадрид, 2025. С. 12-18.

10. Білозьорова Л. В. Інформаційно-правове забезпечення функціонування прокуратури України: суб'єктний аспект: збірник наукових статей, тез доповідей та повідомлень за матеріалами Мультидисциплінарної науково-практичної конференції «Сучасні тенденції соціально-гуманітарного розвитку суспільства», (3-5 листопада 2025 року, Україна, м. Харків, Німеччина, м. Циттау). Соціально-гуманітарний вісник: зб. наук. пр. Вип. 61. Харків: СГ НТМ «Новий курс», 2025. С. 69.

11. Білозьорова Л. В. Юридична відповідальність суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України: Modern Perspectives on Science and Economic Progress: Collection of Scientific Papers with Proceedings of the 2nd International Scientific and Practical Conference. International Scientific Unity (November 5-7, 2025. Vilnius, Lithuania). P. 230-233.

ЗМІСТ

ВСТУП.....	20
РОЗДІЛ 1. МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ.....	34
1.1. Сутність та особливості інформаційного-правового забезпечення діяльності органів прокуратури України.....	34
1.2. Мета, принципи, завдання інформаційного-правового забезпечення діяльності органів прокуратури України.....	47
1.3. Нормативно-правові засади інформаційного-правового забезпечення діяльності органів прокуратури України.....	61
Висновки до розділу 1.....	75
РОЗДІЛ 2. АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ.....	78
2.1. Види інформаційного-правового забезпеченням діяльності органів прокуратури України.....	78
2.2. Рівні та напрями інформаційного-правового забезпечення діяльності органів прокуратури України.....	91
2.3. Адміністративно-правові форми та методи інформаційного-правового забезпечення діяльності органів прокуратури України.....	107
2.4. Адміністративно-правовий статус суб'єктів інформаційного-правового забезпечення діяльності органів прокуратури України.....	124
Висновки до розділу 2.....	143
РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ.....	146

3.1. Зарубіжний досвід інформаційного-правового забезпечення діяльності прокуратури країн ЄС.....	146
3.2. Перспективи формування інформаційно-правових технологій діяльності органів прокуратури України.....	173
3.3. Напрями вдосконалення законодавчої бази з інформаційного-правового забезпечення діяльності органів прокуратури України.....	183
3.4. Особливості юридичної відповідальності суб'єктів інформаційного-правового забезпечення діяльності органів прокуратури України.....	201
Висновки до розділу 3.....	214
ВИСНОВКИ.....	216
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	225
ДОДАТКИ.....	245

ВСТУП

Обґрунтування вибору теми дослідження. Вибір теми дисертаційного дослідження зумовлений поєднанням кількох взаємопов'язаних чинників – трансформацією системи публічного управління, реформуванням органів прокуратури, стрімким розвитком цифрових технологій та зростанням ролі інформації в реалізації публічної влади. Органи прокуратури в сучасних умовах уже не можуть розглядатися виключно крізь призму кримінально-правових чи процесуальних повноважень. Вони функціонують як особливий суб'єкт публічної адміністрації, чия ефективність безпосередньо залежить від якості організації інформаційних процесів, правового режиму обігу даних, прозорості, підзвітності та належного захисту інформації. За цих умов інформаційно-правове забезпечення набуває статусу системоутворюючого елементу адміністративно-правового статусу органів прокуратури, однак у науці адміністративного права воно досі не отримало комплексного теоретичного осмислення саме в прокурорському зрізі.

Актуальність обраної теми підсилюється тим, що інформаційні відносини, в яких перебувають органи прокуратури, є багатовимірними й конфліктогенними: від доступу до публічної інформації та відкритих даних – до обігу службової інформації, персональних даних, матеріалів досудового розслідування, відомостей, що становлять охоронювану законом таємницю. Відсутність цілісної доктринальної моделі інформаційно-правового забезпечення цієї діяльності призводить до фрагментарності нормативного регулювання, колізій між різними масивами законодавства, неоднакової правозастосовної практики, а інколи – до порушення прав людини в інформаційній сфері. Саме тому звернення до проблематики інформаційно-правового забезпечення діяльності органів прокуратури України з позиції адміністративного права є об'єктивною науковою потребою, що має на меті подолати наявні прогалини та забезпечити систематизацію підходів у цій сфері.

Важливим аргументом на користь обраної теми є європейський вектор розвитку України та поступова інтеграція до єдиного правового простору

Європейського Союзу, де стандарти інформаційної відкритості, захисту персональних даних, прозорості функціонування органів правопорядку та прокуратури набули високого рівня формалізації. У цих умовах постає завдання адаптувати кращі практики і моделі, зокрема у сфері інформаційно-правового регулювання, до національної правової системи.

Сукупність указаних обставин свідчить про високу теоретичну й практичну значущість обраної теми та зумовлює необхідність її ґрунтовного дослідження в межах науки адміністративного права.

Зв'язок теми дисертації із сучасними дослідженнями. У контексті наукового забезпечення теми слід відзначити, що вітчизняні вчені такі, як: О.Ю. Амелін, С.В. Банах, Є.М. Блажівський, Р.І. Богданов, Г.В. Гаврюшенко, С. Г. Гайдай, Л. С. Гандзюк, А. Глущенко, М.В. Григорчук, О.Ю. Дрозд, О.Н. Євтушенко, С. С. Єсімов, І.Б. Жилияєв, Г.М. Зайкіна, К.Ю. Ісмайлов, Є.О. Катрич, М.В. Ковалів, Б.А. Кормич, Р.Б. Левочко, В.В. Лушер, С.В. Мазурик, О.С. Малетова, І.В. Піляй, С.В. Подкопаєв, П.С. Покатаєв, В.С. Політанський, Р.М. Савчук, С.П. Садковський, Г.А. Терещук, Т.В. Федоренко, Є.І. Фролова, А.С. Хомич, В.С. Цимбалюк, Р.В. Шаповал, О.Г. Ярема та інші у своїх працях торкалися загальних питань адміністративно-правового регулювання діяльності органів публічної влади, інформаційних відносин у сфері публічного управління, правового статусу органів прокуратури, захисту інформації та персональних даних, запровадження електронного урядування й цифрових сервісів у секторі правосуддя.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано згідно з основними положеннями Стратегії розвитку системи юстиції та конституційного судочинства на 2021-2023 роки, Стратегії розвитку прокуратури на 2021–2023 роки, а також із засадами державної політики у сфері цифрової трансформації та забезпечення інформаційної безпеки, що закріплені у програмних документах України щодо побудови сервісно орієнтованої, відкритої та цифрової держави. Тематика дослідження відповідає завданням реформування органів правопорядку, утвердження верховенства права,

підвищення прозорості та підзвітності органів публічної влади, а також впровадження сучасних інформаційно-правових механізмів у сфері правосуддя та прокуратури. Дисертаційне дослідження виконано відповідно до плану науково-дослідної роботи Науково-дослідного інституту публічного права за напрямом «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 012005390).

Мета і завдання дослідження. *Мета* роботи полягає у комплексному адміністративно-правовому осмисленні та науковому обґрунтуванні інформаційно-правового забезпечення діяльності органів прокуратури України як інституту адміністративного права з урахуванням вимог національного законодавства, європейських стандартів, сучасної практики публічного управління та цифрової трансформації сфери правосуддя, а також у формуванні концептуального бачення його методологічних засад, адміністративно-правового механізму та ключових напрямів удосконалення правових, інституційних і організаційних основ функціонування.

Досягнення поставленої мети передбачає вирішення таких основних завдань дослідження:

- теоретично обґрунтувати сутність, структуру та особливості інформаційно-правового забезпечення діяльності органів прокуратури України, визначивши їх місце в механізмі публічного управління, з розробленням авторської концептуальної моделі цього забезпечення;

- з'ясувати зміст та співвідношення категорій «мета», «принцип» і «завдання» інформаційно-правового забезпечення діяльності органів прокуратури України, розкрити їх роль у формуванні адміністративно-правового режиму функціонування органів прокуратури в інформаційній сфері та виявити взаємозв'язок між ними;

- визначити систему нормативно-правових актів, що формують засади інформаційно-правового забезпечення діяльності органів прокуратури України, виокремити її рівні, з'ясувати їх зміст, взаємозв'язок і роль у регламентації інформаційної діяльності прокуратури;

- розробити багатовимірну класифікацію видів інформаційно-правового забезпечення діяльності органів прокуратури України, конкретизувати зміст кожного з цих видів та обґрунтувати їх значення для формування цілісної моделі прокурорської діяльності в умовах інформатизації;

- обґрунтувати та систематизувати основні рівні й напрями інформаційно-правового забезпечення діяльності органів прокуратури України, розкрити їх зміст, функціональне призначення, взаємозв'язки та роль у формуванні цілісного адміністративно-правового механізму функціонування прокуратури в умовах цифрової трансформації публічної влади;

- визначити юридичну природу та зміст адміністративно-правових форм і методів інформаційно-правового забезпечення діяльності органів прокуратури України, розкривши їх як засоби здійснення публічно-владних повноважень у сфері інформаційної діяльності;

- з'ясувати адміністративно-правовий статус та ієрархію суб'єктів системи органів прокуратури України як суб'єктів інформаційно-правового забезпечення, розкрити їх організаційну побудову й обсяг управлінської компетенції в інформаційній сфері, а також визначити їх роль у багаторівневому механізмі формування та реалізації єдиної інформаційної політики прокуратури;

- здійснити порівняльний аналіз інформаційно-правового забезпечення діяльності органів прокуратури на прикладі Франції та Польщі, з'ясувати їх нормативні, інституційні й технологічні засади та на цій основі виокремити зарубіжний досвід, що може бути використаний для вдосконалення інформаційно-правового забезпечення діяльності органів прокуратури України;

- визначити та теоретично обґрунтувати основні перспективні напрями формування інформаційно-правових технологій у діяльності органів прокуратури України, розкривши їх ключові виміри з урахуванням європейських стандартів, міжнародної взаємодії та умов воєнного стану;

- запропонувати та науково обґрунтувати комплекс змін до законодавчої й відомчої бази інформаційно-правового забезпечення діяльності органів прокуратури України, передбачивши оновлення Дисциплінарного статуту

прокуратури України шляхом розроблення проєкту Закону України Про внесення змін до Статуту, доповнення Кодексу України про адміністративні правопорушення та уточнення інформаційного законодавства, передбачивши новий підхід до дисциплінарної та адміністративної відповідальності за правопорушення в зазначеній сфері;

- охарактеризувати систему юридичної відповідальності суб'єктів інформаційно-правового забезпечення органів прокуратури України, з'ясувавши зміст і нормативні підстави її основних видів та виявити ключові ризикові сегменти функціонування Єдиного реєстру досудових розслідувань (далі – ЄРДР), Системи електронного документообігу (далі - СЕД), Інформаційно-аналітичної системи «Облік та статистика органів прокуратури» (далі – ІАС «ОСОП»), Кваліфікованого електронного підпису (далі – КЕП) і режимно-секретної діяльності.

Об'єктом дослідження є правові відносини, що виникають у сфері діяльності органів прокуратури України.

Предмет дослідження – інформаційно-правове забезпечення діяльності органів прокуратури України.

Методи дослідження. Методологічну основу дисертаційного дослідження становить сукупність загальнонаукових, спеціально-юридичних та міждисциплінарних методів, застосування яких зумовлене комплексним характером інформаційно-правового забезпечення діяльності органів прокуратури України та логікою побудови роботи, що охоплює методологічні засади, адміністративно-правовий механізм і напрями його вдосконалення. Теоретичним підґрунтям обраної методики слугували положення філософії права, загальної теорії держави і права, адміністративного, інформаційного та конституційного права, а також сучасні концепції цифрової трансформації публічного управління й розвитку інформаційного суспільства. Відповідні підходи послідовно імплементовано в усіх трьох розділах дисертації.

Базовим для дослідження є *діалектичний (загальнофілософський) метод*, який дозволив розглядати інформаційно-правове забезпечення діяльності

органів прокуратури у взаємозв'язку його елементів, у динаміці нормативних змін і трансформації інституційних форм під впливом реформ сектору юстиції та цифровізації, простежити внутрішню логіку переходу від методологічних засад до аналізу механізму та подальшого вдосконалення регулювання (розділ 1, підрозділи 1.1–1.3, а також при узагальненні результатів у висновках). *Історико-правовий* метод використано для дослідження етапів становлення інформаційно-правового регулювання в системі публічного управління та еволюції правового статусу органів прокуратури в інформаційній сфері, з'ясування передумов формування сучасних моделей обігу інформації в прокуратурі (розділ 1, підрозділи 1.1–1.2). *Формально-юридичний* метод застосовано під час аналізу норм Конституції України, законів «Про прокуратуру», «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», а також підзаконних і відомчих актів, що регламентують документообіг, режим службової інформації, функціонування електронних реєстрів, інформаційних систем та організацію інформаційної безпеки в органах прокуратури (розділ 1, підрозділ 1.3; розділ 2, підрозділ 2.4; розділ 3, підрозділи 3.3–3.4). *Системно-структурний і функціональний* методи дали змогу дослідити інформаційно-правове забезпечення як цілісний адміністративно-правовий інститут, виокремити його елементи (види, рівні, напрями, форми, методи, суб'єкти), встановити їх вертикальні й горизонтальні зв'язки та практичну роль у забезпеченні виконання функцій органів прокуратури (розділ 1, підрозділи 1.1–1.2; розділ 2, підрозділи 2.1–2.3).

Порівняльно-правовий метод використано для аналізу зарубіжного (передусім європейського, з акцентом на Францію та Польщу) досвіду організації прокуратури, впровадження інформаційно-правових технологій, стандартів доступу до інформації та захисту даних. Його застосування дозволило виявити моделі, придатні для адаптації в Україні, визначити напрями імплементації європейських підходів у національне законодавство та окреслити можливі орієнтири реформування інформаційно-правового забезпечення вітчизняної прокуратури (розділ 3, підрозділ 3.1, а також при формулюванні

окремих пропозицій у підрозділі 3.3). *Логіко-семантичний* метод застосовано для уточнення категоріально-понятійного апарату дослідження, зокрема понять «інформаційно-правове забезпечення», «інформаційно-правові технології», «інформаційна безпека органів прокуратури», «адміністративно-правовий статус суб'єктів інформаційно-правового забезпечення», «рівень» та «напрямок інформаційно-правового забезпечення», «адміністративно-правові форми та методи», а також для формулювання авторських дефініцій, узгоджених із чинним законодавством та доктриною адміністративного права (розділ 1, підрозділи 1.1–1.2; розділ 2, підрозділи 2.1–2.3; частково – у розділі 3, підрозділи 3.2–3.4). *Статистичний та емпірико-аналітичний* методи дали змогу узагальнити окремі показники діяльності органів прокуратури, практику застосування інформаційного законодавства, дані про інформаційні ризики та інциденти, а також судову й дисциплінарну практику у сфері порушення правил обігу інформації, що слугувало емпіричною базою для формулювання висновків щодо ефективності чинного адміністративно-правового механізму та необхідності його вдосконалення (розділ 2, підрозділ 2.4; розділ 3, підрозділ 3.4). *Прогностичний і моделювальний* методи були використані для вироблення авторського бачення перспектив розвитку інформаційно-правових технологій в органах прокуратури, конструювання можливих моделей удосконалення адміністративно-правового механізму інформаційно-правового забезпечення, а також для обґрунтування напрямів реформування законодавства та організаційно-правових форм діяльності органів прокуратури (розділ 3, підрозділи 3.2–3.3). Сукупне застосування зазначених методів забезпечило внутрішню узгодженість теоретичних, нормативно-аналітичних і прикладних результатів дослідження.

Нормативно-правовим підґрунтям дисертаційного дослідження становить система актів національного та міжнародного права, що визначають засади організації й функціонування органів прокуратури України, правовий режим інформації та стандарти її обігу в публічному управлінні. Базу дослідження складають положення Конституції України, зокрема щодо права на інформацію,

гарантій захисту прав і свобод людини та принципів організації державної влади, а також Закон України «Про прокуратуру», який окреслює систему органів прокуратури, їх функції та місце в механізмі публічної влади. Важливу роль відіграють, насамперед, базові інформаційні закони України: «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», далі – процесуальне законодавство (Кодекс України про адміністративні правопорушення, Кримінальний процесуальний кодекс України), Закон України «Про адміністративну процедуру», Дисциплінарний статут прокуратури України, а також спеціальні акти у сфері електронного врядування й цифровізації (закони «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», програмні та стратегічні документи з розвитку цифрової держави та кібербезпеки). Нормативно-правове підґрунтя конкретизується відомчими актами Офісу Генерального прокурора та органів прокуратури (інструкції з організації діловодства, ведення ЄРДР, накази щодо обробки персональних даних, визначення переліку службової інформації та вимог до її захисту тощо), які регламентують внутрішні інформаційні процедури, режими доступу, порядок функціонування інформаційних систем і механізми інформаційної безпеки в органах прокуратури. Сукупність зазначених джерел створює цілісний нормативний масив, що слугує основою для теоретико-правового аналізу інформаційно-правового забезпечення діяльності органів прокуратури України та формування авторських пропозицій щодо вдосконалення відповідного адміністративно-правового механізму.

Науково-теоретичне підґрунтя дисертаційного дослідження формують положення загальної теорії держави і права, сучасної доктрини адміністративного права, інформаційного права та конституційно-правового статусу органів прокуратури, у межах яких інформаційно-правове забезпечення розглядається як міждисциплінарний феномен на стику публічного управління та інформаційних відносин. Концептуальними для роботи є напрацювання щодо природи та функцій публічної адміністрації, адміністративно-правового режиму діяльності органів прокуратури, правового статусу суб'єктів публічної влади, а

також теоретичні підходи до розуміння інформації як об'єкта правового регулювання, правового режиму персональних даних, публічної та службової інформації, інформаційної безпеки та цифрової трансформації врядування. Значну роль відіграють праці вітчизняних і зарубіжних авторів, присвячені інформаційному забезпеченню прокурорської діяльності, інформатизації системи правосуддя, організації електронного документообігу, функціонуванню електронних реєстрів, оцінюванню ризиків витоку, маніпулювання або спотворення службової інформації, а також організаційно-правовим засадам інформаційної безпеки органів прокуратури. Узагальнення та критичний аналіз цих підходів дозволили уточнити зміст категорії «інформаційно-правове забезпечення діяльності органів прокуратури», вибудувати логіку розмежування його методологічних засад, адміністративно-правового механізму та напрямів удосконалення, а також сформулювати авторську позицію щодо інформаційно-правового забезпечення як комплексного інституту адміністративного права, що інтегрує нормативний, інституційний, процедурний та технологічний компоненти у сфері функціонування органів прокуратури України.

Інформаційну та емпіричну основу дисертаційного дослідження становить сукупність нормативних, статистичних, практичних і доктринальних джерел, що відображають реальний стан інформаційно-правового забезпечення діяльності органів прокуратури України. Використано офіційні дані Офісу Генерального прокурора України (статистичну звітність, матеріали щодо функціонування Єдиного реєстру досудових розслідувань, внутрішні регламенти документообігу, відомчі накази й інструкції щодо режиму службової інформації, обробки персональних даних та організації інформаційної безпеки), а також матеріали судової практики. Емпіричну базу доповнюють офіційні звіти й аналітичні документи органів державної влади у сфері цифрової трансформації, інформаційної безпеки та протидії корупції, дані про виявлені випадки витоків та зловживань доступом до інформаційних ресурсів. Важливе місце посідають наукові публікації вітчизняних і зарубіжних дослідників, матеріали науково-практичних заходів, методичні рекомендації та аналітичні огляди, що дозволило

співвіднести нормативну модель інформаційно-правового забезпечення з реальною управлінською практикою та проблемами її реалізації.

Наукова новизна отриманих результатів полягає у здійсненні комплексного адміністративно-правового аналізу інформаційно-правового забезпечення діяльності органів прокуратури України в умовах цифрової трансформації публічного управління та реформування органів правопорядку, що дало змогу вперше обґрунтувати авторське бачення його категоріального апарату, правової природи, структури, змісту та адміністративно-правового механізму, а також розробити конкретні пропозиції щодо вдосконалення законодавства, відомчого нормативного регулювання й інформаційно-правових технологій у системі органів прокуратури. У результаті проведеного дослідження сформовано низку нових наукових положень і висновків, основні з них такі:

вперше:

- сформульовано авторське визначення категорії «інформаційно-правове забезпечення діяльності органів прокуратури України» як комплексної системи правових норм, організаційних процедур, інформаційних ресурсів та інформаційно-технологічних засобів, за допомогою яких забезпечується належний режим створення, збирання, обробки, зберігання, передавання, використання й захисту інформації у процесі реалізації конституційних і законних повноважень прокуратури, з урахуванням її місця в системі публічної влади та особливостей воєнного стану;

- на основі порівняльно-правового аналізу зарубіжного досвіду інформаційно-правового забезпечення діяльності органів прокуратури Франції та Польщі системно виокремлено ключові нормативні, інституційні та технологічні елементи функціонування їхніх інформаційних систем, що можуть бути запозичені та адаптовані в Україні;

- сформульовано авторське бачення категорії «суб'єкт інформаційно-правового забезпечення діяльності органів прокуратури України», на підставі чого розкрито адміністративно-правовий статус Офісу Генерального прокурора,

Спеціалізованої антикорупційної прокуратури, обласних і окружних прокуратур як спеціальних суб'єктів із різним, але взаємопов'язаним обсягом повноважень, обов'язків та відповідальності у сфері обігу інформації;

- розроблено проєкт Закону України Про внесення змін до «Дисциплінарного статуту прокуратури України», який присвячено інформаційним дисциплінарним проступкам працівників прокуратури, у якому запропоновано нормативне визначення таких проступків, їх типологію, критерії тяжкості, спеціальну процедуру фіксації та доказування цифрових інцидентів, вимоги до електронних доказів і «ланцюга збереження», а також запропоновано ескалаційну шкалу дисциплінарних стягнень для працівників органів прокуратури України;

- запропоновано та обґрунтовано комплексний авторський підхід до інформаційного правопорушення у діяльності органів прокуратури України як сукупності дисциплінарних та адміністративних деліктів, пов'язаних із порушенням режиму доступу, обліку, зберігання та використання службової й конфіденційної інформації в інформаційних (автоматизованих) системах, а саме, на цій основі рекомендовано виокремлення підінституту інформаційної дисциплінарної відповідальності, запровадження нового виду дисциплінарного стягнення у вигляді тимчасової заборони доступу до службової інформації та закріплення в КУпАП конструкції «спеціальне право доступу до інформаційних (автоматизованих) систем»;

удосконалено:

- понятійно-категоріальну характеристику «мети», «принципів» і «завдань» інформаційно-правового забезпечення діяльності органів прокуратури України, із виділенням базових загальних принципів (законність, верховенство права тощо), спеціальних інформаційно-правових (принципи відкритості та прозорості інформаційних процесів, цілісності й безперервності інформаційних потоків, захисту персональних даних, інформаційної безпеки), а також прокурорсько-інституційних (інституційної незалежності прокуратури в інформаційній сфері,

внутрішньої ієрархії та підзвітності, відповідальності за інформаційну дисципліну);

- класифікацію видів інформаційно-правового забезпечення діяльності органів прокуратури: на основі критичного осмислення наявних підходів аргументовано доцільність побудови системної типології видів інформаційно-правового забезпечення (інформаційно-аналітичного, інформаційно-комунікаційного, інформаційно-ресурсного, інформаційно-безпекового тощо) як конструктивного інструменту проєктування моделей регулювання, розвитку реєстрів, електронного документообігу та систем кіберзахисту;

- наукові підходи до структуризації інформаційно-правового забезпечення діяльності органів прокуратури України шляхом виокремлення його багаторівневої побудови (нормативно-правового, інституційного, організаційно-процесуального, інфраструктурно-технологічного та індивідуально-посадового рівнів), що дозволило розкрити внутрішню ієрархію елементів цього забезпечення та їх функціональний взаємозв'язок у механізмі адміністративно-правового впливу;

- підходи до розуміння адміністративно-правових форм і методів інформаційно-правового забезпечення: сформовано їх системний перелік та показано зв'язок інформаційно-регулятивних, організаційно-розпорядчих, контрольних, координаційно-комунікаційних і примусових методів з окремими стадіями інформаційних процесів у прокуратурі (збирання, реєстрація, обробка, зберігання, використання, захист інформації);

дістало подальшого розвитку:

- теоретичні уявлення про структуру та проблеми нормативно-правового регулювання інформаційно-правового забезпечення діяльності органів прокуратури України через виявлення колізій між загальним інформаційним законодавством і спеціальними актами, недоліків Дисциплінарного статуту прокуратури України та КУпАП щодо фіксації, кваліфікації й санкціонування порушень інформаційних режимів, а також через деталізацію багаторівневої

структури нормативно-правової бази (конституційний, законодавчий, підзаконний, відомчий та міжнародно-правовий рівні);

- науково обґрунтовані пропозиції щодо вдосконалення законодавства України в частині інформаційно-правового забезпечення діяльності органів прокуратури, які включають: комплекс змін до Дисциплінарного статуту прокуратури України (виділення інформаційних дисциплінарних проступків в окремий розділ, деталізація їх складів, процедур фіксації й доказування цифрових інцидентів); зміни до Кодексу України про адміністративні правопорушення (запровадження нового виду адміністративного стягнення у вигляді тимчасового обмеження спеціального права доступу до інформаційних систем, доповнення Загальної та Особливої частин нормами про порушення правил роботи з інформаційними системами, уточнення статусу «реєстратора», «користувача» та «інформаційних (автоматизованих) систем»); пропозиції щодо удосконалення інформаційного законодавства (уточнення базових дефініцій, посилення гарантій захисту персональних даних, закріплення мінімального технічного профілю безпеки, уніфікації документування інцидентів та ведення реєстру інформаційних проступків);

- бачення перспектив розвитку інформаційно-правових технологій у системі органів прокуратури України, що охоплює пропозиції щодо підвищення рівня інформаційної культури й правосвідомості працівників, вироблення етичних стандартів роботи з інформацією, визначення правового статусу інформаційно-правових технологій та алгоритмів взаємодії суб'єктів у цій сфері;

- підходи до визначення та класифікації видів юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури (дисциплінарної, адміністративної, матеріальної, кримінальної, інформаційно-правової) через деталізацію їх нормативних підстав, об'єктів посягань та особливостей застосування з урахуванням специфіки інформаційних правопорушень.

Практичне значення отриманих результатів полягає у можливості їх безпосереднього використання в різних сферах діяльності, пов'язаних із

удосконаленням інформаційно-правового забезпечення діяльності органів прокуратури України, зокрема у:

- *науково-дослідній сфері* – положення дисертації створюють підґрунтя для подальших досліджень проблематики адміністративно-правового регулювання інформаційних відносин у діяльності органів правопорядку;

- *правотворчій сфері* – запропоновані в дисертації проєкти нормативно-правових змін можуть бути використані під час вдосконалення чинного законодавства у частині регламентації режимів доступу до інформації, роботи з інформаційними системами, відповідальності за інформаційні проступки та захисту персональних даних у діяльності органів прокуратури;

- *освітньому процесі* – результати дослідження можуть бути використані при розробленні та викладанні навчальних дисциплін «Адміністративне право і процес», «Інформаційне право», «Організація діяльності органів прокуратури», «Правові засади інформаційної безпеки» тощо.

Апробація результатів дисертації. Основні положення та результати роботи оприлюднено та обговорено на 4-ох науково-практичних конференціях: «Сектор безпеки України: актуальні питання науки та практики» (м. Харків, 27 березня 2025 року), «Актуальні питання адміністративного права та адміністративного судочинства» (м. Харків, 15 травня 2025 року), «Сучасні тенденції соціально-гуманітарного розвитку суспільства» (м. Харків, 3-5 листопада 2025 року), «Modern Perspectives on Science and Economic Progress» (Vilnius, November 5-7, 2025).

Структура та обсяг дисертації. Дисертаційна робота складається з вступу, 3 розділів, що містять 11 підрозділів, висновків до кожного розділу, загальних висновків, списку використаних джерел (170 найменувань). Загальний обсяг дисертації становить 255 сторінок.

РОЗДІЛ 1

МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

1.1. Сутність та особливості інформаційно-правового забезпечення діяльності органів прокуратури України

У сучасних умовах функціонування інформаційного суспільства інформація набула статусу одного з ключових стратегічних ресурсів державної влади, без належного використання якого неможливе ефективне здійснення публічного управління, зокрема у сфері виконавчої та правоохоронної діяльності. У цьому контексті органи прокуратури, які є невід'ємним елементом системи правосуддя та реалізують функцію нагляду за додержанням законів, особливо потребують високоякісного інформаційно-правового забезпечення своєї діяльності. Водночас процес формування й розвитку інформаційно-правового забезпечення у сфері функціонування органів прокуратури стикається з низкою концептуальних і прикладних проблем — починаючи від відсутності усталеного категоріального апарату до наявних прогалин у нормативно-правовому регулюванні та недостатнього рівня забезпечення інформаційної безпеки.

У загальному теоретико-правовому розумінні категорія «інформаційно-правове забезпечення» постає як складне, міждисциплінарне правове явище, що формується на стику інформаційного права та адміністративного права. Застосування цієї категорії у сфері діяльності органів прокуратури вимагає не лише осмислення змісту самого терміна, а й з'ясування його структурної залежності від функціональної природи прокурорських повноважень у демократичній правовій державі [1, с. 122].

В адміністративно-правовій площині інформаційно-правове забезпечення розглядається як цілісна система правових норм, інституційних утворень та спеціалізованих інструментів, які регламентують суспільні правовідносини, пов'язані з процесами створення, циркуляції, обробки, зберігання, захисту та застосування інформації в межах діяльності органів публічної влади. Така

система охоплює не лише технологічний чи технічний компоненти, а й нормативний, організаційно-процесуальний та інституційний виміри, що в сукупності формують цілісний механізм правового впливу в межах адміністративної юрисдикції [2, с. 33].

У межах адміністративного права поняття «забезпечення» зазвичай трактується як складова системи засобів, механізмів і процедур, за допомогою яких органи публічного управління реалізують свої владні функції. У цьому сенсі інформаційно-правове забезпечення постає не як зовнішній додаток до діяльності органів публічної влади, а як внутрішньоінтегрований структурний елемент механізму їх функціонування, у тому числі й у діяльності органів прокуратури.

У науковій доктрині інформаційно-правове забезпечення діяльності органів прокуратури України зазвичай трактується як система правовідносин, що виникають у процесі створення, обробки та використання інформації в межах органів прокуратури, а також у зв'язку з ними як суб'єктами інформаційного права [3, с. 157]. Втім, така дефініція видається надто вузькою, оскільки не охоплює організаційні, процедурні та інституційні аспекти, що мають вирішальне значення в умовах сучасного адміністративного управління.

На наш погляд, інформаційно-правове забезпечення діяльності органів прокуратури доцільно тлумачити значно ширше — як нормативно врегульовану, інституційно-організовану та процесуально визначену систему засобів, способів і механізмів адміністративно-правового впливу, що спрямовані на формування, отримання, оброблення, накопичення, зберігання, використання, обмін та захист інформації, необхідної для належного виконання прокуратурою своїх функцій у сфері публічного управління. При цьому важливим є дотримання принципів законності, забезпечення інформаційної безпеки та гарантування прав людини в сфері обігу як публічної, так і службової інформації [4, с. 515].

На нашу думку процес становлення інформаційно-правового забезпечення у системі публічного управління України має складну багатовекторну еволюцію, що відображає трансформацію як правового мислення, так і управлінської

парадигми в умовах змін політичного режиму, технологічного розвитку та інтеграційних процесів. Умовно цей процес можна поділити на чотири ключові етапи: радянський, пострадянський (становлення суверенного інформаційного простору), нормативно-інституційний (розвиток інформаційного законодавства), та цифровий (перехід до цифрового врядування і відкритого адміністрування).

На першому етапі (радянський) - інформація була об'єктом централізованого контролю. У радянський період інформація розглядалася насамперед як інструмент ідеологічного впливу й об'єкт суворого державного контролю. Адміністративно-правове регулювання інформаційних процесів базувалося на засадах жорсткої централізації, монополії на інформацію, обмеження доступу до джерел та відсутності будь-яких інституційних форм прозорості. Інформація мала виключно службовий, політичний або виробничий характер. Основним завданням держави було недопущення "несанкціонованого" поширення відомостей, що обмежувало правову природу інформаційної діяльності.

Правовий інструментарій був фрагментарним і обмежувався окремими інструкціями та наказами, спрямованими переважно на охорону державної таємниці, захист виробничої інформації, регламентацію архівного обігу. Конституційного закріплення права на інформацію не існувало. Натомість ключовими були категорії «державна таємниця», «службова інформація», «антирадянська пропаганда» тощо. Такий підхід до інформаційно-правового забезпечення був репресивним за суттю і виключав будь-які механізми демократичного контролю.

Другий етап (пострадянський) - характеризувався становлення інформаційного суверенітету. Із проголошенням незалежності України постала потреба у формуванні національної інформаційної політики, заснованої на демократичних засадах, правах людини та принципі відкритості. Прийняття Конституції України 1996 року, яка вперше закріпила право кожного на вільний доступ до інформації (стаття 34), стало основою формування нової моделі

інформаційно-правового забезпечення [5]. Вагомим кроком стало ухвалення Закону України «Про інформацію» 1992 року, який унормував базові категорії: види інформації, суб'єкти інформаційних правовідносин, способи отримання та поширення інформації, принципи інформаційної діяльності [6]. Проте попри інноваційність для того часу, цей Закон залишався рамковим і не вирішував практичних питань адміністрування інформаційного обігу в органах влади. На цьому етапі інформаційно-правове забезпечення розвивалося переважно декларативно, із запровадженням інституцій (Державний комітет з питань інформаційної політики, Держкомтелерадіо тощо), які мали обмежені повноваження. Інформаційні потоки у публічному управлінні все ще залишалися закритими, а юридичний механізм доступу до них – недосконалим.

Третім етапом був етап нормативно-інституційного оформлення (2000–2015 рр.). Новий імпульс розвитку інформаційно-правовому забезпеченні надало прийняття низки спеціалізованих законів: «Про захист персональних даних» (2010) [7], «Про доступ до публічної інформації» (2011) [8], «Про інформацію» у редакції (2011) [9].

Було закладено нормативні основи забезпечення прозорості діяльності публічної адміністрації, урядового електронного документообігу, відкритих даних, захисту прав суб'єктів персональних даних. Особливу роль відіграв Закон «Про доступ до публічної інформації», який установив адміністративно-правові обов'язки органів публічної влади щодо оприлюднення інформації та забезпечення її надання за запитами громадян. Уперше з'явилися правові поняття: «відкритість публічного управління», «суспільно необхідна інформація», «електронна форма надання інформації», що перетворили ПЗ на складову частину управлінського процесу.

Четвертим етапом є цифровий етап, що заклав перехід до відкритого адміністрування. Це найновіший етап у генезисі інформаційно-правового забезпечення, що пов'язаний із цифровою трансформацією публічного управління, що активізувалася після 2019 року зі створенням Міністерства цифрової трансформації України [10]. Також, було започатковано проєкт

«Держава у смартфоні», запроваджено платформу «Дія», розширено функціонування єдиних реєстрів, запроваджено концепцію «інтероперабельності» державних інформаційних систем [11].

У межах цього етапу інформаційно-правове забезпечення перетворюється на системну категорію цифрового адміністрування, що охоплює: а) інтеграцію електронних сервісів в адміністративні процедури; б) побудову правових механізмів «цифрової довіри» (електронні підписи, блокчейн-рішення); в) гармонізацію українського законодавства з європейським (GDPR, NIS2); г) інституціоналізацію безпекових засад цифрового обміну (кібербезпека, захист критичної інфраструктури, управління ризиками витоку інформації). Таким чином, цифровий етап у розвитку ПЗ ознаменував перехід від фрагментарного регулювання до побудови цілісної системи інформаційно-правового адміністрування.

На наш погляд, інформаційно-правове забезпечення діяльності органів прокуратури є багатокомпонентною системою, що охоплює сукупність нормативних, організаційних, технологічних, кадрових, контрольних-наглядових і правозахисних елементів, кожен з яких відіграє функціонально важливу роль у забезпеченні ефективної, законної та прозорої діяльності прокуратури в інформаційній сфері, так наприклад:

1. Нормативне забезпечення становить засадничу основу функціонування всієї системи. Йдеться про формування і застосування правових норм, що визначають порядок реалізації права на інформацію в межах прокурорської діяльності. Зокрема, це стосується встановлення чіткого порядку отримання, оброблення, використання, зберігання та захисту інформації. До таких актів належать закони, підзаконні нормативно-правові акти, внутрішні інструкції, положення та накази, які регламентують правовий режим інформації у межах повноважень органів прокуратури.

2. Організаційне забезпечення охоплює внутрішню структуру та механізми реалізації інформаційної політики в межах прокурорської системи. Йдеться, передусім, про визначення функціонального поділу обов'язків між

структурними підрозділами, створення та функціонування служб з кібербезпеки, режимно-секретних частин, підрозділів архівного забезпечення, операторів електронного документообігу тощо. Така система дозволяє забезпечити цілісне управління інформаційними потоками в межах органів прокуратури з урахуванням вимог конфіденційності та спеціального режиму доступу до інформації.

3. Технологічне забезпечення включає впровадження і використання сучасних інформаційно-комунікаційних технологій. Це, зокрема, електронні реєстри, автоматизовані системи управління документами, бази даних, внутрішні службові портали, засоби електронного цифрового підпису, інтеграція з іншими державними інформаційними ресурсами (Єдиним реєстром досудових розслідувань — ЄРДР, судовими реєстрами, тощо). Технологічний компонент забезпечує оперативність, точність, цілісність та безпечність обробки інформації у межах реалізації прокурорських повноважень.

4. Кадрове забезпечення означає наявність належної фахової підготовки та підвищення кваліфікації прокурорів і технічного персоналу у сфері інформаційного права, цифрових технологій та захисту даних. Особливу увагу має бути приділено навчанню щодо дотримання законодавства про персональні дані, інформаційної безпеки, доступу до публічної інформації та етичних аспектів роботи з конфіденційною інформацією.

5. Контрольно-наглядове забезпечення включає впровадження ефективних внутрішніх механізмів контролю за дотриманням вимог інформаційного законодавства — у формі внутрішнього моніторингу, перевірок, аудитів, звітності. Крім того, важливою є наявність зовнішнього контролю з боку судових органів, органів державної влади, органів парламентського нагляду, а також інститутів громадського контролю.

6. Правозахисний компонент є фундаментальним в умовах правової держави. Йдеться про забезпечення реалізації конституційного права громадян на доступ до публічної інформації, гарантування дотримання прав людини у сфері інформаційних правовідносин, а також представлення правових позицій

органів прокуратури у випадках судового захисту права на інформацію. Особливого значення такий компонент набуває у контексті обробки персональних даних, доступу до службової інформації та дотримання стандартів інформаційної відкритості.

У контексті функціонування органів прокуратури зазначена система має бути адаптованою до особливостей здійснення прокурорських повноважень, норм кримінального та кримінального процесуального права, а також вимог інформаційної безпеки, режиму професійної таємниці, конфіденційності, з одночасним забезпеченням захисту прав і свобод людини та громадянина у сфері обігу публічної інформації.

У свою чергу варто відзначити, що органи прокуратури України як складова системи публічної влади та суб'єкти адміністративної юрисдикції щоденно оперують значними обсягами даних, що циркулюють у межах складних вертикальних і горизонтальних управлінських структур. Саме через інформаційні потоки реалізуються функції нагляду, представництва, організаційного керівництва та внутрішнього адміністрування. Типологія цих потоків потребує глибокого теоретико-правового осмислення, адже вона безпосередньо впливає на ефективність реалізації функцій прокуратури та дотримання вимог законності, прозорості, відповідальності.

В адміністративно-правовій науці підставами класифікації інформаційних потоків є: а) напрям руху (вхідні, вихідні, внутрішні); б) джерело виникнення (внутрішньоорганізаційні, зовнішні); в) форма подання (документальні, електронні, усні); г) правовий статус (офіційні, службові, неофіційні); г) ступінь відкритості (публічні, обмеженого доступу, таємні); д) функціональна мета (управлінські, контрольні, аналітичні, нормативні тощо). У межах прокуратури ці критерії набувають специфіки з огляду на особливий статус органів як водночас суб'єкта юрисдикції, процесуального учасника і адміністративного органу.

На нашу думку, основними типами інформаційних потоків у межах адміністративної діяльності органів прокуратури є:

1. Вхідні інформаційні потоки - ця категорія охоплює дані, що надходять до органів прокуратури ззовні: з боку громадян, юридичних осіб, інших державних органів, правоохоронних структур, судів тощо. Основними каналами надходження є запити, заяви, повідомлення про вчинення кримінального правопорушення, ухвали суду, матеріали органів досудового розслідування, запити народних депутатів, органів місцевого самоврядування. Адміністративно-правовий режим цих потоків регламентується Законами України «Про звернення громадян» [12], та «Про прокуратуру» [13], Кримінальним процесуальним кодексом України [14], та наказами Генерального прокурора.

2. Внутрішні (вертикальні і горизонтальні) потоки - до цієї категорії належать інформаційні зв'язки між підрозділами прокуратури одного рівня (горизонтальні) та між прокуратурами різного рівня (вертикальні). Прикладами є службові доповідні, зведення, статистичні звіти, аналітичні довідки, внутрішні настанови, доручення, службові листи. Ці потоки забезпечують: а) ієрархічну координацію (Офіс Генерального прокурора → обласні прокуратури → окружні прокуратури); б) управлінський контроль; в) планування й реалізацію функцій нагляду, представництва, аналітики відповідно до ст. 2 Закону України «Про прокуратуру» [13].

3. Вихідні потоки - це інформація, що генерується або оформлюється прокуратурою та адресована зовнішнім суб'єктам: суду, органам досудового розслідування, представницьким органам, ЗМІ, громадськості. До них належать: а) процесуальні документи (постанови, клопотання, обвинувальні акти); б) відповіді на запити; в) прес-релізи, роз'яснення, аналітичні матеріали; г) повідомлення про результати перевірок та нагляду. Належна якість, своєчасність і юридична коректність таких потоків є критично важливими з погляду відповідальності органу прокуратури перед суспільством.

4. Реєстрово-аналітичні потоки - ця категорія охоплює дані, що циркулюють у межах електронних облікових систем, реєстрів, інформаційних банків. Насамперед це: а) Єдиний реєстр досудових розслідувань (ЄРДР); б) Статистичні

модулі внутрішнього звітування; в) Реєстри заяв, рішень, кримінальних проваджень. Ці потоки відіграють ключову роль у цифровій трансформації адміністративної діяльності органів прокуратури, а також у здійсненні моніторингу ефективності.

5. Публічні комунікаційні потоки – це потоки, що спрямовані на публічну комунікацію з суспільством. Вони реалізуються через офіційні сайти прокуратур, публічні звіти, брифінги, соціальні мережі. Такі потоки спрямовані на зміцнення довіри, реалізацію принципу відкритості влади та дотримання інформаційних прав громадян.

Загалом, інформаційні потоки в адміністративно-правовій діяльності органів прокуратури України становлять складну, структуровану систему, що забезпечує реалізацію владних повноважень, управлінську координацію, наглядові та комунікативні функції. Їх типологізація має як практичне, так і теоретичне значення: вона сприяє підвищенню ефективності управління, прозорості діяльності та вдосконаленню нормативного забезпечення.

Загалом, варто відмітити, що діяльність прокуратури має специфіку, що накладає особливі вимоги на інформаційно-правове забезпечення. Ці особливості пов'язані з функціональною роллю прокуратури, її правовим статусом, компетенцією та процесуальними обмеженнями.

Хоча прокуратура реалізує ключові повноваження у сфері кримінального провадження, вона також виконує адміністративно-правові функції, а саме здійснює нагляд за дотриманням законів органами влади, представляє інтереси громадян або держави в суді, реагує на звернення тощо. У таких випадках прокуратура виступає суб'єктом адміністративного права, а інформаційно-правове забезпечення виконує роль інструменту реалізації відповідних функцій.

Адміністративно-правовий підхід до інформаційно-правового забезпечення дозволяє чітко окреслити межі повноважень прокурора щодо інформації, визначити процедури, гарантії та баланс між відкритістю та захистом інформації. Так, згідно із ст. 2 Законом України «Про прокуратуру», прокуратура реалізує чотири основні функції: 1) підтримання державного обвинувачення в суді; 2)

представництво інтересів громадянина або держави в суді у визначених законом випадках; 3) нагляд за додержанням законів органами, що провадять оперативно-розшукову діяльність, дізнання, досудове слідство; 4) нагляд за додержанням законів при виконанні судових рішень у кримінальних справах, а також при застосуванні інших заходів примусового характеру, пов'язаних з обмеженням особистої свободи громадян [13].

Кожна з цих функцій передбачає правове, організаційне й технічне інформаційне забезпечення. Воно виконує дві ключові ролі: 1) забезпечення доступу прокурора до баз даних, реєстрів, аналітики, доказової інформації, без чого неможливо реалізувати функцію обвинувачення або прийняття процесуального рішення; 2) регламентація внутрішніх інформаційних процесів — документообігу, обробки персональних даних, звітності, внутрішнього контролю та зовнішньої комунікації.

На наш погляд, здійснення зазначених функцій висуває такі особливості: 1) Оперативний інформаційний обмін - прокурори активно взаємодіють із держорганами, судом, правоохоронцями, формуючи запити й отримуючи відповіді через електронні канали; 2) Обробка конфіденційної інформації - частина даних має статус державної чи службової таємниці (зокрема, банківська інформація, дані слідства); 3) Аналітична складова - прокуратура має не лише акумулювати, а й аналізувати великі обсяги даних, прогнозувати криміногенні процеси, готувати звіти й аналітичні продукти; 4) Доступ до публічної інформації - як суб'єкт публічного управління, прокуратура зобов'язана реагувати на інформаційні запити громадян, оприлюднювати звіти, забезпечувати відкритість, із дотриманням вимог законодавства; 5) Інформаційна безпека - з огляду на чутливість справ, витік інформації здатен завдати шкоди правосуддю й довірі до прокуратури, а тому система має гарантувати кіберзахист від внутрішніх і зовнішніх загроз.

В основі інформаційного функціонування прокуратури — запровадження електронних систем (баз даних, електронного документообігу, міжвідомчих порталів), які повинні відповідати вимогам безпеки (шифрування, ізоляція

каналів зв'язку), резервного копіювання, контролю цілісності даних, обліку доступу та фіксації дій користувачів.

Крім цього, надзвичайно важливими є ефективні механізми контролю за дотриманням інформаційних норм: а) внутрішній контроль (внутрішній аудит, служби безпеки, ревізії); б) зовнішній контроль (нагляд державних органів, судовий контроль, контроль з боку громадськості); в) відповідальність (наприклад, дисциплінарна, адміністративна, матеріальна та кримінальна).

Водночас, варто відзначити важливість інформаційної безпеки, яка є однією з ключових складових інформаційно-правового забезпечення діяльності органів прокуратури України. Вона безпосередньо впливає на ефективність реалізації прокурорських повноважень і водночас слугує гарантією законності у поводженні з відомостями, що мають службовий, персональний, процесуальний або оперативний характер. У межах прокуратури циркулюють інформаційні ресурси з різним правовим режимом: від електронних кримінальних проваджень у ЄРДР і документів досудового розслідування до службового листування та внутрішніх аналітичних матеріалів. Значна частина цих даних підлягає обмеженому доступу та потребує спеціальних заходів захисту.

У цьому контексті інформаційна безпека розглядається не як суто технічна категорія ІТ-адміністрування, а як елемент адміністративно-правової організації діяльності органу публічної влади. Через неї реалізуються принципи законності, контролю, відповідальності та захисту прав людини. Вона охоплює нормативну, організаційну, кадрову та технічну складові, інтегровані в загальну систему інформаційно-правового забезпечення прокуратури.

Сутнісно інформаційна безпека передбачає створення комплексної системи запобіжників, що поєднують правові, технічні, організаційні та етичні заходи. Така система повинна унеможливити несанкціонований доступ, витоки, спотворення або знищення даних, а також забезпечувати відповідність їх обробки вимогам законодавства — зокрема, щодо державної таємниці, конфіденційної інформації, персональних даних і електронних доказів. Вона повинна враховувати як внутрішні ризики (низький рівень підготовки персоналу,

порушення процедур, зловживання доступом), так і зовнішні загрози (кібератаки, фішинг, втручання у канали зв'язку) [15, с. 111].

З адміністративно-правової точки зору, інформаційна безпека реалізується через нормативне регулювання, що визначає правила поведінки з інформацією, її класифікацію, доступ і відповідальність за порушення. Закон України «Про прокуратуру» містить лише окремі згадки про інформаційно-правове забезпечення, без системних положень щодо захисту інформаційної інфраструктури. Частково цю прогалину заповнюють внутрішні акти: інструкції щодо ЄРДР, накази Генерального прокурора, регламенти діловодства. Зокрема, наказ № 77 від 26.07.2014 регулює порядок обробки персональних даних у прокуратурі, включно з ЄРДР [16], а наказ № 578 від 09.12.2020 встановлює перелік службової інформації та вимоги до її захисту [17].

До основних адміністративно-організаційних заходів інформаційної безпеки можна віднести: а) чіткий поділ доступу до інформаційних систем за рівнем повноважень; б) функціонування режимно-секретних підрозділів, що контролюють дотримання вимог безпеки; в) застосування технічних засобів захисту (шифрування, журналювання, виявлення вторгнень, багатфакторна аутентифікація); г) службовий контроль, інструктажі, етичні зобов'язання персоналу; г) взаємодія з державними структурами кібербезпеки для реагування на інциденти.

Окремої уваги потребує захист цифрових доказів у досудовому розслідуванні. Електронні дані мають зберігатися в автентичному вигляді, бути захищеними від спотворення чи втрати, відповідати технологічним та процесуальним стандартам. Це вимагає розробки внутрішніх інструкцій, запровадження засобів фіксації змін (наприклад, блокчейн), а також належного правового регулювання застосування електронних доказів у суді.

Таким чином, ефективна інформаційна безпека органів прокуратури повинна бути інтегрованою у всю систему інформаційно-правового забезпечення від законодавчого регулювання до формування внутрішньої інформаційної культури персоналу.

У свою чергу, невід'ємною частиною інформаційно-правового забезпечення діяльності органів прокуратури України є належне виявлення та мінімізація ризиків, пов'язаних із витоком, маніпулюванням або спотворенням службової інформації. Особливої актуальності зазначені ризики набувають в умовах цифрової трансформації, коли обробка, зберігання й передача даних здійснюються із застосуванням електронних систем та автоматизованих реєстрів, зокрема Єдиного реєстру досудових розслідувань.

У межах адміністративно-правового підходу до інформаційної безпеки органів прокуратури доцільно виокремити три базові групи ризиків: 1) ризик витоку інформації – пов'язаний із порушенням встановленого порядку доступу до інформації, недотриманням вимог щодо збереження службової та персональної інформації, застосуванням неналежних каналів зв'язку, зокрема особистих пристроїв або несанкціонованих застосунків; 2) ризик маніпулювання інформацією – проявляється через спотворене подання інформації в медіа, вибіркоче або цілеспрямоване поширення внутрішніх даних з метою тиску, дискредитації або втручання в хід провадження; 3) ризик спотворення інформації – охоплює як ненавмисні, так і навмисні помилки при внесенні даних у внутрішні електронні бази, їх редагуванні або зберіганні, що може мати наслідком порушення процедур законного реагування. Кожен із вказаних типів ризиків має оцінюватися з позиції ймовірності настання та масштабів потенційної шкоди [18, с. 312].

Проведення оцінювання ризиків у межах діяльності органів прокуратури передбачає: а) аналіз внутрішніх процедур обробки інформації, включаючи адміністрування доступу, права редагування та обсяги даних, що передаються через електронні канали; б) виявлення типових вразливих зон – зокрема, використання незахищених мереж, дублювання інформації на особистих носіях, недостатнє логування змін у базах даних; в) запровадження системного аудиту та моніторингу – обов'язковий облік доступу до ЄРДР, журналювання змін у реєстрах, службові перевірки при виявленні інцидентів; г) формалізацію

процедур реагування – включаючи встановлення відповідальності за неналежне поводження з інформацією, як дисциплінарної, так і адміністративної.

Слід зазначити, що аудит витоків у межах правоохоронних органів виявляє системну проблему недостатності внутрішніх запобіжників. Зокрема, Національне агентство з питань запобігання корупції у звіті за 2023 рік підкреслює, що значна частина витоків інформації відбувається через людський фактор та недотримання регламентів [19, с. 67].

Узагальнюючи викладене, слід зазначити, що інформаційно-правове забезпечення діяльності органів прокуратури України є системним і багаторівневим інститутом публічного права, який охоплює як нормативну регламентацію обігу інформації, так і інституційну організацію цифрових процесів у межах прокурорської юрисдикції. Воно забезпечує реалізацію конституційних функцій прокуратури через правове оформлення доступу до даних, ведення електронного діловодства, використання баз даних і захисту інформаційних ресурсів. Сучасне розуміння сутності цього явища потребує врахування не лише формально-юридичних засад, а й адміністративно-управлінських механізмів, інноваційних цифрових технологій та вимог інформаційної безпеки. Особливості інформаційно-правового забезпечення в прокуратурі зумовлюються як спеціальним статусом органу, так і характером функцій, що поєднують правозастосування, нагляд, представництво держави та обов'язок дотримання прав і свобод людини.

1.2. Мета, принципи, завдання інформаційного-правового забезпечення діяльності органів прокуратури України

Мета, принципи та завдання виступають фундаментальними системоутворюючими категоріями у праві загалом і в адміністративному праві зокрема. Їхнє наукове осмислення дозволяє не лише структурувати знання про сутність правових інститутів, а й забезпечити узгоджене формування та реалізацію державної політики, зокрема у сфері організації та функціонування органів прокуратури.

У теорії права категорії «мета», «принцип», «завдання» виконують функцію концептуальних «опор», через які формуються та пояснюються правові інститути, процедури і режими. Вони задають вектор, межі та інструменти правового регулювання: мета визначає бажаний нормативно-організаційний стан; принципи — імперативні ідеї та правила-орієнтири, що структурують зміст і спосіб правової дії; завдання — конкретизовані етапи досягнення мети засобами права й управління [20, с. 197-220]. Такий трикутник категорій забезпечує внутрішню логіку й відтворюваність адміністративно-правових рішень у сфері публічної влади, включно з діяльністю органів прокуратури як особливого суб'єкта публічної влади.

В українській правовій системі це триєдине підґрунтя матеріалізується у спеціальних законах, що визначають функції прокуратури, інформаційний порядок, стандарти доступу, обмежень і захисту даних. Закон України «Про прокуратуру» прямо фіксує функції органів прокуратури, через які конкретизуються як мета інституційної діяльності (охорона прав, свобод, інтересів держави та суспільства), так і завдання (підтримання публічного обвинувачення, процесуальне керівництво досудовим розслідуванням тощо) [13]. Натомість принципи інформаційного порядку формалізовані у законах «Про інформацію» (відкритість, законність, достовірність, повнота) і «Про доступ до публічної інформації» (презумпція відкритості, максимальне сприяння доступу, пропорційність обмежень, прозорість). Спільно ці норми створюють нормативний каркас, у межах якого органи прокуратури організують збирання, обробку, зберігання, доступ і захист інформації — від персональних даних до службової й таємної інформації.

У загальнотеоретичному сенсі мета - це нормативно окреслений і ціннісно виправданий стан суспільних відносин, якого домагаються правовими засобами; у сфері публічного управління - це «цільова функція» адміністративно-правового впливу, що задає програму дій органів влади. У контексті діяльності органів прокуратури мета інформаційно-правового забезпечення полягає у створенні таких правових, технічних, організаційних та інституційних умов, які

б сприяли ефективному виконанню конституційно закріплених функцій прокуратури — підтримання державного обвинувачення, представництво інтересів держави, нагляд за досудовим розслідуванням тощо.

У свою чергу, принципи - це вихідні, загальнообов'язкові установки, що на рівні норм і практик встановлюють, як саме досягається мета та виконується завдання. Вони виконують методологічну і регулятивну функції. У площині інформаційно-правового забезпечення для прокуратури ключовими є: законність, відкритість/прозорість (у межах дозволеного законом), достовірність і повнота інформації, пропорційність обмежень, відповідальність розпорядника за доступ. Для персональних даних - принципи належності, добросовісності, мінімізації, точності, обмеження строків зберігання, цілісності та конфіденційності, підзвітності (системний стандарт ЄС) [21].

Тоді, як завдання - це конкретні, вимірювані кроки (процедури, регламенти, інструменти), які служать реалізації мети з дотриманням принципів. У публічно-управлінській практиці завдання матеріалізуються у внутрішніх регламентах, інформаційних процедурах (реєстрація, оприлюднення, обмеження доступу, облік запитів) і технічних рішеннях (реєстри, системи документообігу, логування доступів). Прийняття Закону України «Про адміністративну процедуру» надало завданням процедурно-процесуальну визначеність (належне інформування, мотивовані акти, участь заінтересованих осіб, електронні форми взаємодії, пропорційність тощо) [22].

Загалом, категорії «мета - принципи - завдання» формують адміністративно-правовий режим - цілісну систему дозволів, заборон і приписів, що визначає «правила гри» для усіх суб'єктів владних повноважень у сфері інформації. У відношенні органів прокуратури цей режим проявляється у трьох взаємопов'язаних площинах: 1) Нормативно-цільова - визначення мети діяльності прокуратури («для чого» здійснюється обробка і використання інформації) через законодавчі функції; 2) Принципова - закріплення обов'язкових стандартів інформаційної діяльності - відкритість/прозорість, достовірність, пропорційність, правова визначеність, підзвітність; 3)

Процедурно-організаційна - оформлення завдань у процедури адміністративної діяльності, ведення реєстрів, оприлюднення, реагування на запити, забезпечення режимів обмеження, захисту і аудиту доступів.

Сам режим є похідною від поєднання цих трьох категорій, де мета задає критерій належності інформаційних дій прокуратури, принципи - рамки й межі, а завдання - технологію реалізації. Порушення будь-якого елемента породжує деформацію режиму, від неправомірного обмеження доступу (ігнорування принципу пропорційності) до некоректної обробки персональних даних і порушення принципів мінімізації, цілісності, підзвітності.

Виходячи із цього, можна з упевненістю сказати, що українське право вибудовує логічний ланцюг: мета доступу до інформації це забезпечення прозорості влади і реалізація права кожного на інформацію; принципи забезпечення доступу, це відкритість, максимально можливий доступ, своєчасність, достовірність; завдання розпорядників, це організувати доступ (визначити відповідальних осіб, оприлюднювати дані, вести облік документів), своєчасно й повно відповідати на запити. У межах прокуратури це комплекс доповнюється функціональною метою кримінального переслідування й представництва інтересів держави та процесуальними завданнями КПК (керівництво досудовим розслідуванням, підтримання обвинувачення), що вимагають дотримання спеціальних режимів доступу/обмежень (службова, таємна інформація).

Обробка персональних даних у прокуратурі (кадрові, процесуальні, дисциплінарні, реєстрові дані) вимагає збалансування мети публічного інтересу та принципів належної обробки (законність, мінімізація, точність, обмеження зберігання, безпека, підзвітність), що узгоджуються як із українським законом, так і з європейськими стандартами (GDPR art. 5) [21].

Що стосується саме мети інформаційно-правового забезпечення діяльності органів прокуратури України то її визначення є не лише теоретичною задачею, але й практичною передумовою ефективного функціонування прокурорської системи як елемента державного управління та контролю.

Правове підґрунтя цього висновку міститься в положеннях ст. 1 Закон України «Про прокуратуру», який встановлює, що «прокуратура України становить єдину систему, яка ... здійснює встановлені Конституцією України функції з метою захисту прав і свобод людини, загальних інтересів суспільства та держави» [13]. З цього випливає логіка, що мета інформаційно-правового забезпечення діяльності органів прокуратури повинна бути похідною від загальної мети прокуратури, оскільки воно є засобом реалізації покладених на неї функцій.

Дослідники підкреслюють, що інформаційне забезпечення органів прокуратури — це комплексна правова, організаційна та техніко-технологічна діяльність, спрямована на створення, обробку, передачу, зберігання та використання інформації, яка забезпечує реалізацію прокурорських функцій. Наприклад, Святослав Мазурик формулює інформаційне забезпечення як: «система інформаційних ресурсів органів прокуратури, які формують можливості для здійснення організаційних заходів, пов'язаних із досягненням цілей прокуратури та реалізацією її функцій» [2, с. 32]. Звідси випливає, що мета такого забезпечення - це не просто створення інформаційної інфраструктури, а її спрямування на реалізацію функцій і забезпечення цілей органів прокуратури.

Отже, з позиції адміністративного права мета інформаційно-правового забезпечення органів прокуратури України може бути витлумачена як формування правового, організаційного та інформаційно-технологічного середовища, що забезпечує ефективну, прозору, законну, оперативну, контрольовану діяльність органів прокуратури, а також реалізацію їх функцій у сфері підтримання державного обвинувачення, представництва інтересів держави, здійснення нагляду та іншого (згідно з профільним законодавством). Ця мета має стратегічний характер, вона виступає орієнтиром для побудови системи інформаційно-правового забезпечення.

На нашу думку, мету інформаційно-правового забезпечення слід розглядати через низку складових, кожна з яких вимагає окремого нормативно-правового і організаційного втілення, зокрема:

1. Забезпечення законності, реалізації прав і свобод людини і громадянина - органи прокуратури виходячи із ст. 2 Закону України «Про прокуратуру» мають функцію нагляду за додержанням законів, де інформаційно-правове забезпечення сприяє цьому за допомогою створення правового поля обміну інформацією, реагування на порушення, аналізу даних. Наприклад, у публікації С. Г. Гайдай відзначено, що органами прокуратури «зросла кількість скерованої до державних органів влади інформації про стан законності та протидію злочинності», що є елементом мети інформаційного забезпечення [23, с. 87].

2. Оперативність, ефективність, інтеграція інформаційно-аналітичних процесів - сучасні виклики (кібератаки, цифрові злочини, маніпуляція інформацією) вимагають, щоб органи прокуратури були забезпечені необхідною інформацією вчасно та якісно.

3. Прозорість, комунікація з суспільством та інтеграція з системою публічного управління - інформаційно-правове забезпечення має сприяти відкритості діяльності органів прокуратури, підзвітності суспільству, обґрунтованому довірі громадян до інституції. Як зазначено в дослідженні Мазурика: «інформаційне забезпечення діяльності органів прокуратури формує передумови для правильного сприйняття суспільством прокурорської діяльності шляхом надання ... повної, достовірної та своєчасної інформації про процеси, які відбуваються в системі прокуратури» [2, с. 32].

4. Інституційна безпека, захист інформації та правова культура - важливою складовою є захист інформаційних ресурсів, забезпечення безпеки персональних даних, належне ведення електронного документообігу, що також відповідає завданню прокуратури щодо законності [15, с. 109].

5. Сприяння цифровізації, інтеграції інформаційних систем та електронному управлінню - мета інформаційно-правового забезпечення має складову модернізації правового процесу, використання електронних систем документообігу, автоматизації, що підвищує ефективність органів прокуратури.

Підсумовуючи, можна констатувати, що визначення чіткої та комплексної мети інформаційно-правового забезпечення діяльності органів прокуратури

України є важливим етапом структуризації адміністративно-правового режиму функціонування прокурорської системи. Мета, як системоутворююча категорія, виступає орієнтиром для виокремлення принципів та формулювання завдань. Розроблене вище формулювання мети дозволяє інтегрувати правову, організаційну та технологічну площини діяльності органів прокуратури, спрямованої на реалізацію їх функцій у правовій державі. При цьому успішна реалізація цієї мети потребує відповідної нормативно-правової бази, технічної та кадрової підготовленості, наукового супроводу та системного моніторингу.

У свою чергу принципи в контексті діяльності органів прокуратури України виступають як правове підґрунтя їх інформаційно-правового забезпечення.

Вони дозволяють визначити, як має здійснюватися створення, обробка, передача, зберігання і використання інформації у прокурорській діяльності, які стандарти мають дотримуватись, з якою орієнтацією. В законодавстві України (ст. 3 Закону України «Про прокуратуру») закріплено, що діяльність органів прокуратури «ґрунтується на засадах: верховенства права та визнання людини, її життя і здоров'я, честі і гідності ...; законності, справедливості, неупередженості та об'єктивності; територіальності; презумпції невинуватості тощо» [13]. Хоча тут формулювання «засади», а не «принципи», проте концептуально в правознавчій літературі засади та принципи часто співвідносяться як споріднені категорії правового регулювання.

Для інформаційно-правового забезпечення органів прокуратури України можна виокремити специфічні принципи, що інтегрують загальноадміністративні й прокурорські засади (принципи) з вимогами інформаційного права. На нашу думку правильним є викладення систематизації таких принципів у трьох групах: базові загальні, спеціально інформаційно-правові та прокурорсько-інституційні.

До базових загальних принципів, які мають застосовуватись при інформаційно-правовому забезпеченні діяльності органів прокуратури, належать:

1. Принцип законності - діяльність органів прокуратури, як і будь-якого суб'єкта публічної адміністрації, має здійснюватись виключно на підставі та в межах закону, з урахуванням конституційних прав і свобод. В інформаційному контексті це означає, що обробка інформації, створення баз даних, передача матеріалів повинні бути правомірними, мати законодавче підґрунтя, відповідати встановленим правилам.

2. Принцип пріоритету прав і свобод людини та громадянина - цей принцип впливає з положень Конституції України і означає, що права і свободи людини є найвищою цінністю, невідчужуваними та непорушними. У діяльності органів прокуратури це має означати, що інформаційно-правове забезпечення не може порушувати права людини, в першу чергу право на приватність, захист персональних даних, право на справедливий розгляд.

3. Принцип рівності перед законом та об'єктивності - у адміністративному праві часто наголошується на тому, що всі суб'єкти знаходяться у рівних правових умовах, та що рішення мають прийматись на об'єктивній основі [24]. В інформаційно-правовому забезпеченні це означає, що інформаційні ресурси, доступ до них, обробка мають бути організовані без дискримінації, з об'єктивною оцінкою даних, без упередженості.

4. Принцип прозорості та відкритості - хоча не завжди прямо названий у класичних списках принципів адміністративного права, проте сучасна доктрина виділяє принципи «прозорості», «доступності», «відкритості» публічного управління [25]. Для прокуратури це означає, що інформаційне забезпечення має забезпечувати можливість контролю громадськості, аудиту, незалежного моніторингу, надання достовірної інформації відповідно до закону.

Окрім базових, окреслених вище, існує низка принципів, які виникають із самої природи інформаційно-правового забезпечення і мають специфічне значення для прокурорської сфери. Так наприклад:

1. Принцип достовірності інформації - інформаційно-правове забезпечення органів прокуратури базується на тому, що інформаційні дані, що генеруються, передаються, зберігаються, мають бути достовірними та перевіреними. Це

впливає з функції органів прокуратури здійснювати нагляд за додержанням законів та підтримувати державне обвинувачення - такі функції потребують надійної інформаційної бази. У правовому регулюванні це означає, що система документообігу, електронної комунікації, обміну має бути побудована з гарантіями, що інформація не піддається фальсифікації, маніпуляції.

2. Принцип інформаційної безпеки і захисту персональних даних - оскільки органи прокуратури працюють із значним обсягом інформації, часто конфіденційної, пов'язаної з досудовим розслідуванням, необхідність права на захист інформації та персональних даних є ключовою. Принцип інформаційної безпеки означає, що створення, зберігання та передача інформації організовується із врахуванням ризиків несанкціонованого доступу, витоку, зловживань, а також з метою дотримання прав осіб. На нашу думку, цей принцип виходить за межі класичних адміністративних принципів і відповідає сучасним викликам цифровізації та кібербезпеки.

3. Принцип оперативності та своєчасності інформаційного реагування - інформаційно-правове забезпечення повинно бути організоване таким чином, щоб інформація надходила, оброблялась і була використана своєчасно для здійснення функцій органів прокуратури. Завдання нагляду, підтримання державного обвинувачення, представництва інтересів громадянина або держави мають часову динаміку, де затримка, застарілий випадок, втрачена інформація знижують ефективність. Таким чином, принцип оперативності виступає нормою, що визначає часову параметризацію інформаційних процесів.

4. Принцип інтеграції та взаємодії інформаційних систем - у сучасній системі державного управління інформація рухається між багатьма суб'єктами: органами прокуратури, поліцією, судовою владою, державною системою електронного управління. Принцип інтеграції означає, що інформаційно-правове забезпечення повинно бути сумісним, взаємодіючим, володіти режимом обміну, стандартизації, інтероперабельності. Це забезпечує максимальне використання інформаційних ресурсів і зменшує дублювання, витрати, час.

5. Принцип публічної підзвітності та контролю - оскільки діяльність органів прокуратури пов'язана із захистом державних і публічних інтересів, їх інформаційна діяльність має бути підзвітною суспільству, підлягати контролю та оцінці. Принцип публічної підзвітності означає, що інформаційно-правове забезпечення має передбачати механізми звітності, аудиту, доступу до публічної інформації у межах закону. Це формує суспільну довіру і підвищує легітимність прокуратури.

У межах діяльності саме органів прокуратури принципи набувають специфічного застосування, а саме сформульовані на рівні інституційної організації прокуратури та її функцій. Тому до прокурорсько-інституційних принципів діяльності органів прокуратури в контексті інформаційно-правового забезпечення можна віднести:

1. Принцип незалежності прокурора та неупередженості - хоча універсально цей принцип належить до організації прокуратури в цілому, він має інформаційно-правове відгалуження, адже інформаційні процеси в прокуратурі повинні забезпечувати, щоб прокурор міг приймати рішення на підставі об'єктивної інформації, без зовнішнього неправомірного впливу, маніпуляції інформацією чи доступу, що компрометує незалежність. Відповідно, доступ до інформаційних систем, документообігу має бути захищений від втручання. У ст. 16 Закону України «Про прокуратуру» зазначено, що серед засад діяльності прокуратури є незалежність прокурорів, що передбачає гарантії від незаконного впливу [13].

2. Принцип територіальності та координації інформаційних потоків – виходить із положень ст. 3 Закону «Про прокуратуру» та означає, що інформаційні процеси мають враховувати територіальний поділ системи прокуратури, забезпечувати взаємодію між різними рівнями (місцевими, регіональними, центральними). В інформаційному забезпеченні це означає узгодження інформаційних систем, стандартизацію, передачу інформації між структурами із врахуванням географічного та адміністративного розмежування.

3. Принцип професійної етики, конфіденційності та захисту інформації - оскільки прокурорська діяльність пов'язана з високим рівнем відповідальності, конфіденційності, збереження слідчої та оперативної інформації, то принцип етики та конфіденційності стає невід'ємною складовою. Це включає норму, що інформація, що обробляється, передається чи зберігається, має охоронятись від неправомірного розголошення, витоку, зловмисного використання.

Проте, ми вважаємо, що побудова інформаційно-правової системи забезпечення діяльності органів прокуратури України вимагає не просто переліку принципів, але їх інтеграції в єдину модель. Принципи взаємопов'язані: базові задають фундамент, спеціальні формують конкретні вимоги, інституційні адаптують до прокурорської специфіки.

Так наприклад, принцип законності та пріоритету прав людини, наприклад, створюють нормативне поле, в якому будуються правила доступу до інформації, захисту даних, взаємодії з громадськістю. Принцип оперативності та інтеграції забезпечують, щоб інформація мала практичну цінність - не залишалась «архівом», а служила інструментом прокурорської діяльності. Принцип публічної підзвітності та контролю формує зворотний зв'язок із громадянським суспільством і підвищує довіру.

У системному розумінні, інформаційно-правове забезпечення діяльності органів прокуратури повинно бути організоване так, щоб жоден з принципів не залишався формальним положенням - всі вони мають бути відображені в нормативно-правових актах, внутрішніх регламентах, організаційних процедурах та технічних рішеннях. Наприклад, впровадження автоматизованих систем документообігу повинно враховувати принципи достовірності, безпеки, оперативності, та відкритості в межах законодавства.

Що стосується визначення завдань інформаційно-правового забезпечення діяльності органів прокуратури України, то в першу чергу варто відзначити, що у системі правового регулювання категорія «завдання» має операційний характер і виступає безпосереднім інструментом реалізації цілей, сформованих відповідно до визначених принципів. В адміністративному праві завдання є

конкретизованими напрямками організаційної, управлінської чи владно-реалізаційної діяльності органів публічної адміністрації, які уособлюють практичні дії щодо досягнення певної мети.

У контексті інформаційно-правового забезпечення діяльності органів прокуратури України завдання повинні бути витлумачені як правові, організаційні та технічні дії, спрямовані на формування, захист, обробку, передачу, збереження та використання інформації, необхідної для ефективної реалізації функцій прокуратури. Ці завдання можуть реалізовуватись як на рівні окремих прокурорів, так і через функціонування спеціалізованих структурних підрозділів, зокрема Департаменту інформаційних технологій, Департаменту документального забезпечення та Управління організаційного забезпечення Єдиного реєстру досудових розслідувань та інформаційно-аналітичної роботи Офісу Генерального прокурора.

Аналіз чинного законодавства України, зокрема Закону України «Про прокуратуру», а також низки підзаконних актів, дозволяє виокремити такі ключові завдання інформаційно-правового забезпечення діяльності органів прокуратури:

1. Забезпечення повного, своєчасного та безперервного інформаційного супроводу функцій прокуратури - органи прокуратури реалізують свої функції на підставі та через аналіз, обробку, зберігання і використання інформації, що отримується як від інших суб'єктів, так і генерується внутрішньо. Відповідно, ключовим завданням інформаційно-правового забезпечення є формування системи, яка забезпечить безперервність, оперативність і законність інформаційного обігу в органах прокуратури. Зокрема, це реалізується через адміністрування та супровід функціонування ІС «ЄРДР», ІАС «ОСОП», ІС «СЕД», автоматизованої системи «Кадри-WEB» та інших інформаційних систем, що документально підтверджено у наказах Генерального прокурора.

2. Формування та адміністрування внутрішніх інформаційних реєстрів і аналітичних систем - це включає адміністрування реєстрів досудових розслідувань, ведення статистичних баз даних, формування аналітичних звітів

про стан злочинності, хід розслідування та ефективність прокурорського нагляду. Це завдання покладено, зокрема, на Управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи, яке здійснює координацію статистики, звітності, наповнення ЄРДР, а також розробляє нові цифрові продукти для прокурорських потреб

3. Впровадження та супровід новітніх інформаційних технологій - одним із ключових завдань є технологічна трансформація органів прокуратури. Департамент інформаційних технологій виконує функцію впровадження та супроводу сучасних інформаційних та комунікаційних технологій, адміністрування комп'ютерних мереж, підтримки електронного підпису, технічного захисту інформації. Так, Департамент несе відповідальність за експлуатацію цифрового зв'язку, систем відеоконференцзв'язку, адміністрування інформаційних ресурсів та розробку технічної документації для цифрового документообігу. Він також координує роботу обласних відділів інформаційних технологій, формуючи єдину цифрову політику органів прокуратури України

4. Документування управлінської інформації та стандартизація діловодства - на рівні внутрішньої організації прокуратури важливе значення має завдання уніфікації документообігу. Департамент документального забезпечення здійснює організацію та контроль за дотриманням єдиного порядку оформлення, збереження, передання, знищення та архівування документів. Він забезпечує методичну підтримку обласних прокуратур, опрацьовує документи з грифами обмеженого доступу, забезпечує редагування та комунікацію через системи електронної взаємодії з іншими органами влади

5. Забезпечення інформаційної безпеки та захисту персональних даних - в умовах воєнного стану, кібератак і високих ризиків витоку службової інформації, окремим завданням інформаційно-правового забезпечення є реалізація заходів щодо технічного та правового захисту даних. Йдеться про адміністрування програмно-технічного комплексу захисту в ІС, проведення аудиту інформаційної

безпеки, впровадження політик захисту персональних даних, застосування електронного підпису та верифікації доступу до закритих систем.

6. Моніторинг, аналітика та забезпечення статистичної достовірності - завданням інформаційно-правового забезпечення є також статистичне супроводження прокурорської діяльності. Це включає збір, систематизацію, аналіз та візуалізацію даних, що стосуються кримінальної протиправності, організації прокурорського нагляду та виконання державних функцій. Підрозділи, відповідальні за статистичну звітність, мають забезпечити достовірність, повноту та актуальність даних у ЄРДР, ІАС «ОСОП» та в комунікації з міжнародними платформами.

7. Внутрішній контроль, аудит та інституційне навчання - це проведення внутрішнього аудиту інформаційної діяльності, розробка внутрішніх регламентів, підготовка аналітичних довідок, а також організація навчань для прокурорів і державних службовців у сфері роботи з інформаційними ресурсами. Ці функції реалізуються не лише у Департаменті інформаційних технологій, а й у структурі управлінь кадрів, які проводять підготовку щодо правил користування електронними підписами, захисту інформації, роботи в електронних базах та реєстрах.

Загалом, ми вважаємо, що завдання інформаційно-правового забезпечення діяльності органів прокуратури України охоплюють усі сфери прокурорської роботи - від цифрової трансформації до нормативно-організаційного регулювання, від зберігання інформації до її захисту, від внутрішньої звітності до комунікації із зовнішніми базами даних. Усе це формує підґрунтя для ефективного, сучасного, відкритого й захищеного функціонування органів прокуратури як інституції в демократичній державі.

Узагальнюючи результати дослідження, слід констатувати, що мета, принципи та завдання інформаційно-правового забезпечення діяльності органів прокуратури України становлять фундаментальні, системоутворюючі елементи, які забезпечують цілісність, ефективність і законність функціонування прокурорської системи в умовах сучасної цифровізації та інформаційної

взаємозалежності. Визначення мети інформаційно-правового забезпечення дозволяє формулювати стратегічні орієнтири прокурорської діяльності, принципи - забезпечують її ціннісно-нормативну стабільність, а завдання - конкретизують напрями практичного впровадження механізмів обігу, захисту та використання інформації. Такий взаємозв'язок сприяє побудові ефективної моделі інформаційного управління в прокуратурі, що відповідає вимогам демократичної правової держави, забезпечує належну реалізацію функцій прокуратури та зміцнення суспільної довіри до неї.

1.3. Нормативно-правові засади інформаційно-правового забезпечення діяльності органів прокуратури України

У сучасних умовах функціонування публічної влади інформаційне забезпечення набуває визначального значення, особливо для таких органів, як органи прокуратури. З огляду на адміністративно-правову природу цієї діяльності, інформаційне забезпечення органів прокуратури доцільно розглядати як самостійний правовий інститут, який охоплює сукупність нормативно-правових приписів, організаційних методів і технічних засобів, спрямованих на регламентацію правовідносин у сфері збору, обробки, збереження, передачі, використання та захисту інформації у межах реалізації прокурорських повноважень.

Інформаційно-правове забезпечення діяльності органів прокуратури формується на перетині інформаційного права та публічного управління, що зумовлює його комплексний і водночас подвійний характер. З одного боку, інформаційно-правовий аспект цього інституту полягає у врегулюванні відносин щодо правового статусу інформації, визначенні прав і обов'язків суб'єктів інформаційних відносин, а також у встановленні правових механізмів обмежень доступу, забезпечення захисту, збереження конфіденційності та недоторканності інформації. З іншого боку, адміністративно-управлінський аспект проявляється як організаційна функція, що спрямована на забезпечення ефективної реалізації завдань прокуратури через раціональне управління інформаційними потоками,

шляхом моніторингу, аналітичної обробки даних, внутрішньої комунікації, функціонування інформаційних систем, звітності, електронного документообігу тощо.

Системна інтеграція зазначених аспектів дає підстави характеризувати інститут інформаційно-правового забезпечення органів прокуратури як міжгалузевий правовий інститут, що поєднує елементи адміністративного регулювання та інформаційного права. Він ґрунтується на загально правових засадах, зокрема таких як право на доступ до інформації, прозорість діяльності публічної влади, захист персональних даних, а також на спеціальних положеннях, які встановлюють правові механізми функціонування органів прокуратури, передбачених нормативно-правовими актами.

У свою чергу в процесі вивчення нормативно-правових засад інформаційно-правового забезпечення діяльності органів прокуратури України особливого значення набуває вибір відповідної методології правового дослідження. Методологічна основа відіграє ключову роль не лише для уточнення меж предмета дослідження, а й для забезпечення його наукової достовірності, обґрунтованості та релевантності до сучасного стану адміністративного та інформаційного права.

На нашу думку методологічна досліджуваного питання базується на застосуванні таких підходів: 1) Системний підхід - дозволяє розглядати нормативно-правові засади інформаційно-правового забезпечення як частину цілісної системи публічного управління, в якій органи прокуратури виконують специфічні функції у сфері інформаційної безпеки, захисту персональних даних, забезпечення доступу до публічної інформації, обігу службової інформації тощо; 2) Структурно-функціональний підхід - дозволяє визначити місце кожного елементу нормативно-правового регулювання (законів, підзаконних актів, відомчих нормативів, внутрішніх інструкцій) у забезпеченні управлінської ефективності та юридичної визначеності діяльності органів прокуратури; 3) Аксиологічний підхід спрямований на виявлення ціннісних основ нормативно-правового забезпечення, що відображають демократичні, гуманістичні, правові

та етичні засади, зокрема, у питаннях дотримання прав людини в інформаційній сфері.

Початково слід зазначити, що поняття «засади» в праві трактується як базові положення, що закладають фундамент для побудови системи норм, інститутів і процедур. В контексті адміністративного права така категорія служить фоновим елементом, який формує правове середовище діяльності публічної влади. Нормативно-правові засади - це не лише констатація певних норм, але й їх взаємозв'язок, структурність, організуюча роль у правовій системі. У наукових дослідженнях поняття «інформаційно-правове забезпечення» розглядається як комплекс нормативно-правових заходів, спрямованих на регулювання інформаційних відносин у межах діяльності прокурорських органів [26, с. 339].

Виходячи з цього, нормативно-правові засади інформаційно-правового забезпечення слід розуміти як правову основу (нормативну, структурну, процедурну, ціннісну) діяльності органів прокуратури у сфері обігу, захисту, доступу до інформації, документообігу, електронного діловодства, баз даних тощо.

На нашу думку до нормативно-правових засад можна віднести: 1) Законодавчі акти, які прямо регулюють діяльність органів прокуратури в інформаційній сфері; 2) Законодавство про інформацію та доступ до неї; 3) Підзаконні акти, видані органами прокуратури або уповноваженими органами, які регламентують порядок організації інформаційного обігу, електронного документообігу, баз даних, захисту інформації; 4) Принципи, які лежать в основі цієї діяльності; 5) Інституційні механізми; 6) Процедурні норми.

У відповідній площині слід чітко диференціювати концептуальні рівні: 1) Інформаційно-правове забезпечення - ширше поняття, яке окреслює весь комплекс правового, організаційного, технічного, процесуального, інституційного забезпечення інформаційної діяльності органів прокуратури (доступ, обіг, захист, аналіз, використання інформації); 2) Нормативно-правові засади - складова цього комплексу, що відображає саме правову основу

(нормування: закони, підзаконні акти, принципи, процедури) інформаційно-правового забезпечення [2, с. 32].

Отже, нормативно-правові засади виступають юридичною рамкою, в межах якої реалізується інформаційно-правове забезпечення. Інформаційно-правове забезпечення охоплює також технічні, технологічні, організаційні механізми, що можуть виходити за межі нормативного регулювання (наприклад, вибір програмного забезпечення, алгоритмів штучного інтелекту), але завжди мають спиратися на нормативно-правові засади.

Також варто відзначити, що серед нормативно-правових засад інформаційного-правового забезпечення діяльності органів прокуратури особливе значення належить його функціональним засадам, які найбільш повно розкривають практичну природу інформації як інструмента управлінського впливу, контролю й координації у межах публічної адміністрації. У цьому контексті інформація постає не лише об'єктом правового регулювання, а й ключовим елементом управлінського процесу в системі органів прокуратури, засобом реалізації владних повноважень, а також гарантією законності, ефективності й публічної підзвітності їх діяльності.

З погляду адміністративного права, функціональні засади інформаційно-правового забезпечення слід тлумачити як комплекс цільових напрямів, завдань та процедур, що забезпечують реалізацію державної інформаційної політики в органах прокуратури, сприяють оптимізації управлінських процесів та посиленню правових гарантій громадян. Ці засади мають чітко виражений нормативний характер, закріплені у законодавчих та підзаконних актах, а також у внутрішньоорганізаційних документах. Їх призначення - це забезпечити правову визначеність і регламентованість усіх інформаційних процесів, починаючи зі збору даних і закінчуючи їх публічним оприлюдненням, з дотриманням таких принципів, як законність, об'єктивність, достовірність, інформаційна безпека.

Центральне місце серед функціональних засад посідає інформаційно-аналітична функція, яка покликана забезпечити науково обґрунтовану,

статистично підтвержену та документально верифіковану основу для управлінських рішень у межах діяльності органів прокуратури. Її зміст включає: а) системне збирання та узагальнення даних щодо стану законності, рівня злочинності, перебігу досудового розслідування, дисциплінарної практики, кадрових процесів; б) підготовку аналітичних звітів і прогнозних матеріалів для стратегічного та оперативного планування; в) використання інформаційно-аналітичних технологій, таких як електронні бази даних, аналітичні панелі, реєстри; г) моніторинг ефективності діяльності органів прокуратури із застосуванням цифрових систем оцінювання.

Іншою важливою функцією є комунікаційно-інформаційна, що забезпечує ефективну взаємодію між органами прокуратури, іншими державними інституціями, громадськістю та суб'єктами правовідносин. Вона є проявом принципу відкритості діяльності органів публічної влади та конкретизується у Законі України «Про доступ до публічної інформації», а також у відповідних положеннях європейських стандартів щодо ролі прокуратури (European Guidelines on the Role of Prosecutors) [27, с. 144].

Ця функція реалізується через такі напрями: а) забезпечення доступу до публічної інформації (через офіційні вебресурси, бази даних, механізми інформаційних запитів); б) налагодження електронної взаємодії з судами, органами досудового розслідування, державними реєстрами (зокрема обмін процесуальними документами); в) формування внутрішніх інформаційних каналів (електронний документообіг, службові накази, цифрові розсилки, корпоративна пошта). У науково-теоретичному розумінні зазначена функція відображає адміністративно-правову природу управління інформаційними потоками в межах компетенції прокуратури, як планування, так і контроль та координацію.

До числа базових належить і інформаційно-захисна функція, що спрямована на охорону інформації, яка становить державну, службову або професійну таємницю, а також на захист персональних даних і конфіденційних відомостей. Зміст цієї функції охоплює не лише технічні аспекти, а й глибокі правові

питання, зокрема дотримання балансу між правом на інформацію і обов'язком держави захищати її конфіденційність у кримінальному провадженні, забезпечуючи при цьому законні інтереси сторін.

У тісному зв'язку з цим функціонує інформаційно-координаційна функція, яка забезпечує міжвідомчу взаємодію, обмін інформацією, стандартизацію форматів і процедур у межах публічного управління. Йдеться про створення єдиного інформаційного простору, в якому обіг даних є оперативним, сумісним та надійно захищеним.

Не менш важливою є інформаційно-превентивна функція, яка передбачає використання інформаційних ресурсів для запобігання правопорушенням, формування правової культури, підвищення рівня довіри до органів прокуратури. Вона реалізується через: а) інформування суспільства про результати наглядової діяльності; б) оприлюднення статистичних та аналітичних даних на відкритих платформах; в) просвітницьку діяльність, спрямовану на правове виховання та протидію корупції.

Функції інформаційно-правового забезпечення органів прокуратури утворюють взаємопов'язану систему. Інформаційно-аналітична функція формує дані, комунікаційна - поширює їх, захисна - гарантує безпеку, координаційна - забезпечує узгодженість, а превентивна - формує соціальну легітимність і довіру до прокурорських органів [28, с. 14].

Загалом, функціональні засади інформаційно-правового забезпечення є практичним втіленням нормативно визначеної ідеї організаційної побудови інформаційно-правових процесів. Вони: а) забезпечують єдність права і управління; б) дозволяють інтегрувати інформаційні потоки в систему публічної адміністрації; в) гарантують правову визначеність кожної дії в межах прокурорської діяльності; г) створюють передумови для цифрової трансформації прокуратури як сучасного органу публічної влади, здатного функціонувати в умовах електронного урядування.

Крім того, ми вважаємо, що контексті функціональних засад нормативно-правового регулювання інформаційно-правового забезпечення діяльності

органів прокуратури України особливої актуальності набуває питання правового врегулювання використання цифрового підпису посадовими особами. Як інструмент цифрової ідентифікації, кваліфікований електронний підпис (КЕП) виконує функцію підтвердження юридичної значущості документів в електронній формі, забезпечує достовірність переданої інформації, засвідчує авторство та гарантує цілісність даних у межах адміністративної діяльності органів прокуратури.

Цифровий підпис у цьому аспекті слід розглядати не лише як технічний засіб автентифікації, а як функціональний елемент управлінської дії, інтегрований у регламентовані інформаційні процедури прокуратури. Йдеться, зокрема, про електронне погодження документів, офіційне листування, затвердження розпорядчих актів, цифрове підписання статистичних звітів та організаційних матеріалів, що циркулюють між структурними підрозділами органів прокуратури, а також у взаємодії з іншими органами державної влади. Використання цифрового підпису є не тільки інструментом ідентифікації, а й елементом процедурної відповідальності, внутрішнього контролю та персоніфікованого адміністрування.

Правові підстави використання КЕП у діяльності органів прокуратури визначаються положеннями Закону України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII [29], Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV [30], а також відомчими нормативно-правовими актами, зокрема внутрішніми наказами Офісу Генерального прокурора, що регламентують правила застосування КЕП у внутрішньому електронному документообігу, захисті інформації та в межах цифрового діловодства. Застосування електронного підпису є обов'язковим під час роботи з Єдиним реєстром досудових розслідувань (ЄРДР), системою електронного документообігу (СЕД), а також при підготовці офіційних запитів, відповідей на звернення, взаємного обміну інформацією між органами державної влади.

З адміністративно-правової точки зору, використання цифрового підпису посадовими особами органів прокуратури становить форму реалізації адміністративної процедури в цифровому форматі. Це відповідає положенням Закону України «Про адміністративну процедуру» від 17.11.2021 № 2073-IX [22], який закріплює засади правомірного застосування електронних засобів комунікації в межах публічного адміністрування. У такому сенсі КЕП є не лише інструментом ідентифікації особи, але й засобом забезпечення прозорості, підзвітності, правової визначеності дій службових осіб органів прокуратури, а також превентивним інструментом запобігання службовим зловживанням через фіксацію та атрибуцію управлінських дій.

Таким чином, цифровий підпис у системі органів прокуратури виконує не лише підтверджувальну та засвідчувальну функцію, а й набуває статусу правового інструмента реалізації функціональної спроможності органів прокуратури у сфері інформаційного забезпечення, формуючи невід'ємну частину їх електронної інституційної ідентичності.

У межах дослідження важливе місце також посідають інституційні та організаційні засади, які поєднують правові механізми реалізації інформаційної політики з практичними моделями управління. Інституційні засади охоплюють сукупність правових норм, що визначають коло суб'єктів, уповноважених здійснювати регламентацію, адміністрування та контроль у сфері інформаційного забезпечення, а також обсяг їх повноважень, відповідальність і механізми взаємодії. Натомість організаційні засади відображають внутрішні форми реалізації інституційних компетенцій (діловодні процедури, цифрові інструменти, моделі обміну інформацією, механізми внутрішнього контролю та управління інформаційними потоками).

Загалом можна стверджувати, що інституційні й організаційні засади формують підґрунтя ефективного та легітимного інформаційного середовища в органах прокуратури. Вони забезпечують: а) чітке визначення суб'єктів і відповідальних осіб; б) упорядкування внутрішньої взаємодії; в) формалізацію

адміністративних процедур; г) підвищення прозорості та підзвітності; г) наближення до європейських стандартів електронного врядування.

Разом із тим, доцільно підкреслити значущість системи нормативно-правових актів, що визначають засади нормативно-правового регулювання інформаційно-правового забезпечення діяльності органів прокуратури України. Одним із ключових чинників інституційної спроможності органів прокуратури в умовах сучасного демократичного правопорядку є належне нормативне врегулювання інформаційної діяльності, яка охоплює всі напрямки функціонування, від супроводу кримінальних проваджень і захисту прав громадян до представництва інтересів держави в судах.

У цьому контексті система нормативно-правових актів постає як багатопланова, структурована й динамічна правова конструкція. Її розвиток відбувається в умовах постійних трансформацій інформаційного середовища, посилення вимог до відкритості влади та необхідності збереження функціональної конфіденційності, характерної для органів прокуратури.

Система нормативно-правових актів, що визначає інформаційне забезпечення органів прокуратури, не є простою сукупністю документів. Це багаторівнева правова архітектура, що охоплює врегулювання у сферах інформаційного адміністрування, взаємодії, захисту даних, електронного документообігу, доступу до публічної інформації, кібербезпеки, захисту персональних даних та права громадян на отримання інформації про діяльність прокуратури. Ця система постійно адаптується до викликів цифровізації, змін очікувань суспільства та появи нових ризиків. Її ефективність забезпечується системністю, де акти діють у взаємозв'язку, а не ізольовано.

З позицій адміністративного права, ця система включає нормативні акти різних рівнів, від конституційного до підзаконного та міжнародно, які формують правові рамки реалізації інформаційної політики, визначають гарантії прав у сфері інформаційних відносин та регламентують механізми обміну, доступу, обробки й захисту інформації. Крім того, вона має організаційно-

функціональний характер, оскільки безпосередньо впливає на практику прокурорської діяльності. Так наприклад:

1. Конституційно-правовий рівень охоплює положення Конституції України, зокрема ст. 34, яка гарантує право на свободу думки та слова, а також на збирання, зберігання й поширення інформації. Статті 3, 6, 19, 92, 131-1 формують підвалини публічного управління, верховенства права й організації державної влади, що мають значення для інформаційної діяльності прокуратури [5].

2. Законодавчий рівень охоплює: 1) Загальне інформаційне законодавство: а) Закон України «Про інформацію» - визначає правові засади поводження з інформацією [31]; б) Закон України «Про доступ до публічної інформації» - регулює процедури надання, збереження та обмеження доступу до інформації [32]; в) Закон України «Про захист персональних даних» - визначає правовий режим персональних даних, зокрема у межах кримінальних проваджень і кадрової роботи [33]; г) Закон України «Про електронні документи та електронний документообіг» - визначає юридичну силу та вимоги до електронних документів, що актуально в умовах цифровізації [30].

2) Спеціальне законодавство: а) центральним актом є Закон України «Про прокуратуру», який визначає статус, структуру та функції органів прокуратури, а також закріплює обов'язки щодо інформування суспільства, забезпечення прозорості та обміну даними з іншими суб'єктами публічної влади [13]; б) Кримінальний процесуальний кодекс України - регламентує інформаційні аспекти у кримінальних провадженнях [14]; в) Закон «Про національну безпеку України» - встановлює засади кіберзахисту [34]; г) Закон «Про державну таємницю» - визначає правовий режим секретної інформації [35].

3. Підзаконний рівень охоплює акти, що деталізують норми законів: 1) Наказ Генерального прокурора України № 266 від 28 грудня 2018 року «Про впровадження в промислову експлуатацію та забезпечення функціонування інформаційної системи «Система електронного документообігу органів прокуратури України» [36]; 2) Наказ Генерального прокурора України № 27 від

12 лютого 2019 року «Про затвердження Тимчасової інструкції з діловодства в органах прокуратури України» [37]; 3) Інші положення щодо зберігання, архівування, розсекречення документів, роботи з інформаційними системами; 4) Спільний наказ Офісу Генерального прокурора та Міністерства внутрішніх справ України від 22 листопада 2021 року № 371/846 «Про затвердження Порядку електронної інформаційної взаємодії між Офісом Генерального прокурора та Міністерством внутрішніх справ України» - ним регламентовано порядок обміну даними між ЄРДР, який адмініструється органами прокуратури, та інформаційними ресурсами МВС [38]. Тут важливо зазначити, що підзаконні акти мають внутрішньо-організаційне значення, проте саме вони визначають практичні механізми реалізації інформаційного забезпечення в межах повсякденної діяльності органів прокуратури, у тому числі технічні параметри систем зберігання даних, кібербезпеки, електронної звітності.

4. Міжнародно-правові акти та стандарти: Зокрема: 1) Конвенція про захист прав людини і основоположних свобод 1950 року, ст. 10 якої гарантує свободу отримання і передавання інформації [39]; 2) Конвенція Ради Європи про доступ до офіційних документів 2009 року [40]; 3) Директива ЄС 2016/680 про захист персональних даних у правоохоронній сфері [41]; 4) Стандарти Ради Європи щодо прокуратури (Європейські керівні принципи щодо функцій прокурора поза кримінальним процесом), які встановлюють рекомендації щодо прозорості та звітності [42]. Попри рамковий характер, вони істотно впливають на формування концепту інформаційної відкритості прокуратури, забезпечуючи гармонізацію національного законодавства з міжнародними підходами.

Таким чином, система нормативно-правових актів, що визначає нормативно-правові засади інформаційного-правового забезпечення діяльності органів прокуратури України, є багаторівневою та міжгалузевою. Вона об'єднує конституційні норми, адміністративні, інформаційні й процесуальні положення, підзаконні інструменти регулювання а також міжнародно-правові документи. Її сучасний стан вимагає подальшої систематизації, цифрової модернізації та адаптації до європейських стандартів, з урахуванням балансу між відкритістю,

правами громадян і необхідною конфіденційністю в умовах публічного управління [43, с. 751-752].

У межах аналізу нормативно-правових засад інформаційно-правового забезпечення діяльності органів прокуратури України особливої уваги набуває питання системності правового регулювання, його багаторівневого характеру та спроможності забезпечити належне функціонування інституту інформаційної взаємодії в межах публічного управління. З огляду на адміністративно-правову природу діяльності органів прокуратури, інформація відіграє не лише технічну, але й управлінську функцію, будучи засобом реалізації державного нагляду, процесуального керівництва та захисту інтересів держави.

Однією з ключових характеристик нормативно-правових засад інформаційного забезпечення в системі прокуратури є їх розгалужена структура. Правові приписи, що регулюють інформаційні процеси, закріплені в актах різної юридичної сили: від законів України до підзаконних нормативних актів Генерального прокурора, положень про функціонування інформаційних реєстрів, інструкцій з документообігу тощо. Така фрагментарність ускладнює інтегральне сприйняття правової системи інформаційного забезпечення, породжуючи колізії, дублювання норм або прогалини у правозастосуванні.

У цьому контексті важливо наголосити на недосконалої нормативній деталізації функціонального статусу суб'єктів, задіяних у здійсненні інформаційної діяльності в органах прокуратури. Ідеться, зокрема, про відсутність чітких регламентів для інформаційних адміністраторів, модераторів баз даних, уповноважених з питань захисту персональних даних та електронного документообігу. Невизначеність їхніх повноважень, прав і обов'язків послаблює інституційний контроль, розмиває зони відповідальності та може ускладнювати внутрішні розслідування у разі порушення інформаційної дисципліни.

Ще одним вразливим елементом нормативно-правових засад є повільне реагування законодавства на динамічні технологічні зміни. Правові акти здебільшого не враховують використання хмарних сервісів, інтеграцію штучного інтелекту в аналітичні модулі, обмін даними через API тощо.

Внаслідок цього відбувається цифрова модернізація без належного юридичного супроводу, що створює ризики витоку інформації, неналежної обробки персональних даних та порушення норм кримінального процесуального законодавства.

Важливою складовою нормативно-правових засад є також правове регулювання інформаційної взаємодії між органами прокуратури та іншими суб'єктами публічної адміністрації. Хоча на сьогодні така взаємодія базується на чинних законодавчих та підзаконних актах, вона залишається роз'єднаною - окремі нормативні документи регулюють обмін даними з Міністерством внутрішніх справ, Міністерством юстиції, Службою безпеки України, НАЗК тощо. Відсутність єдиного узагальнюючого нормативного акта, що окреслював би порядок, технічні вимоги, захисні протоколи та зобов'язання сторін, ускладнює ефективне правозастосування в межах інформаційного середовища.

З урахуванням сучасного стану нормативно-правових засад інформаційно-правового забезпечення діяльності органів прокуратури України, логічним є формулювання ключових напрямів їх подальшого вдосконалення. Вони охоплюють комплекс організаційних, технологічних і правових змін, спрямованих на забезпечення цілісності, прозорості та ефективності функціонування інформаційної інфраструктури прокуратури. Так наприклад:

1. Удосконалення законодавчої бази, зокрема ініціювання розробки Концепції інформаційної політики органів прокуратури як стратегічного документа, що визначатиме підходи до управління інформацією, цифровізації та захисту даних.

2. Встановлення інституційної моделі інформаційного адміністрування в системі прокуратури шляхом законодавчого або підзаконного визначення повноважень суб'єктів, відповідальних за формування, супровід, захист і обробку інформації, а також механізмів їхньої взаємодії.

3. Оновлення підзаконного нормативного масиву, насамперед наказів, інструкцій і положень, що регулюють діловодство, обіг інформації, ведення

електронних реєстрів, включно з адаптацією до цифрових форматів, безпечного електронного обміну та фіксації цифрових слідів адміністративних дій.

4. Нормативна фіксація цифрових інструментів, які застосовуються в органах прокуратури, включаючи автоматизовані аналітичні системи, алгоритмічну обробку даних, машинне навчання та штучний інтелект, із одночасним визначенням правових меж їх застосування, технічних вимог та критеріїв достовірності результатів.

5. Регулювання міжвідомчої інформаційної взаємодії, що передбачає як формалізацію технічних протоколів (API, шлюзи, інтерфейси), так і нормативне закріплення правових підстав для обміну даними між органами прокуратури та іншими суб'єктами публічної адміністрації.

6. Упровадження механізмів сертифікації та контролю інформаційних систем, які використовуються в діяльності органів прокуратури, зокрема шляхом запровадження вимог до їх сертифікації та здійснення незалежного аудиту процедур зберігання, обробки й передачі даних.

7. Нормативне забезпечення захисту інформаційних прав осіб, персональні дані яких обробляються в межах прокурорської діяльності — потерпілих, свідків, захисників, посадових осіб тощо. Йдеться про встановлення чітких юридичних гарантій прав на доступ, обмеження використання та виправлення інформації.

Таким чином, зазначені напрями мають стати основою для цілісного оновлення нормативно-правових засад інформаційно-правового забезпечення діяльності органів прокуратури України, що відповідатиме сучасним стандартам цифрового врядування, вимогам правової визначеності та публічної підзвітності.

Отже, нормативно-правові засади інформаційно-правового забезпечення діяльності органів прокуратури України становлять цілісну правову основу, яка охоплює законодавчі, підзаконні та відомчі акти, що регулюють функціонування інформаційних процесів у межах прокурорської діяльності. Вони не лише визначають межі допустимої поведінки у сфері обігу, зберігання та захисту інформації, але й формують інституційно-процедурні механізми реалізації функцій органів прокуратури в інформаційній площині. Ретельне теоретичне

осмислення цього феномену дає змогу окреслити його структуру, методологічні межі, місце в системі адміністративного права, а також виокремити засади, що потребують оновлення відповідно до викликів цифрової трансформації, стандартів правової держави та вимог інформаційної безпеки. Таким чином, формування чіткої нормативно-правової бази інформаційно-правового є запорукою легітимності, ефективності та прозорості діяльності органів прокуратури в умовах сучасного інформаційного суспільства.

Висновки до розділу 1

1. Інформаційно-правове забезпечення діяльності органів прокуратури України є багатоаспектним правовим інститутом, який поєднує в собі елементи інформаційного, адміністративного, конституційного та кримінального процесуального права. Його сутність полягає у створенні та функціонуванні нормативно врегульованої, інституційно організованої, процесуально визначеної та технологічно забезпеченої системи збирання, обробки, зберігання, використання, захисту та обміну інформацією, що необхідна для реалізації функцій органів прокуратури в умовах публічного управління. Особливістю цього інституту є його системність, міжгалузевість і внутрішня інтегрованість, що зумовлює необхідність його комплексного правового осмислення у площині адміністративного права.

2. Історико-правовий аналіз, засвідчує, що генезис інформаційно-правового забезпечення органів прокуратури України має чітко виражену етапність і відображає глибокі зміни у підходах до інформаційно-правового регулювання. Виділено чотири ключові періоди: а) радянський етап - характеризувався репресивним та ізоляціоністським підходом до обігу інформації, централізованим контролем, відсутністю доступу до даних і домінуванням державної таємниці; б) пострадянський етап - започаткував становлення інформаційного суверенітету, був відзначений прийняттям Конституції України, Закону «Про інформацію», спробами інституціоналізації політики відкритості; нормативно-інституційний етап - передбачав системне формування

законодавства про доступ до публічної інформації, персональні дані, електронне врядування; цифровий етап - ознаменований впровадженням цифрової трансформації, електронного документообігу, проєкту «Держава у смартфоні», концепції інтероперабельності, кібербезпеки та інформаційної стійкості. Сукупність цих етапів свідчить про перехід від фрагментарного і декларативного регулювання до побудови цілісної цифрово-правової системи інформаційного адміністрування прокуратури.

3. Інформаційно-правове забезпечення діяльності органів прокуратури України є комплексною системою, що охоплює нормативні, організаційні, технологічні, кадрові, контрольно-наглядові та правозахисні елементи. Кожен із них виконує важливу функцію в забезпеченні законної та ефективної прокурорської діяльності. Нормативний компонент формує правову базу обігу інформації, організаційний - забезпечує управління інформаційними процесами, а технологічний - створює цифрову інфраструктуру. Кадровий блок гарантує професійну підготовку, контрольно-наглядовий - моніторинг і відповідальність, а правозахисний - дотримання прав людини в інформаційній сфері. Злагоджене функціонування цих елементів визначає системність і результативність інформаційно-правового забезпечення прокурорської діяльності.

4. Мета, принципи та завдання інформаційно-правового забезпечення формують методологічну основу правового режиму функціонування органів прокуратури. Метою є формування ефективного, правового, безпечного та прозорого середовища для виконання конституційно визначених функцій прокуратури. Принципи - законності, відкритості, пропорційності, конфіденційності, достовірності, публічної підзвітності, оперативності та інші, виконують роль орієнтирів, що регламентують спосіб реалізації цієї мети. Завдання, у свою чергу, матеріалізуються у вигляді нормативних приписів, адміністративних процедур, внутрішніх регламентів і технічних рішень, які забезпечують повноцінне функціонування інформаційного середовища прокуратури. Такий триєдиний підхід дозволяє забезпечити цілісність,

керованість і результативність інформаційно-правової системи прокуратури у правовій державі.

5. Система нормативно-правових засад, що визначає інформаційно-правове забезпечення діяльності органів прокуратури України, є багаторівневою, структурованою та функціонально взаємопов'язаною. Вона охоплює норми конституційного, законодавчого, підзаконного та міжнародного права, які забезпечують правову визначеність у сфері обігу, захисту та доступу до інформації. Така система не лише формує нормативну базу, але й виконує організаційно-функціональну роль, безпосередньо впливаючи на практику прокурорської діяльності в умовах цифровізації. Її подальший розвиток має бути спрямований на систематизацію, оновлення підзаконних актів та імплементацію міжнародних стандартів із урахуванням особливостей функціонування органів прокуратури.

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ
ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ
ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

2.1. Види інформаційного-правового забезпечення діяльності органів прокуратури України

Сучасна модель діяльності органів прокуратури України дедалі більше ґрунтується на інтенсивному використанні інформаційних ресурсів, цифрових технологій та мережевої взаємодії з іншими суб'єктами публічної влади. Це радикально змінює уявлення про допоміжний характер інформаційного супроводу. Інформаційно-правове забезпечення перетворюється на один із базових елементів адміністративно-правового статусу органів прокуратури, що визначає реальну спроможність виконувати конституційні функції у сфері підтримання державного обвинувачення, представництва інтересів громадянина або держави та нагляду за додержанням законів [44, с. 120].

У законодавстві інформаційно-правове забезпечення опосередковано впливає з положень Закону України «Про інформацію», який закріплює правові основи інформаційних відносин, види інформації, принципи її обігу, режим доступу та обов'язки суб'єктів владних повноважень щодо її збирання, зберігання, поширення і захисту [31]. Зі свого боку, спеціальні закони, зокрема Закон України «Про доступ до публічної інформації», деталізують вимоги прозорості та відкритості для органів публічної влади, включно з органами прокуратури, через встановлення процедур доступу до документів, реєстрів, статистичних даних та іншої офіційної інформації [32]. У працях, присвячених адміністративно-правовому регулюванню інформаційно-правового забезпечення діяльності органів прокуратури, обґрунтовано, що інформаційно-правове забезпечення слід розуміти як комплексну систему норм, процедур, організаційних структур і технічних рішень, спрямованих на створення, оброблення, використання, захист і поширення інформації в процесі реалізації

прокурорських повноважень [2, с. 30–31].

Наукові дослідження у сфері правової інформатики й інформаційного права підкреслюють, що без чіткої структуризації інформаційних потоків, визначення режимів доступу та відповідальних суб'єктів неможливо забезпечити ефективне управління в органах публічної влади [45, с. 22]. Це повною мірою стосується і органів прокуратури, де інформація одночасно виступає: а) матеріальною основою для прийняття процесуальних рішень; б) інструментом управління організаційною системою прокуратури; в) об'єктом правового захисту (наприклад, персональні дані, конфіденційна, службова чи таємна інформація).

Окремі автори, досліджуючи інформаційно-правові аспекти прокурорської діяльності, уже роблять спроби розмежувати різновиди інформації, що циркулює в органах прокуратури, за режимом доступу, функціональним призначенням і зв'язком із реалізацією тих чи інших функцій прокуратури [2, с. 33-34]. Однак, попри наявність окремих класифікацій інформаційних ресурсів, системна типологія саме видів інформаційно-правового забезпечення органів прокуратури як самостійного інституту адміністративного права досі не сформована. У результаті нормативна база, внутрішньо-організаційні регламенти, інформаційні системи та практичні управлінські рішення розвиваються фрагментарно, без єдиного концептуального підходу до видів, критеріїв та внутрішньої побудови системи інформаційно-правового забезпечення.

У загальній теорії інформаційного права справедливо наголошується, що робоча класифікація видів інформаційно-правового забезпечення є не лише пізнавальним, а й конструктивним інструментом, вона задає рамки для вибору моделей регулювання, визначення пріоритетів цифрової трансформації, побудови електронних реєстрів, організації документообігу й оцінювання ризиків інформаційної безпеки. Для прокуратури, яка перебуває під постійним тиском як з боку суспільства (вимоги відкритості), так і з боку криміногенного середовища (загрози втручання, витоків і маніпуляції даними), така системна класифікація набуває не меншого значення, ніж традиційні класифікації форм і методів прокурорської діяльності [46, с. 134].

Крім того, варто ми вважаємо що потреба в класифікації обумовлена кількома чинниками. По-перше, багатоманітність інформаційних процесів у роботі органів прокуратури - від збору даних, обліку, аналізу, передачі до публічного інформування, свідчить про те, що інформаційно-правове забезпечення не є монолітним явищем, а складається з різних компонентів, що мають власні логіку та специфіку. По-друге, правове регулювання інформаційної діяльності органів прокуратури містить цілу низку законодавчих актів, підзаконних нормативів, внутрішніх інструкцій і технологічних рішень. Відсутність єдиної системної моделі класифікації веде до фрагментарності підходів, дублювання повноважень, невизначеності у межах компетенції, що знижує ефективність як управління, так і відповідальності у сфері інформаційно-правового забезпечення. По-третє, з точки зору адміністративного права, реалізація публічних повноважень органів прокуратури передбачає чіткі процедури обміну інформацією, контролю над нею, а також захисту інформаційних прав і свобод громадян. Тому класифікація видів інформаційно-правового забезпечення є засобом заснування єдиних підходів до організації внутрішньої та зовнішньої інформаційної діяльності, регламентування процесів, стандартизації форм документування, автоматизації та звітності.

У системному аспекті класифікація створює структуру, яка дозволяє виділити окремі категорії забезпечення, наприклад, інформаційно-правове забезпечення процесуального керівництва, організаційно-управлінське інформаційне забезпечення, забезпечення публічної комунікації та інформаційної безпеки. Кожна з цих категорій має свою специфіку, зміст, суб'єкти, механізми і ризики. Це означає, що класифікація не має бути лише тематичною, але й структурованою за функціональним призначенням і правовою природою.

Водночас, важливим є те, що класифікація має служити інструментом аналітичної оцінки. Саме за її допомогою можливо здійснювати діагностику стану інформаційно-правового забезпечення, визначати його слабкі ланки,

ступінь відповідності нормативно-правовій базі, технічному рівню, вимогам інформаційної безпеки. Як зазначає Г. А. Терещук у статті про інформаційну безпеку органів прокуратури, процеси забезпечення інформації потребують систематизації для якісного функціонування [15, с. 111].

Виходячи із цього ми вважаємо, що потреба в класифікації видів інформаційно-правового забезпечення діяльності органів прокуратури України є обґрунтованою як з теоретичної, так і з практичної точки зору. Теоретично вона дозволяє упорядкувати знання про інформаційну складову прокурорської функції, формалізувати поняття, виділити категорії та механізми. Практично - забезпечує підвищення ефективності діяльності, координацію інформаційних процесів, підвищення прозорості та захищеності інформації, стандартизацію процедур і відповідальності.

Зрештою, класифікація дозволяє оновити стратегічне бачення прокуратури як органу, що не лише контролює законність, а й володіє складною інформаційною інфраструктурою, здатною реагувати на виклики XXI століття, включаючи кіберзагрози, гібридні впливи, спотворення цифрових доказів тощо.

Тому ми вважаємо, що постановка питання про види інформаційно-правового забезпечення діяльності органів прокуратури України є логічним кроком розвитку національної доктрини адміністративного права. Вона дозволяє перейти від опису окремих інформаційних процесів до побудови цілісної моделі, де види інформаційно-правового забезпечення чітко співвіднесені з функціями прокуратури, рівнями правового регулювання, режимами доступу та технологічними форматами реалізації (паперовий, електронний, змішаний обіг інформації).

На нашу думку, класифікація видів інформаційно-правового забезпечення діяльності органів прокуратури України є не просто технічною схемою впорядкування інформаційних потоків, а ключовим методологічним інструментом побудови цілісної моделі прокурорської діяльності в умовах інформатизації. Вона дозволяє відобразити багаторівневу природу інформаційних процесів, що обслуговують як реалізацію конституційно

визначених функцій органів прокуратури (ст. 2 Закону України «Про прокуратуру»), так і внутрішню організаційно-управлінську діяльність, зовнішню комунікацію та забезпечення інформаційної безпеки [13]. Саме через призму класифікації стає можливим побачити, що «інформаційно-правове забезпечення прокуратури» – це не один вид діяльності, а ціла система спеціалізованих видів інформаційно-правового забезпечення, кожен з яких має власний правовий режим, суб'єктний склад, технологічні засоби та ризики.

Наукові дослідження останніх років підтверджують, що без розмежування видів інформаційно-правового забезпечення діяльності прокуратури важко говорити про її інституційну спроможність у цифровому середовищі. Так, С. Мазурик, аналізуючи органи прокуратури як специфічного суб'єкта інформаційних відносин, пропонує детальну класифікацію інформації, якою оперують прокурори: за змістом, правовим режимом, функціональним призначенням, сферою застосування, формальним закріпленням і спрямовуючим впливом [7, с. 34]. Водночас, як слушно підкреслюють А. Колесніков і С. Банах, саме інформаційне забезпечення прокурорської діяльності являє собою «систему правовідносин, що виникають у процесі збирання, накопичення, обробки, збереження і використання інформації органами прокуратури та щодо органів прокуратури», що вимагає комплексного – а не фрагментарного – підходу до його організації [47, с. 130].

Виходячи із цього, ми вважаємо за доцільне побудувати багатовимірну класифікацію видів інформаційно-правового забезпечення діяльності органів прокуратури України, яка включає принаймні чотири групи критеріїв: 1) функціональне призначення; 2) джерело і походження інформації; 3) правовий режим і рівень доступу; 4) форма реалізації та ступінь стандартизації. Так наприклад:

1. Функціональна класифікація видів інформаційно-правового забезпечення. Першим і, безперечно, базовим видом є інформаційно-правове забезпечення реалізації процесуальних повноважень органів прокуратури. Його змістом є правове й організаційне врегулювання інформаційних процесів, що

пов'язані з: внесенням відомостей до Єдиного реєстру досудових розслідувань (ЄРДР); документуванням процесуальних рішень; збиранням, зберіганням та оцінкою доказової інформації; взаємодією з органами досудового розслідування та судами; відображенням результатів прокурорського нагляду у відповідних базах даних і реєстрах.

Нормативне підґрунтя цього виду формують, зокрема, Закон України «Про прокуратуру», Кримінальний процесуальний кодекс України, Закон України «Про інформацію», Закон України «Про захист персональних даних», а також спеціальні відомчі акти, що встановлюють порядок ведення обліків, реєстрів та архівів. Відповідно до підходу С. Мазурика, саме в цій площині інформаційне забезпечення набуває вигляду «сукупності даних, які є актуальними для прокурорської діяльності та підлягають обов'язковій реєстрації, збереженню й опрацюванню» з одночасним дотриманням режиму їх безпеки.

Особливість цього виду полягає в тому, що будь-які збої або прогалини в інформаційно-правовому забезпеченні (неналежна реєстрація, некоректне ведення баз даних, відсутність належних процедур доступу) безпосередньо впливають на законність і результативність кримінального провадження, а отже – на реалізацію основних функцій прокуратури, перелічених у ст. 2 Закону «Про прокуратуру».

Крім того, у межах інформаційно-правового забезпечення реалізації процесуальних повноважень доцільно виокремити щонайменше три підвиди: 1) реєстраційно-облікове забезпечення (внесення відомостей до ЄРДР, облік процесуальних рішень, формування електронних «досьє» проваджень); 2) доказово-цифрове забезпечення, що охоплює збір, верифікацію та збереження електронних доказів (дані з інформаційних систем, цифрові сліди, електронні повідомлення, записи з камер спостереження, лог-файли тощо); 3) міжнародно-правове інформаційне забезпечення спільних розслідувань, у тому числі за лінією Євроюст, Європолу, спільних слідчих груп. Сучасні європейські підходи до електронних доказів наголошують на необхідності спеціальних процедур доступу до інформаційних систем, стандартів допустимості таких доказів та

інтегрованих платформ обміну даними між органами правопорядку різних держав [48]. Саме тому в межах української прокуратури доказово-цифровий підвид інформаційно-правового забезпечення потребує окремої внутрішньої регламентації - від технічних форматів зберігання цифрових носіїв до порядку їх процесуального легалізування у суді.

Другим видом є організаційно-управлінське інформаційно-правове забезпечення, яке охоплює правове регулювання та організацію інформаційних процесів, спрямованих на забезпечення внутрішньої управлінської діяльності органів прокуратури: кадрової роботи, планування, внутрішнього контролю, статистичної звітності, підготовки аналітичних матеріалів, впровадження цифрових систем управління та документообігу.

У монографії Р. Калюжного та співавторів «Інформаційне забезпечення управлінської діяльності в умовах інформатизації» пропонує розглядати інформаційне забезпечення як органічний компонент управлінського процесу, який включає інформаційні ресурси, канали, технології, процедури і правові механізми, що обслуговують прийняття й реалізацію управлінських рішень [46, с. 25-29]. Перенесення цього підходу на прокуратуру дає змогу говорити про специфічний вид інформаційно-правового забезпечення, зорієнтований на підтримку внутрішньої організаційної спроможності: від ведення електронних особових справ прокурорів до формування відомчої статистики, планів роботи, внутрішніх аудитів і службових розслідувань.

У цьому сегменті важливою є поява автоматизованих систем кадрового, фінансового, господарського й управлінського обліку (АІС «Кадри», системи електронного документообігу тощо), на що звертав увагу В. Цимбалюк, описуючи «типові розробки» інформаційних систем у прокуратурі ще на початку 2000-х років [45, с. 20]. Сьогодні такі системи потребують більш жорсткого правового регулювання, як з погляду захисту даних, так і з погляду відповідальності за прийняття управлінських рішень на основі аналітичної інформації.

На нашу думку, на практиці організаційно-управлінське інформаційно-

правове забезпечення включає не лише класичні обліково-кадрові та статистичні процедури, а й інформаційно-аналітичну підтримку управлінських рішень, наприклад: формування профілів криміногенних ризиків, оцінювання навантаження на прокурорів, індикатори ефективності та якості процесуального керівництва, аналіз практики дисциплінарної відповідальності.

У зв'язку можемо виділити як підвид аналітико-прогнозне інформаційно-правове забезпечення, що органічно перетинається з організаційно-управлінським, але має акцент на побудові прогнозів злочинності, виявленні латентних тенденцій, оцінюванні ефективності законодавчих змін та управлінських рішень. У праці О. Блажівського наголошується, що інформація для прокурора – це не лише «сировина» для прийняття рішень, але й основа формування стратегічних пріоритетів, у тому числі щодо протидії корупції, організованій злочинності, кіберзлочинам [49, с. 117]. Відтак аналітико-прогнозний вид інформаційно-правового забезпечення має бути інституційно відрефлексований у відомчих актах – через закріплення ролі аналітичних підрозділів, процедур доступу до масивів даних, стандартів підготовки аналітичних продуктів.

Третім видом доцільно виділити інформаційно-комунікаційне забезпечення відкритості та підзвітності органів прокуратури. Його сутність полягає в правовому та організаційному врегулюванні: надання доступу до публічної інформації про діяльність прокуратури; оприлюднення статистики, звітів, узагальнень практики; комунікації з громадськістю та засобами масової інформації; ведення офіційних веб-ресурсів, сторінок у мережі Інтернет; реагування на інформаційні запити та публічні звернення.

Тут базовими є положення Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації», які встановлюють режим публічності, принципи забезпечення доступу, підстави для віднесення інформації до такої, що має обмежений доступ, а також форми й строки надання інформації громадянам. Застосовані до органів прокуратури ці вимоги трансформуються у спеціальні внутрішні порядки реагування на запити,

підготовки пресрелізів, організації брифінгів тощо.

У наукових дослідженнях інформаційне забезпечення органів публічної влади дедалі частіше розглядається як елемент публічної комунікації та інструмент формування довіри до держави [50, с. 1047]. Для прокуратури, яка традиційно сприймається як «закритий» орган, належне інформаційно-комунікаційне забезпечення набуває значення окремого виду інформаційної діяльності, що має бути чітко розмежований із процесуальною сферою, з одного боку, і з політичною комунікацією, з іншого.

На нашу думку, інформаційно-комунікаційне забезпечення відкритості та підзвітності також може бути деталізоване через виділення підвидів: 1) відкрито-звітне забезпечення (оприлюднення річних та спеціальних звітів, статистики, індикаторів ефективності); 2) прес-комунікаційне забезпечення (пресрелізи, брифінги, коментарі щодо резонансних проваджень); 3) електронно-прозоре забезпечення, пов'язане із запровадженням е-прозорості, оприлюдненням на офіційних веб-порталах структурованих наборів даних, інтерактивних карт, публічних реєстрів. У дослідженні І. Піляй акцентовано, що для запровадження електронної прозорості органів прокуратури необхідне створення цілісної системи інформаційно-аналітичного забезпечення, включно з уніфікованими стандартами даних і внутрішніми регламентами комунікації [51, с. 67]. Таким чином, інформаційно-комунікаційне забезпечення слід розглядати не як допоміжний напрям, а як самостійний комплекс видів забезпечення, що реалізують конституційний принцип гласності й публічності.

Четвертим функціональним видом є інформаційно-правове забезпечення безпеки та захисту інформації. Воно охоплює: правові режими конфіденційної, службової, таємної інформації; захист персональних даних; організацію криптографічного та технічного захисту інформації; процедури обмеження доступу, аудиту, реагування на інциденти; взаємодію з уповноваженими органами з питань захисту інформації та персональних даних.

Цей вид інформаційно-правового забезпечення спирається не лише на загальні закони «Про інформацію», «Про захист персональних даних», а й на

спеціальні акти у сфері інформаційної безпеки, а також на внутрішньовідомчі акти Генерального прокурора щодо порядку роботи з документами з грифами обмеження доступу, електронними носіями, засобами криптозахисту. У структурі органів прокуратури інформаційна безпека усе частіше виділяється в окремий напрям адміністративно-правової діяльності, що зумовлює необхідність визнання відповідного виду інформаційно-правового забезпечення на рівні доктрини.

Зі свого боку, інформаційно-правове забезпечення безпеки та захисту інформації вимагає врахування як національних, так і європейських стандартів. На рівні Європейського Союзу посилюються вимоги до кібербезпеки і керування ризиками для критичних суб'єктів, зокрема через Директиву (ЄС) 2022/2555 (так звана NIS2), яка встановлює обов'язок для органів влади впроваджувати комплексні системи управління кіберризиками [52]. Для органів прокуратури це означає, що інформаційно-правове забезпечення безпеки має включати не лише класичний режим охорони таємниці й персональних даних, а й нормативно закріплені політики управління кіберризиками, регулярні аудити інформаційних систем, процедури реагування на інциденти, у тому числі в координації з національними центрами кібербезпеки.

2. Класифікація за джерелом і походженням інформації: 1) Внутрішньо-організаційне інформаційно-правове забезпечення, що охоплює інформацію, яка генерується в самій системі прокуратури (внутрішні накази, методичні рекомендації, статистика, аналітичні довідки, внутрішня переписка, службові розслідування); 2) Міжвідомче інформаційно-правове забезпечення, пов'язане з обміном інформацією з іншими органами публічної влади (судами, органами досудового розслідування, Національним антикорупційним бюро України, Національним агентством з питань запобігання корупції, Державною податковою службою тощо). Воно передбачає укладання міжвідомчих угод, протоколів обміну, інтеграцію інформаційних систем, узгодження форматів даних; 3) Зовнішнє (суспільне) інформаційно-правове забезпечення, яке охоплює інформацію, що надходить від громадян, юридичних осіб, засобів масової

інформації, громадських організацій, а також з відкритих джерел (відкриті державні реєстри, офіційні веб-портали, відкриті дані). У цій площині ключову роль відіграє законодавство про звернення громадян, доступ до публічної інформації та електронне урядування. Кожен із зазначених підвидів потребує окремого інформаційно-правового регламенту: різних процедур реєстрації, строків зберігання, підстав для обмеження доступу, механізмів обміну та відповідальності.

3. Класифікація за правовим режимом і рівнем доступу - відповідно до Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» розрізняють публічну інформацію, інформацію з обмеженим доступом і таємну інформацію (державну, професійну, банківську, персональні дані тощо). Застосована до органів прокуратури ця тріада трансформується в три види інформаційно-правового забезпечення: 1) Забезпечення роботи з відкритою (публічною) інформацією - оприлюднення актів, статистики, узагальнень практики, забезпечення доступу до публічної інформації за запитами, ведення офіційних ресурсів; 2) Забезпечення роботи з інформацією з обмеженим доступом - службова, конфіденційна, професійна інформація, окремі категорії процесуальних даних (наприклад, інформація досудового розслідування до її розсекречення); 3) Забезпечення роботи з таємною інформацією - відомості з грифами «таємно», «цілком таємно», що входять до сфери державної таємниці, а також особливо захищені масиви персональних даних, пов'язані з безпекою осіб, задіяних у кримінальному провадженні. Кожен із цих трьох видів інформаційно-правового забезпечення має різні правові режими доступу, архівування, знищення, використання в суді, а також різні рівні відповідальності за порушення встановлених процедур (дисциплінарна, адміністративна, кримінальна відповідальність).

4. Класифікація за формою реалізації та ступенем стандартизації. По-перше, можна говорити про традиційне (паперове) та електронне (цифрове) інформаційно-правове забезпечення. Як показують праці І. Жиляєва та Р. Калюжного, перехід до електронних систем управління інформацією суттєво

змінює вимоги до правового регулювання: з'являється потреба в нормативному закріпленні електронного документообігу, статусу електронних носіїв, електронного підпису, процедур архівування електронних документів, інтеграції реєстрів тощо [53, с. 44].

По-друге, доцільно розмежувати стандартизоване та нестандартизоване інформаційно-правове забезпечення. Стандартизоване охоплює форми звітності, уніфіковані реєстраційні картки, затверджені шаблони процесуальних документів, типові регламенти функціонування інформаційних систем. Нестандартизоване - це аналітичні довідки, експертні висновки, situational reports, внутрішні записки. У межах прокуратури це означає, що класифікація видів інформаційно-правового забезпечення має враховувати, чи оперує той чи інший вид жорстко формалізованими документами, чи результатами творчого, ситуаційного аналізу.

Таким чином, класифікація видів інформаційно-правового забезпечення діяльності органів прокуратури України має багатовимірний характер і повинна будуватися як система взаємопов'язаних критеріїв: 1) за функціональним призначенням – процесуальне, організаційно-управлінське, комунікаційне, безпекове інформаційно-правове забезпечення; 2) за джерелом походження – внутрішньоорганізаційне, міжвідомче, зовнішнє (суспільне) забезпечення; 3) за правовим режимом і рівнем доступу – види, пов'язані з роботою з публічною, інформацією з обмеженим доступом і таємною інформацією; 4) за формою реалізації та ступенем стандартизації – паперове й електронне, стандартизоване й нестандартизоване забезпечення.

Кожен із виділених видів має бути наповнений конкретним нормативним змістом (законодавчі, підзаконні, відомчі акти), організаційними процедурами, технічними рішеннями та механізмами відповідальності. Саме така детальна класифікація дозволяє, по-перше, усунути фрагментарність правового регулювання інформаційної діяльності органів прокуратури; по-друге, вибудувати цілісну систему інформаційно-правового забезпечення, яка відповідає вимогам цифрової доби; по-третє, створити базу для подальших

законодавчих та відомчих реформ у сфері інформаційної діяльності прокуратури, відповідно до загальної доктрини інформаційного права України.

Зрештою, пропонована багатовимірна класифікація не лише описує наявний стан речей, а й виконує нормативно-проектну функцію. Вона дає змогу сформулювати конкретні напрямки вдосконалення законодавства й відомчих актів: закріпити на рівні закону окремі види інформаційно-правового забезпечення (принаймні процесуальне, управлінське, комунікаційне, безпекове), розробити типові положення про інформаційні підсистеми (ЄРДР, аналітичні системи, відкриті дані), уніфікувати внутрішні стандарти захисту інформації, процедур доступу та відповідальності. У цьому сенсі класифікація видів інформаційно-правового забезпечення діяльності органів прокуратури України стає не лише елементом теоретичного опису, а концептуальним «каркасом» майбутньої кодифікації інформаційної складової прокурорської діяльності.

Узагальнюючи викладене, слід підкреслити, що види інформаційно-правового забезпечення діяльності органів прокуратури України формують складну, багаторівневу та водночас цілісну систему, у межах якої інформація виступає не лише об'єктом правового регулювання, а й самостійним інструментом реалізації публічно-владних повноважень. Функціональне, джерельне, режимне, технологічне та організаційне розмежування інформаційно-правового забезпечення дає змогу чітко окреслити його процесуальний, управлінський, комунікаційний та безпековий виміри, виявити специфіку кожного з них, пов'язати їх із відповідними нормативними моделями та інституційними механізмами. Така класифікація не є суто теоретичною конструкцією: вона створює підґрунтя для впорядкування внутрішніх процедур, усунення прогалин і дублювання у правовому регулюванні, посилення інформаційної безпеки та прозорості, а відтак — для формування сучасної, концептуально виваженої та здатної до цифрової трансформації системи інформаційно-правового забезпечення органів прокуратури України.

2.2. Рівні та напрями інформаційного-правового забезпечення діяльності органів прокуратури України

У сучасних умовах цифрової трансформації держави прокуратура функціонує в багаторівневому інформаційному середовищі, від конституційно-правових та міжнародно-правових стандартів до внутрішньоорганізаційних інструкцій, від національних інформаційних систем до локальних баз даних окремого органу прокуратури. При цьому інформаційно-правове забезпечення вже не може розглядатися як суто допоміжний компонент правового статусу прокуратури, воно визначає реальну можливість реалізації повноважень, ефективність управлінських рішень, прозорість і підзвітність, а також рівень гарантій прав людини у сфері кримінальної юстиції [54, с. 15-18].

У науковій літературі домінує підхід, за яким інформаційно-правове забезпечення органів прокуратури описується через класифікацію видів інформації, суб'єктів і процесів, однак недостатньо дослідженими залишаються саме рівні (наприклад, горизонтальні та вертикальні рівні правового регулювання й організації інформаційних процесів) та напрями (наприклад, функціональні вектори застосування інформації).

Сучасні європейські підходи до організації інформаційного забезпечення органів правосуддя акцентують на поєднанні багаторівневої моделі управління інформаційними ресурсами з чітким поділом напрямів їх використання – процесуальним, управлінським, комунікаційним, аналітичним [55]. Досвід розвитку електронного судочинства та е-урядування у державах – членах ЄС, що поступово імплементується і в Україні, підтверджує, що саме розмежування рівнів (від наднаціонального до локального) та напрямів інформаційно-правового забезпечення є ключовою умовою прозорості, ефективності та відповідальності органів публічної влади, у тому числі й прокуратури [56].

У цьому контексті виникає потреба в побудові цілісної концепції рівнів та напрямів інформаційно-правового забезпечення діяльності органів прокуратури України, яка була б узгоджена з адміністративно-правовою доктриною, національним законодавством та практикою європейських країн, а також

дозволяла б здійснювати системний аналіз і подальшу модернізацію інформаційної інфраструктури прокуратури.

У свою чергу, методологічне підґрунтя аналізу рівнів та напрямів інформаційно-правового забезпечення діяльності органів прокуратури України має комплексний характер і поєднує загальнонаукові, спеціально-юридичні та міждисциплінарні підходи.

По-перше, визначальне значення має системний підхід, який дозволяє розглядати інформаційно-правове забезпечення як цілісну систему, що складається з взаємопов'язаних елементів: нормативних приписів, інституційних структур, інформаційних ресурсів і технологій, управлінських процедур, механізмів контролю та відповідальності. Системність передбачає виокремлення горизонтальних (напрями діяльності) та вертикальних (рівні організації й регулювання) зв'язків між цими елементами, а також аналіз їхньої взаємодії в умовах постійної цифрової модернізації.

По-друге, застосування структурно-функціонального підходу дає можливість пов'язати кожен рівень інформаційно-правового забезпечення з певними функціями прокуратури та її адміністративно-правовим статусом. Так, на макрорівні (державному) інформаційно-правове забезпечення відбиває конституційні засади, базові закони («Про інформацію», «Про прокуратуру», «Про доступ до публічної інформації» тощо); на мезорівні (відомчому) – внутрішню регламентацію інформаційних процесів у системі прокуратури; на мікрорівні – організацію інформаційної діяльності конкретного органу прокуратури та окремого прокурора.

По-третє, інституційний підхід дозволяє дослідити, як різні інститути публічного права – прокуратура, суди, органи виконавчої влади, органи місцевого самоврядування, а також органи Європейського Союзу та Ради Європи – формують спільний інформаційно-правовий простір, у межах якого прокуратура є і суб'єктом, і об'єктом інформаційних відносин [57, с. 164]. Це особливо важливо з огляду на потребу узгодження відомчих інформаційних систем прокуратури з національними й наднаціональними системами

електронного правосуддя.

По-четверте, порівняльно-правовий та євроінтеграційний підхід забезпечує можливість зіставлення моделей інформаційно-правового забезпечення в Україні з практикою держав – членів ЄС. Аналіз документів (СЕРЕJ – European Commission for the Efficiency of Justice, Європейська комісія з питань ефективності правосуддя), Європейської комісії та національного законодавства окремих країн (наприклад, Польщі, Франції) щодо використання інформаційних технологій у правосудді демонструє чіткий поділ рівнів інформаційної політики (європейський, національний, відомчий, локальний) та напрямів використання інформації (управління справами, статистика, відкриті дані, внутрішня комунікація, захист даних) [58].

По-п'яте, адміністративно-правовий підхід дозволяє виявити, як інформаційно-правове забезпечення інтегрується в механізм публічного адміністрування у сфері правосуддя, насамперед через процедури прийняття управлінських рішень, адміністративні регламенти, інструменти внутрішнього контролю та дисциплінарної відповідальності за порушення інформаційних режимів. У цьому контексті важливими є напрацювання в галузі управлінського документознавства та документно-інформаційного забезпечення органів публічної влади.

Таким чином, методологічне підґрунтя класифікації рівнів і напрямів інформаційно-правового забезпечення діяльності органів прокуратури України базується на поєднанні системного, структурно-функціонального, інституційного, порівняльно-правового та адміністративно-правового підходів, що забезпечує цілісність і практичну релевантність одержаних результатів.

Що стосується визначення понять «рівень» і «напрямок», то у загальнонауковому значенні «рівень» розуміється як певний щабель у структурі системи, що відрізняється ступенем узагальненості, масштабом впливу та набором властивих йому елементів і зв'язків. У правовій доктрині рівень часто використовується для позначення ієрархії нормативного регулювання (міжнародний, конституційний, законодавчий, підзаконний, локальний), а також

ієрархії органів публічної влади (центральні, регіональні, місцеві).

Напрямок у теорії управління та права означає відносно однорідний комплекс функцій і видів діяльності, спрямованих на досягнення певної мети в межах загальної компетенції суб'єкта публічної влади. У сфері адміністративного права напрямками зазвичай вважають окремі напрями державної політики (інформаційна, антикорупційна, правоохоронна політика тощо), а також спеціалізовані напрями діяльності конкретного органу – наприклад, у межах прокуратури це наглядова, процесуальна, представницька, аналітична, організаційно-управлінська діяльність.

Рівень інформаційно-правового забезпечення – це відносно самостійний щабель організації та правового регулювання інформаційних процесів у системі прокуратури, який характеризується певним масштабом (державний, відомчий, організаційний, індивідуальний), специфічним набором суб'єктів, джерел правового регулювання, інформаційних ресурсів та управлінських процедур.

Напрямок інформаційно-правового забезпечення – це відносно однорідна сукупність інформаційних процесів (збирання, реєстрація, зберігання, обробка, використання, захист інформації), правових засобів їх регулювання та організаційних форм реалізації, пов'язаних із виконанням певної функції прокуратури.

Ми вважаємо, що відсутність чіткого, науково виваженого розподілу інформаційно-правового забезпечення за рівнями та напрямками призводить до низки проблем, які прямо впливають на керованість, ефективність і відповідальність в діяльності органів прокуратури. До таких проблем належать: дублювання інформаційних потоків, несумісність відомчих інформаційних систем, нечіткість розмежування повноважень щодо доступу до інформації, прогалини у відповідальності за порушення інформаційних режимів, недостатня прозорість і відсутність уніфікованих стандартів публічної звітності

На нашу думку, для органів прокуратури України системний розподіл рівнів та напрямів інформаційно-правового забезпечення має щонайменше три аспекти:

1. Керованість - чітка прив'язка кожного інформаційного процесу до конкретного рівня (від Офісу Генерального прокурора до місцевої прокуратури) і напряму (процесуального, управлінського, комунікаційного, аналітичного, безпекового) дозволяє оптимізувати потоки інформації, уникнути дублювання, забезпечити узгодженість між правовими приписами й організаційною практикою;

2. Ефективність - завдяки структуризації рівнів і напрямів можливо обґрунтовано планувати ресурси (людські, фінансові, технічні), оцінювати результативність інформаційних систем, запроваджувати сучасні цифрові рішення саме там, де вони дають найбільший ефект (наприклад, у сфері електронного кримінального провадження, аналітичних платформ, відкритих даних);

3. Відповідальність і контроль - розмежування рівнів та напрямів інформаційно-правового забезпечення дозволяє чітко визначити суб'єктів відповідальності за порушення режиму інформації, за неналежну організацію інформаційних процесів, за не розкриття або, навпаки, неправомірне оприлюднення відомостей.

Загалом, ми вважаємо, що системна класифікація рівнів та напрямів інформаційно-правового забезпечення діяльності органів прокуратури України є не лише теоретично корисною, а й практично необхідною умовою побудови сучасної, прозорої, технологічно розвиненої та відповідальної прокуратури, здатної функціонувати в європейському правовому просторі та відповідати викликам цифрової доби.

У свою чергу, що стосується питання рівнів інформаційно-правового забезпечення діяльності органів прокуратури України, то на нашу думку основні його рівні доцільно розглядати як багаторівневу систему, у якій правові норми, організаційні структури, управлінські процедури та цифрова інфраструктура взаємопов'язані й утворюють єдиний контур адміністративно-правового впливу. Саме рівнева організація інформаційно-правового забезпечення дозволяє забезпечити керованість великих масивів даних, їх своєчасне використання в

процесуальній та адміністративній діяльності прокурорів, а також дотримання стандартів прав людини у сфері доступу до інформації та її захисту.

Виходячи із того, що у вітчизняній доктрині під інформаційним забезпеченням прокурорської діяльності, зокрема, пропонується розуміти комплекс правовідносин та практичних заходів, спрямованих на збирання, накопичення, обробку, зберігання, аналіз і використання інформації органами прокуратури та щодо цих органів. То на нашу думку адміністративно-правовий підхід дозволяє структурувати цей комплекс за рівнями: нормативно-правовим, інституційним, організаційно-процесуальним, інфраструктурно-технологічним та індивідуально-посадовим.

Базовим є нормативно-правовий рівень, на якому визначаються засади інформаційних правовідносин у державі загалом і в діяльності прокуратури зокрема. Він охоплює як загальне інформаційне законодавство (Закон України «Про інформацію», Закон України «Про доступ до публічної інформації», Закон України «Про захист персональних даних»), так і спеціальне законодавство про прокуратуру – насамперед Закон України «Про прокуратуру». Саме на цьому рівні закріплюються: режим доступу до інформації, категорії відкритої, службової, конфіденційної інформації; правові засади обробки персональних даних; гарантії захисту інформаційних прав учасників кримінального провадження та інших суб'єктів, з якими взаємодіє прокуратура.

У межах адміністративного права нормативно-правовий рівень виконує подвійну функцію. З одного боку, він задає рамки адміністративної діяльності органів прокуратури як суб'єктів публічної адміністрації – встановлює вимоги до відкритості, підзвітності, прозорості, процедурності, електронної взаємодії з іншими органами влади та громадськістю. З іншого – визначає правовий режим відомчих інформаційних систем (зокрема, Єдиного реєстру досудових розслідувань, кадрових, статистичних та аналітичних баз), що прямо впливає з положень загального інформаційного законодавства про автоматизовані системи та персональні дані.

За своїм змістом цей рівень є багат шаровим, до нього належать:

конституційні положення щодо прав людини на інформацію й судовий захист; закони, що визначають статус прокуратури та засади інформаційних правовідносин; підзаконні акти – накази Генерального прокурора, інструкції, положення про інформаційні системи, порядки доступу до відомчої інформації тощо. У науковій літературі слушно підкреслюється, що саме «нормативний пласт» інформаційно-правового забезпечення створює передумови для системності інформатизації в органах прокуратури й узгодженості між галузевими та загальноправовими вимогами.

До нормативно-правового рівня доцільно віднести й міжнародно-правові стандарти, акти Ради Європи та ЄС, у яких фіксуються вимоги до використання ІКТ у правосудді, відкритості судових та прокурорських даних, захисту персональних даних, етичного застосування цифрових технологій. Тематичний звіт СЕРЕJ про використання інформаційних технологій у судах Європи підтверджує, що законодавче врегулювання є передумовою впровадження інформаційних систем у судах і прокуратурах, а також оцінки їх впливу на ефективність правосуддя [55, р. 5–8]. Для України врахування цих стандартів важливе в контексті євроінтеграції та гармонізації інформаційно-правового забезпечення прокуратури з європейськими підходами.

Наступним є інституційний рівень, який охоплює систему органів прокуратури як організаційний «каркас» інформаційно-правового забезпечення. Йдеться про Генеральну прокуратуру (Офіс Генерального прокурора), обласні, окружні прокуратури, спеціалізовані підрозділи, а також відомчі науково-дослідні й навчальні установи, що формують і реалізують інформаційну політику в межах прокуратури.

З позицій адміністративного права інституційний рівень відображає статус органів прокуратури як суб'єктів публічної адміністрації, що реалізують визначені законом функції на професійній основі й діють у межах встановленої ієрархії та підпорядкування. На цьому рівні формуються: відомча політика у сфері інформатизації; внутрішні регламенти обміну даними між підрозділами; механізми взаємодії з іншими органами публічної влади, правоохоронними

органами, судами й органами місцевого самоврядування. Водночас інституційний рівень включає мережу зовнішніх інституцій – органів публічної влади, з якими прокуратура перебуває в постійних інформаційних взаємовідносинах (Національна поліція, ДБР, органи виконавчої влади, суди тощо).

До елементів інституційного рівня належать спеціалізовані структурні підрозділи (управління інформаційних технологій, аналітичні відділи, прес-служби), науково-методичні ради, що формують стандарти обробки інформації, готують методичні рекомендації, забезпечують координацію інформатизації. Як слушно зауважує В. Цимбалюк, саме організаційно-правове забезпечення «системності інформатизації» в органах прокуратури (наявність відповідальних підрозділів, єдиних стандартів і процедур) відрізняє цілеспрямовану політику у сфері інформації від фрагментарного впровадження окремих технологічних рішень [45, с. 21-23].

У свою чергу, організаційно-процесуальний рівень охоплює інформаційно-правове забезпечення конкретних управлінських, координаційних та процесуальних процедур у діяльності прокуратури. На цьому рівні відбувається переклад нормативних вимог та інституційних рішень у конкретні алгоритми дій: порядок формування інформаційних ресурсів, регламенти документообігу, стандарти аналітичної роботи, процедури взаємодії з ЄРДР, статистичну та звітну діяльність, порядок доступу до публічної інформації, реагування на запити журналістів, обмін інформацією з іншими органами.

Організаційно-процесуальний рівень має очевидну адміністративно-процесуальну природу, адже значна частина відповідних процедур оформлюється у вигляді адміністративних регламентів, положень про структурні підрозділи, інструкцій із діловодства, стандартів внутрішнього контролю. Від того, наскільки чітко ці процедури формалізовані, залежить передбачуваність і відтворюваність інформаційних потоків у прокуратурі. Саме на цьому рівні особливо гостро постає питання балансування між відкритістю та захистом інформації: наприклад, реалізація Закону України «Про доступ до публічної

інформації» потребує внутрішніх регламентів, які поєднують виконання обов'язків з розкриття інформації з вимогами режиму службової та таємної інформації.

До організаційно-процесуального рівня належать і форми правового інформування, які прокуратура здійснює щодо суспільства: оприлюднення статистики, прес-брифінги, повідомлення про процесуальні рішення, роз'яснення практики застосування законодавства. Ці форми, з одного боку, є елементом демократичного контролю, а з іншого – потужним інструментом профілактики правопорушень та формування правової культури.

Окремий, дедалі вагоміший рівень становить інфраструктурно-технологічний, який охоплює сукупність інформаційно-комунікаційних систем, технічних засобів, програмних комплексів та мережевої інфраструктури, що забезпечують функціонування інформаційно-правового контенту прокуратури. Йдеться про Єдиний реєстр досудових розслідувань, внутрішні документообігові системи, статистичні та аналітичні підсистеми, системи моніторингу, електронний цифровий підпис, захищені канали зв'язку тощо.

У сучасних дослідженнях інформатизації прокурорських органів підкреслюється, що без впровадження автоматизованих систем і сучасної комп'ютерної техніки ефективне виконання завдань прокуратури стає фактично неможливим [3, с. 157–158]. Інформатизація розглядається як сприятливе середовище для впровадження аналітичних, мережевих та комунікаційних технологій у прокурорській діяльності, що має ґрунтуватися на належному організаційно-правовому та фінансовому забезпеченні. При цьому інформаційно-правове забезпечення й інформатизація перебувають у відносинах взаємозумовленості, з одного боку, правові норми визначають вимоги до створення та експлуатації інформаційних систем, з іншого – саме ці системи стають інструментом реалізації правових приписів, зокрема у сфері обліку кримінальних правопорушень, контролю за додержанням законів, аналізу криміногенних процесів.

Міжнародний досвід також підтверджує, що інфраструктурно-

технологічний рівень є критичним для підвищення ефективності правосуддя. Звіти СЕРЕЖ щодо використання ІКТ у європейських судах і прокуратурах фіксують пряму кореляцію між рівнем розвитку судових інформаційних систем і швидкістю розгляду справ, доступністю інформації для учасників процесу, можливостями аналітичної оцінки судової практики. Для України релевантною є тенденція переходу від «електронного документообігу» в прокуратурі до комплексних систем e-justice та e-prosecution, інтегрованих з інформаційними ресурсами судової системи й інших правоохоронних органів.

Останнім, фундаментальним, хоча часто недооціненим, є індивідуально-посадовий рівень, який пов'язаний із правовим статусом конкретного прокурора, рівнем його інформаційної компетентності, професійної етики та персональної відповідальності за роботу з інформацією. Інформаційно-правове забезпечення на цьому рівні проявляється у вигляді: закріплених у законодавстві прав і обов'язків прокурора щодо доступу до інформації, збереження таємниці слідства, захисту персональних даних, недопущення розголошення відомостей, що становлять державну чи іншу охоронювану законом таємницю; вимог до підвищення кваліфікації та цифрової грамотності; етичних стандартів комунікації в інформаційному середовищі.

У межах загальної теорії інформаційного права підкреслюється, що саме людський фактор є найслабкішою ланкою будь-якої інформаційної системи, адже від ставлення конкретних посадових осіб до інформаційної безпеки та прав людини залежить реальна ефективність правових і організаційних механізмів.

Для прокуратури це має особливе значення, оскільки прокурор одночасно виступає носієм широких повноважень у доступі до інформації та гарантом її правомірного використання. Кваліфікаційні вимоги до прокурорів, програми їх підготовки й підвищення кваліфікації мають включати блоки, присвячені інформаційному праву, правовій інформатиці, етиці цифрової комунікації, захисту персональних даних.

На індивідуально-посадовому рівні інформаційно-правове забезпечення проявляється також через систему внутрішнього контролю та дисциплінарної

відповідальності за порушення інформаційного законодавства, що впливає зі Закону України «Про захист персональних даних» та відповідних положень Закону України «Про прокуратуру» щодо дисциплінарної відповідальності прокурорів. Саме загроза персональної відповідальності стимулює дотримання встановлених правил доступу й обігу інформації.

Узагальнюючи, основні рівні інформаційно-правового забезпечення діяльності органів прокуратури України утворюють цілісну систему, в якій кожен рівень виконує власну функцію, але водночас залежить від інших. Нормативно-правовий рівень задає загальні «правила гри»; інституційний – формує організаційний каркас реалізації цих правил; організаційно-процесуальний – забезпечує їх втілення в конкретних адміністративних та процесуальних процедурах; інфраструктурно-технологічний – надає інструменти для обробки й аналізу інформації; індивідуально-посадовий – гарантує персоналізацію відповідальності та професійну спроможність застосовувати ці інструменти. Така багаторівнева модель відповідає сучасним тенденціям розвитку інформаційного права й адміністративної юстиції та створює концептуальну рамку для подальшої деталізації напрямів удосконалення інформаційно-правового забезпечення прокуратури, зокрема в контексті цифрової трансформації публічної влади.

У свою чергу, основні напрями інформаційно-правового забезпечення діяльності органів прокуратури України доцільно описувати не як перелік окремих функцій чи технологій, а як системно впорядковані вектори використання інформації, що опосередковують реалізацію конституційно визначених повноважень прокуратури. З позицій адміністративного права цей феномен розгортається через низку базових напрямів: процесуально-інформаційний, організаційно-управлінський, комунікаційно-прозорий, аналітико-прогнозний, інформаційно-безпековий та міжвідомчий і міжнародний (інтеграційний), кожен із яких має власну нормативну основу, суб'єктний склад, інформаційні ресурси і механізми відповідальності.

Процесуально-інформаційний напрям є серцевиною інформаційно-

правового забезпечення прокуратури, оскільки безпосередньо забезпечує реалізацію функцій у кримінальному провадженні, представництві інтересів держави та здійсненні нагляду за додержанням законів. Він охоплює правове регулювання та організацію інформаційних процесів, пов'язаних із внесенням відомостей до Єдиного реєстру досудових розслідувань, формуванням і веденням електронних матеріалів проваджень, збиранням і збереженням доказової інформації (у тому числі електронних доказів), обміном даними з органами досудового розслідування й судами, фіксацією та документуванням процесуальних рішень.

Саме у сфері процесуальної діяльності найвиразніше виявляється залежність між якістю інформаційно-правового забезпечення та законністю, обґрунтованістю й своєчасністю рішень прокурора. Порушення правил реєстрації кримінальних правопорушень, неналежне наповнення електронних баз, відсутність чітких процедур доступу до інформаційних систем, недосконалість регламентації роботи з електронними доказами безпосередньо впливають на можливість реалізації завдань кримінального провадження, гарантованих Кримінальним процесуальним кодексом України, та підривають довіру до прокуратури як суб'єкта публічної влади.

Процесуально-інформаційний напрям має складну структуру. По-перше, він включає реєстраційно-облікову складову (ЄРДР, електронні журнали, електронні описи матеріалів), де ключовими є вимоги до повноти, достовірності й своєчасності фіксації даних. По-друге, доказово-цифрову складову, що охоплює доступ до телекомунікаційних даних, лог-файлів, аудіо- та відеозаписів, іншої цифрової інформації, яка використовується як доказ, а отже повинна зберігатися й оброблятися з дотриманням спеціальних процедур автентифікації та захисту. По-третє, міжнародно-процесуальну складову, пов'язану з обміном інформацією в рамках міжнародної правової допомоги, спільних слідчих груп, взаємодії з Євроюстом та іншими інституціями, де інформаційні потоки регламентуються одночасно національним та міжнародним правом.

Усе це зумовлює потребу в стійкій нормативній основі процесуально-

інформаційного напрямку: від загальних приписів Закону України «Про інформацію», Закону України «Про захист персональних даних» до спеціальних положень Кримінального процесуального кодексу, Закону України «Про прокуратуру» та відомчих інструкцій щодо ведення ЄРДР, зберігання матеріалів проваджень і використання технічних засобів фіксації.

Другий базовий напрям - це організаційно-управлінський, який зорієнтований на забезпечення внутрішньої діяльності органів прокуратури як системи публічної адміністрації, кадрової роботи, планування, внутрішнього контролю, управління ресурсами, документообігу, відомчої статистики.

Перенесення цього підходу на сферу прокуратури означає, що організаційно-управлінський напрям охоплює: а) інформаційні масиви кадрового характеру (особові справи, відомості про кваліфікацію, дисциплінарну відповідальність, оцінювання ефективності); б) планово-звітну інформацію (річні й квартальні плани роботи, звіти, службові записки, аналітичні довідки); в) інформацію внутрішнього контролю й аудиту (результати перевірок, внутрішніх розслідувань, моніторингу виконання рішень); г) фінансово-господарську інформацію (бюджетні показники, закупівлі, облік майна).

З позицій адміністративного права цей напрям забезпечує реалізацію прокуратурою функцій як суб'єкта публічного управління у власній системі, саме тут проявляються принципи плановості, ієрархічності, підзвітності, прозорості та персоніфікованої відповідальності керівництва [54, с. 44-49].

Особливість цього напрямку полягає в тому, що він не є самоціллю: його зміст визначається потребами управління процесуальною, наглядовою, представницькою діяльністю. Як слушно зауважує В. Цимбалюк, без організаційно-правового забезпечення системності інформатизації – тобто без вибудованої структури управління інформаційними ресурсами – технічні новації перетворюються на набір несумісних рішень, які не підвищують ефективність роботи прокуратури [45, с. 21].

У свою чергу, комунікаційно-прозорий напрям інформаційно-правового забезпечення пов'язаний із реалізацією принципів відкритості, гласності та

підзвітності прокуратури суспільству. Його змістом є правове та організаційне врегулювання процесів надання доступу до публічної інформації, оприлюднення статистики й узагальнень практики, комунікації з засобами масової інформації, ведення офіційних веб-ресурсів, опрацювання запитів громадян та ЗМІ.

Закон України «Про доступ до публічної інформації» закріплює загальні вимоги до розкриття інформації суб'єктами владних повноважень, установлюючи принципи прозорості, максимального сприяння запитувачеві, обмеженість підстав для відмови в наданні інформації. Застосований до прокуратури, цей закон зобов'язує забезпечувати доступ до рішень, статистики, структур і функцій органів прокуратури, інформації про використання бюджетних коштів, за винятком випадків, коли така інформація підпадає під режим обмеженого доступу.

На нашу думку, комунікаційно-прозорий напрям включає три взаємопов'язані блоки: 1) офіційно-звітний, що охоплює підготовку й оприлюднення річних і спеціальних звітів, статистичних даних, індикаторів ефективності; 2) медійно-комунікаційний, пов'язаний з організацією пресконференцій, брифінгів, наданням коментарів щодо резонансних справ, взаємодією з журналістською спільнотою; 3) електронно-відкритий, у межах якого прокуратура виступає суб'єктом електронного урядування, публікуючи набори відкритих даних, використовуючи інтерактивні онлайн-сервіси, забезпечуючи доступ до актуальної інформації через офіційні веб-портали.

Що стосується аналітико-прогнозного напрямку, то він орієнтований на використання інформаційних ресурсів для глибокого аналізу стану законності, криміногенної ситуації, ефективності застосування законодавства та формування стратегічних рішень у діяльності прокуратури. Йдеться про систематизацію й узагальнення матеріалів кримінальних проваджень, судової практики, статистики правопорушень, дисциплінарної практики, соціологічних та експертних даних для вироблення прогнозів і рекомендацій.

На нашу думку, в системі прокуратури аналітико-прогнозний напрям передбачає: а) підготовку узагальнень слідчої та судової практики; б)

формування кримінологічних та віктимологічних профілів регіонів; в) оцінювання ефективності законодавчих новацій; г) розробку пропозицій щодо вдосконалення правового регулювання й організації роботи прокуратури.

Аналітико-прогнозний напрям тісно пов'язаний з адміністративно-правовою функцією прокуратури щодо участі у формуванні державної політики у сфері кримінальної юстиції. На основі узагальненої інформації прокуратура подає парламенту й уряду пропозиції щодо змін законодавства, організації роботи правоохоронних органів, пріоритетів в антикорупційній, антинаркотичній, антикорупційній політиці. Відсутність розвинутого аналітичного компоненту знижує роль прокуратури як суб'єкта вироблення публічної політики й обмежує її функцію до констатації порушень без їхнього стратегічного осмислення [59, с. 188].

У свою чергу, інформаційно-безпековий напрям спрямований на забезпечення належного режиму охорони та захисту інформації у діяльності органів прокуратури. Він охоплює правове регулювання та практичну організацію захисту конфіденційної, службової, таємної інформації, персональних даних; впровадження комплексних систем технічного й криптографічного захисту; управління кіберризиками; реагування на інциденти інформаційної безпеки.

У загальній теорії інформаційного права підкреслюється, що захист інформації в органах публічної влади є складним поєднанням правових, організаційних і технічних заходів. Для прокуратури це має особливе значення з огляду на концентрацію великої кількості чутливої інформації – від персональних даних потерпілих, підозрюваних, свідків до відомостей, що становлять державну таємницю, а також внутрішньої службової інформації. Закони України «Про інформацію», «Про захист персональних даних», «Про державну таємницю», а також внутрішні накази Генерального прокурора утворюють нормативний каркас цього напрямку, доповнюваний спеціальними стандартами у сфері кібербезпеки.

В українських реаліях інформаційно-безпековий напрям потребує

подальшої інституціоналізації, а саме: створення спеціалізованих підрозділів інформаційної безпеки в системі прокуратури; запровадження регулярних аудитів інформаційних систем; уніфікації політик доступу та зберігання даних; розроблення стандартів реагування на витоки інформації.

Останнім є міжвідомчий та міжнародний (інтеграційний) напрям, що стосується інформаційної взаємодії прокуратури з іншими органами публічної влади України, а також із зарубіжними й міжнародними інституціями. Йдеться про обмін інформацією з судами, органами досудового розслідування, Державною податковою службою, НАБУ, НАЗК, органами місцевого самоврядування, а також з інституціями ЄС та Ради Європи в рамках міжнародної правової допомоги, спільних проектів та програм технічної допомоги.

На міжвідомчому рівні інформаційно-правове забезпечення реалізується через укладання угод про обмін даними, інтеграцію інформаційних систем, визначення форматів та протоколів обміну, уніфікацію класифікаторів і довідників. Адміністративно-правовий аспект тут полягає в регламентації повноважень органів прокуратури щодо доступу до державних реєстрів і баз даних, порядку проведення спільних перевірок, застосування електронної взаємодії між реєстрами.

На міжнародному рівні цей напрям формують багатосторонні та двосторонні договори, рекомендації міжнародних організацій, участь у європейських проектах з кіберправосуддя, використання спільних інформаційних платформ. Зокрема, СЕРЕJ у тематичних дослідженнях розглядає інформаційні технології як засіб зближення стандартів ефективності та якості правосуддя в різних країнах, а також як інструмент обміну статистичними даними й судовою практикою [55, с. 6-8]. Відтак для прокуратури України інтеграційний напрям має означати не лише технічну сумісність інформаційних систем, а й методологічну узгодженість підходів до збору, обробки й аналізу даних.

Таким чином, основні напрями інформаційно-правового забезпечення

діяльності органів прокуратури України утворюють цілісну, але внутрішньо диференційовану систему. Кожен із них відбиває певний аспект адміністративно-правового статусу прокуратури, наприклад: здійснення публічно-владних повноважень, управління внутрішньою організацією, забезпечення відкритості й підзвітності, вироблення публічної політики у сфері правосуддя, гарантування інформаційної безпеки та інтеграції в європейський правовий простір. Розмежування й водночас взаємозв'язок цих напрямів створюють теоретичне й практичне підґрунтя для подальшої модернізації законодавства й відомчих актів, розроблення комплексної концепції інформатизації прокуратури та вдосконалення механізмів відповідальності за порушення інформаційних режимів.

Узагальнюючи, слід зазначити, що рівні та напрями інформаційно-правового забезпечення діяльності органів прокуратури України утворюють цілісну, проте внутрішньо диференційовану систему, в межах якої нормативно-правові засади, інституційно-організаційна структура, управлінсько-процесуальні процедури, техніко-технологічна інфраструктура та індивідуально-посадові аспекти взаємодіють як взаємопов'язані елементи єдиного адміністративно-правового механізму. Їх доктринальне розмежування за рівнями та напрямками дозволяє не лише глибше описати реальний зміст інформаційної діяльності прокуратури, а й виявити структурні дисбаланси, прогалини у правовому регулюванні, організаційну та технологічну несумісність окремих її компонентів. Саме така системна оптика створює підґрунтя для подальшої конкретизації кожного рівня та напрямку, розроблення цільових моделей їх удосконалення та формування сучасної концепції інформаційно-правового забезпечення прокуратури, здатної відповідати вимогам європейської правової інтеграції й викликам цифрової доби.

2.3. Адміністративно-правові форми та методи інформаційно-правового забезпечення діяльності органів прокуратури України

У сучасних умовах трансформації системи публічної влади України, що

відбувається в руслі європейських цінностей правової держави, особливого значення набуває ефективне функціонування інституцій, відповідальних за забезпечення законності, правопорядку та дотримання прав людини. У цьому контексті діяльність органів прокуратури України постає як один із ключових елементів механізму правового захисту держави та суспільства. Зважаючи на інформаційну насиченість сучасного середовища, забезпечення ефективної прокурорської діяльності неможливе без належного рівня інформаційно-правового забезпечення, що включає створення, оброблення, захист та обіг правової інформації в межах компетенції цих органів.

Інформаційно-правове забезпечення діяльності органів прокуратури як складна юридико-адміністративна категорія не обмежується лише нормативним регулюванням. Воно реалізується через чітко визначені адміністративно-правові форми та методи, які становлять інструментальну основу для виконання завдань органів прокуратури. Системний аналіз цих форм і методів дозволяє з'ясувати, яким чином інформація як публічне благо набуває юридично значущої форми, яким чином регламентуються процедури її оброблення, передавання та збереження, і які адміністративні впливи використовуються для досягнення визначених законом цілей.

Що стосується категоріально-понятійного апарату визначення понять «форми» та «методи» то у правовій науці вони традиційно розглядаються як дві взаємопов'язані, але самостійні категорії, які характеризують зовнішній і внутрішній вимір правового впливу.

У загальній теорії адміністративного права під адміністративно-правовими формами традиційно розуміють юридично врегульовані зовнішні способи вираження змісту діяльності суб'єктів публічної адміністрації, у яких об'єктивуються їхні управлінські рішення, дії чи бездіяльність [60, с. 132–134]. Йдеться, зокрема, про видання нормативних і індивідуальних актів управління, укладення адміністративних договорів, здійснення реєстраційних, дозвільних, контрольно-наглядових, юрисдикційних та інших дій, оформлених у встановленому законом процедурному та документальному режимі. Саме через

форми забезпечується легітимність, передбачуваність та контрольованість адміністративної діяльності.

У свою чергу, адміністративно-правові методи, характеризуються як сукупність юридично врегульованих прийомів, способів і засобів впливу суб'єктів публічної адміністрації на поведінку підвладних суб'єктів, спрямованих на досягнення визначених законом публічних цілей [61, с. 229].

Перенесення цих загальнотеоретичних конструкцій у площину інформаційно-правового забезпечення діяльності органів прокуратури вимагає певної адаптації. По-перше, інформаційно-правове забезпечення має виразно процесуально-адміністративний характер. де переважна частина інформаційних операцій (збір, обробка, передача даних, прийняття рішень на їх основі) здійснюється в умовах чітко визначених процедур, регламентів, інструкцій. По-друге, значна частина відповідних дій пов'язана з обігом інформації з обмеженим доступом (службова, конфіденційна, таємна інформація, персональні дані), що обумовлює специфічні правові режими й додаткові гарантії.

У цьому контексті адміністративно-правові форми інформаційно-правового забезпечення діяльності органів прокуратури доцільно визначати як встановлені законодавством та відомчими актами зовнішні форми реалізації інформаційних повноважень прокуратури, що проявляються у виданні інформаційно насичених актів (наказів, розпоряджень, методичних рекомендацій, інформаційних листів, довідок, звітів), здійсненні інформаційних процедур (реєстрація кримінальних правопорушень, ведення ЄРДР, формування статистичної звітності, оприлюднення публічної інформації), а також у виконанні окремих інформаційних дій (надання відповідей на запити, передача матеріалів іншим органам, завантаження чи верифікація даних в інформаційних системах).

Відповідно, адміністративно-правові методи інформаційно-правового забезпечення діяльності органів прокуратури можна визначити як встановлені адміністративно-правовими нормами способи і прийоми, за допомогою яких органи прокуратури організовують інформаційні процеси, впливають на поведінку підпорядкованих працівників, інших органів державної влади, органів

місцевого самоврядування, юридичних і фізичних осіб у сфері інформаційних відносин.

У свою чергу, значення адміністративно-правових форм і методів у сфері інформаційно-правового забезпечення діяльності органів прокуратури України проявляється, передусім, у тому, що саме через них забезпечується юридична визначеність і передбачуваність інформаційних процесів. Так наприклад:

1. Адміністративно-правові форми інформаційного забезпечення виступають гарантією легітимності інформаційних рішень прокуратури. Видання наказів, інструкцій, методичних рекомендацій щодо ведення ЄРДР, статистичних звітів, внутрішніх інформаційних систем створює нормативну основу для дій працівників прокуратури, чітко окреслює їхні обов'язки та повноваження в інформаційній сфері. Належне оформлення правозастосовних рішень (постанов, актів реагування, листів) забезпечує можливість їх контролю й оскарження, а отже – реалізацію принципу верховенства права в інформаційних відносинах.

2. Адміністративно-правові методи інформаційно-правового забезпечення визначають характер і інтенсивність впливу прокуратури на інших суб'єктів – органи досудового розслідування, суди, органи виконавчої влади, органи місцевого самоврядування, юридичних та фізичних осіб. Саме через методи координації, контролю, адміністративного примусу, інформаційно-правового регламентування формується інформаційна дисципліна у взаємодії між цими суб'єктами, а також встановлюються строки подання інформації, формати її надання, відповідальність за ненадання або надання недостовірних відомостей, механізми виправлення помилок. Це істотно підвищує керованість інформаційних потоків та зменшує ризики інформаційних збоїв у діяльності прокуратури.

3. Чітко вибудована система форм і методів інформаційно-правового забезпечення є ключовою умовою прозорості та підзвітності органів прокуратури суспільству. Закон України «Про доступ до публічної інформації» покладає на прокуратуру обов'язок забезпечувати доступ до значного масиву

інформації, що стосується її організації та діяльності, за винятком випадків, коли така інформація підлягає обмеженню [32].

4. Адміністративно-правові форми й методи відіграють вирішальну роль у забезпеченні інформаційної безпеки в системі прокуратури. В умовах широкого застосування електронних реєстрів, віддаленого доступу, хмарних технологій та поступового впровадження елементів штучного інтелекту (аналітичні системи, ризик-орієнтовані моделі) особливого значення набувають процедури і методи, спрямовані на захист конфіденційної інформації, персональних даних, службової та державної таємниці. Саме через відповідні форми (політики безпеки, інструкції, протоколи доступу, аудиторські процедури) й методи (контроль, аудит, санкції за порушення режимів, навчання персоналу) забезпечується баланс між відкритістю та захистом прав людини в інформаційній сфері [62, с. 158].

5. Адміністративно-правові форми та методи інформаційно-правового забезпечення виконують інтеграційну функцію в системі органів прокуратури, пов'язуючи між собою рівні інформаційної діяльності. Наявність уніфікованих форм статистичної звітності, стандартів наповнення ЄРДР, єдиних правил документообігу й обігу електронних документів, методів внутрішнього контролю й оцінювання якості інформаційної роботи забезпечує порівнюваність даних, можливість їх агрегації й аналізу, а отже – формування обґрунтованої аналітичної та прогнозної бази для управлінських рішень.

6. Значення адміністративно-правових форм і методів інформаційно-правового забезпечення діяльності органів прокуратури виявляється й у їхній еволюційній здатності, тобто спроможності адаптуватися до нових технологічних і соціальних викликів. Сучасні європейські документи у сфері кіберправосуддя наголошують, що впровадження ІКТ та штучного інтелекту в діяльність органів правосуддя не може відбуватися поза рамками чітких процедурних форм, прозорих методів обробки даних і відповідних механізмів контролю.

Отже, адміністративно-правові форми та методи інформаційно-правового

забезпечення діяльності органів прокуратури України виконують не лише технічну чи процедурну функцію, а й виступають системоутворюючими елементами адміністративно-правового механізму, що забезпечує законність, ефективність, прозорість, безпеку та відповідальність у сфері використання інформації. Їх комплексне доктринальне осмислення є необхідною передумовою подальшої розробки спеціальних моделей удосконалення інформаційно-правового забезпечення прокуратури в умовах цифрової трансформації та європейської інтеграції [63, с. 571].

Що стосується основних адміністративно-правових форм інформаційно-правового забезпечення діяльності органів прокуратури України, які зазвичай розглядаються як специфічні, юридично врегульовані зовнішні прояви реалізації інформаційних повноважень прокуратури, у яких об'єктивується зміст її владної діяльності в інформаційній сфері. То на нашу думку до таких форм можна віднести:

1. Нормотворчі та відомчо-регламентаційні форми - які охоплюють участь органів прокуратури в підготовці проєктів нормативно-правових актів з питань інформаційних відносин, а також видання внутрішньовідомчих актів (наказів, інструкцій, положень, регламентів), що безпосередньо врегульовують інформаційні процеси. Формально прокуратура не є класичним органом виконавчої влади, однак згідного ст. 9 Закону України «Про прокуратуру» Генеральний прокурор наділений правом видання нормативних актів, обов'язкових для органів прокуратури, що виступають основним інструментом деталізації вимог законодавства в частині ведення ЄРДР, документообігу, статистичної звітності, доступу до інформації, захисту персональних даних тощо [13].

Саме у формі наказів і інструкцій встановлюються: порядок реєстрації кримінальних правопорушень та внесення відомостей до ЄРДР; правила формування й подання звітності; вимоги до структури й наповнення інформаційних систем; режими доступу до службової інформації; алгоритми реагування на інформаційні запити громадян, журналістів, органів влади. Такі

акти є класичними правовими формами адміністративної діяльності, оскільки вони спричиняють юридичні наслідки для працівників прокуратури та визначають їхні обов'язки в інформаційній сфері.

Нормотворчі форми мають і зовнішній вимір: у процесі узагальнення практики органи прокуратури готують пропозиції щодо вдосконалення законодавства у сфері інформації й процесуального регулювання електронних доказів, доступу до реєстрів, відкритих даних. Вони втілюються у вигляді проєктів законів, висновків до законопроектів, аналітичних довідок, що надходять до парламенту й уряду. Така участь прокуратури в нормотворчому процесі є однією з форм реалізації її конституційно визначених функцій та каналом імплементації європейських інформаційних стандартів (у тому числі напрацювань СЕРЕJ щодо використання ІКТ у правосудді) у національне законодавство [55].

2. Правозастосовні (індивідуально-актні) форми - охоплюють постанови, акти прокурорського реагування, рішення про надання чи відмову в наданні публічної інформації, про обмеження доступу, про передачу матеріалів іншим органам, а також інші індивідуальні акти, які базуються на аналізі певних інформаційних масивів. Йдеться насамперед про постанови прокурора в кримінальному провадженні (про визнання доказів, про доручення слідчому, про закриття провадження тощо), які спираються на оцінку зібраних відомостей, у тому числі електронних доказів, файлів, телекомунікаційних даних, результатів НСРД.

До правозастосовних форм інформаційно-правового забезпечення належать також: а) відповіді на запити про доступ до публічної інформації (надання, відмова, відстрочка тощо), які оформлюються письмово й повинні відповідати вимогам Закону України «Про доступ до публічної інформації»; б) рішення про віднесення певних відомостей до службової інформації, їх розсекречування чи зміни режиму доступу відповідно до Закону України «Про інформацію» та спеціальних актів; в) акти прокурорського реагування (подання, вимоги, письмові вказівки) щодо порушень інформаційного законодавства іншими

органами публічної влади. Ці форми мають важливе гарантійне значення, оскільки саме через них реалізуються суб'єктивні інформаційні права громадян та юридичних осіб, забезпечується можливість оскарження рішень прокуратури в адміністративному чи судовому порядку, що підсилює принцип верховенства права в інформаційній сфері.

3. Реєстраційно-облікові та статистичні форми - в них конкретизується обов'язок прокуратури щодо ведення державних реєстрів і баз даних, формування статистичних звітів, обліку проваджень і рішень. Передусім це стосується внесення відомостей до Єдиного реєстру досудових розслідувань, реєстрації заяв і повідомлень про кримінальні правопорушення, обліку процесуальних рішень, формування електронних справ, а також відомчих статистичних форм щодо стану злочинності, результатів досудового розслідування, ефективності підтримання публічного обвинувачення тощо.

У роботах з адміністративного права реєстраційно-облікові форми розглядаються як різновид правових адміністративних форм, оскільки внесення запису до реєстру, видача довідки, формування статистичної звітності прямо впливають на виникнення, зміну чи припинення правовідносин або на оцінку ефективності діяльності органів влади [64, с. 67]. У випадку прокуратури реєстраційно-облікові форми виконують додаткову, кримінально-процесуальну функцію, будучи необхідною передумовою реалізації права особи на доступ до правосуддя й належне розслідування.

Крім того, ведення статистичних форм відповідно до єдиних стандартів та класифікаторів є основою для формування аналітичних звітів, узагальнень практики, кримінологічних прогнозів, що зумовлює тісний зв'язок зазначених форм із аналітико-прогнозним напрямом інформаційного забезпечення прокуратури.

4. Контрольно-наглядові та юрисдикційні форми - реалізуються у вигляді перевірок додержання інформаційного законодавства, службових розслідувань, дисциплінарних проваджень щодо порушення режимів доступу до інформації, а також розгляду скарг на рішення, дії чи бездіяльність працівників прокуратури в

інформаційній сфері.

На нашу думку контрольні форми діяльності правоохоронних органів відіграють системо-утворюючу роль у забезпеченні законності, будучи спрямованими на перевірку відповідності фактичного стану справ вимогам нормативно-правових актів. Для прокуратури це, зокрема, означає: контроль за своєчасністю й повнотою внесення відомостей до ЄРДР; перевірку дотримання строків розгляду запитів на публічну інформацію; аудит доступу до інформаційних систем та логів користувачів; перевірку дотримання правил захисту персональних даних, службової таємниці.

Юрисдикційні форми проявляються в межах дисциплінарних проваджень стосовно прокурорів та інших працівників, які допустили витік інформації, незаконний доступ до неї, поставили під загрозу конфіденційність даних або порушили встановлені процедури їх обробки. Такі форми поєднують інформаційно-правовий і владно-розпорядчий аспекти, оскільки водночас фіксують факт порушення інформаційних обов'язків та забезпечують персоналізацію юридичної відповідальності.

5. Організаційні форми внутрішньої інформаційної діяльності – вони не породжують безпосередніх юридичних наслідків, але забезпечують підготовку й реалізацію правових рішень, планування й координацію діяльності органів публічної адміністрації. У контексті прокуратури до таких форм належать: проведення оперативних і стратегічних нарад із питань інформатизації; робота координаційних і робочих груп, науково-методичних рад; розроблення внутрішніх планів інформатизації; організація навчання працівників щодо роботи з інформаційними системами; підготовка методичних матеріалів з питань роботи з інформацією.

Хоча ці форми формально не змінюють правового статусу суб'єктів, саме вони забезпечують належне функціонування правових форм, створюючи організаційне підґрунтя для ефективного використання відомчих інформаційних ресурсів. Сучасні дослідження інформатизації прокурорських органів підкреслюють, що без належно організованої підготовки кадрів, внутрішньої

координації й методичного супроводу навіть технічно досконалі інформаційні системи не дають очікуваного ефекту.

6. Комунікативно-прозорі (публічно-інформаційні) форми – це оприлюднення офіційних повідомлень, статистики, узагальнень практики, звітів про діяльність прокуратури, ведення офіційних веб-сайтів і сторінок у соціальних мережах, надання коментарів ЗМІ, проведення пресконференцій, публічних слухань тощо. Вони безпосередньо пов'язані з виконанням обов'язків, передбачених ст. 14-15 Закону України «Про доступ до публічної інформації», який вимагає від суб'єктів владних повноважень проактивного оприлюднення інформації про свою діяльність та структуру.

Ці форми мають виражений інформаційно-правовий характер: по-перше - встановлюють для прокуратури обов'язок перетворювати внутрішню службову інформацію (статистику, аналітичні дані, узагальнення практики) на публічний інформаційний продукт; по-друге - забезпечують реалізацію права суспільства на доступ до інформації про діяльність органів публічної влади; по-третє - слугують інструментом формування довіри й громадського контролю за діяльністю прокуратури.

7. Договірні та координаційні форми інформаційної взаємодії - у межах яких прокуратура формалізує інформаційну взаємодію з іншими суб'єктами публічної влади й недержавними інституціями. Це можуть бути: меморандуми й угоди про обмін інформацією з правоохоронними органами, судами, органами місцевого самоврядування, міжнародними організаціями; протоколи про інтеграцію інформаційних систем; спільні накази про порядок інформаційної взаємодії. У сучасних умовах такі форми набувають дедалі більшого значення в зв'язку з переходом до комплексних електронних систем правосуддя, де ефективність діяльності кожного органу залежить від сумісності інформаційних стандартів і регламентів

Договірні форми дозволяють узгодити режими доступу до даних, визначити канали й протоколи обміну, встановити взаємні гарантії дотримання інформаційного законодавства й захисту персональних даних, що особливо

актуально в контексті європейських вимог до безпеки та конфіденційності судових даних.

Підсумовуючи, можна констатувати, що основні адміністративно-правові форми інформаційно-правового забезпечення діяльності органів прокуратури України утворюють цілісну багаторівневу систему. Їх належне доктринальне осмислення дозволяє не лише класифікувати різноманітні прояви інформаційної діяльності прокуратури, а й виявити вузькі місця правового регулювання, прогалини у відомчих актах, організаційні дисфункції та технологічні виклики. Саме вивчення цих форм у взаємозв'язку із загальноєвропейськими тенденціями цифровізації правосуддя створює базу для подальшого реформування інформаційно-правового забезпечення органів прокуратури України в руслі європейських стандартів верховенства права, прозорості та захисту прав людини.

У свою чергу, на відміну від загальних методів публічного адміністрування, які описують «як саме» публічна влада впливає на поведінку адресатів у будь-якій сфері, адміністративно-правові методи у сфері інформаційного забезпечення прокурорської діяльності концентруються на регулюванні руху даних, режимів доступу, якості інформаційних ресурсів та інформаційної безпеки. У вітчизняній адміністративно-правовій науці наголошується, що саме методи, поряд із формами, надають публічному адмініструванню керованого, цілеспрямованого характеру, визначаючи міру владності, інтенсивність та інструменти впливу на учасників правовідносин.

На нашу думку, до основних адміністративно-правових методів інформаційно-правового забезпечення діяльності органів прокуратури України можна віднести:

1. Регулятивно-нормувальні методи - їх зміст полягає у встановленні та деталізації через підзаконні й відомчі акти обов'язкових правил поведіння з інформацією, наприклад: порядку реєстрації відомостей у ЄРДР, ведення обліків і реєстрів, формування статистичних даних, визначення категорій інформації з обмеженим доступом, процедур доступу до відомчих інформаційних систем

тощо.

У випадку прокуратури регулятивно-нормувальний метод проявляється передусім через: а) видання Генеральним прокурором наказів та інструкцій, що детально описують процедури введення даних до ЄРДР, формування електронних справ, зберігання носіїв інформації; б) прийняття відомчих регламентів електронного документообігу, які визначають вимоги до електронного підпису, маршрутизації документів, строків обробки; в) запровадження внутрішніх політик щодо обробки персональних даних, службової інформації, інформації з обмеженим доступом. Такий метод забезпечує єдине розуміння «правил гри» в інформаційній сфері для всіх працівників прокуратури та пов'язаних органів, а отже виступає гарантією передбачуваності та юридичної визначеності інформаційних процесів.

2. Координаційно-організаційні методи управління інформаційними потоками - спрямовані на узгодження інформаційних потоків у межах системи прокуратури та у взаємодії з іншими суб'єктами публічної влади. Йдеться не лише про формальні угоди чи спільні накази, а й про адміністративно-правові прийоми узгодження стандартів даних, протоколів обміну, квот доступу до інформаційних ресурсів.

У сучасних дослідженнях публічного адміністрування звертається увага на те, що координація як метод стає особливо важливою в умовах мережевих, інтегрованих інформаційних систем, де результат діяльності одного органу безпосередньо залежить від якості й своєчасності даних, що їх надають інші органи [65, с. 210-212].

Для прокуратури координаційно-організаційні методи включають: а) погодження форматів та структур інформації, яка надходить від органів досудового розслідування, судів, контролюючих органів; б) установлення регламентів міжвідомчого обміну даними (канали передачі, строки, відповідальні особи); в) створення спільних інформаційних платформ (наприклад, для обміну даними в рамках спільних слідчих груп або між прокуратурою й антикорупційними органами).

3. Інформаційно-аналітичні та управлінсько-прогностичні методи - за допомогою яких органи прокуратури перетворюють «сирі» масиви даних на аналітичні продукти, потрібні для прийняття управлінських і процесуальних рішень. На відміну від класичних методів переконання чи примусу, тут йдеться про аналітичний вплив на управлінську волю суб'єктів прокуратури через статистику, узагальнення практики, кримінологічні прогнози, рейтингування показників діяльності тощо.

У монографії Р. Калюжного та співавторів підкреслюється, що інформаційне забезпечення управління включає не лише збирання даних, а й створення системи показників, критеріїв, алгоритмів аналізу, які дозволяють керівництву приймати раціональні, науково обґрунтовані рішення [46, с. 97–103].

У діяльності органів прокуратури це знаходить вираз у таких методах: а) побудова системи внутрішніх індикаторів якості роботи (строки внесення даних до ЄРДР, частка виправлених записів, кількість повернутих на доопрацювання статистичних звітів); б) використання порівняльного аналізу (бенчмаркінг) між регіональними прокуратурами на основі єдиних інформаційних масивів; в) застосування програмних засобів бізнес-аналітики для виявлення аномалій, типових помилок, корупціогенних ризиків.

Як зазначає Н. Лесько, запровадження сучасних інформаційних технологій дає змогу не просто прискорити документообіг, а й якісно змінити характер управління, перевівши його з інтуїтивного на даноцентричний рівень [3, с. 157–160]. Таким чином, інформаційно-аналітичні методи стають інструментом підвищення обґрунтованості прокурорських рішень, управлінського планування й стратегічного розвитку відомства.

4. Методи переконання, роз'яснення та формування інформаційної культури - традиційні для адміністративного права методи переконання та роз'яснення набувають у сфері інформаційно-правового забезпечення специфічного змісту. Вони спрямовані передусім на формування належної інформаційної культури працівників прокуратури, розвитку їхньої спроможності

коректно працювати з електронними ресурсами, дотримуватися режимів доступу, розуміти ризики порушення інформаційної безпеки.

Розділяючи позицію Є. І. Фролова, ми вважаємо що метод переконання передувє примусу й дозволяє досягати цілей управління без застосування репресивних засобів, шляхом навчання, роз'яснень, професійного «соціалізування» кадрів у необхідних стандартах поведінки [66, с. 115].

У діяльності органів прокуратури до таких методів належать: а) проведення навчальних семінарів і тренінгів з роботи в інформаційних системах, захисту інформації, обробки персональних даних; б) розроблення методичних рекомендацій, пам'яток, внутрішніх документів у форматі «питання–відповідь» щодо типових ситуацій (реагування на запити, робота з відкритими даними, публікація інформації на сайті); в) інформаційно-просвітницька робота з громадськістю, коли прокуратура пояснює межі доступності інформації, обмеження, пов'язані з таємницею досудового розслідування, правила подання інформаційних запитів тощо.

5. Контрольні та наглядові методи забезпечення інформаційної дисципліни - становлять окремий, надзвичайно значущий пласт адміністративно-правових методів у досліджуваній сфері. Їх завданням є забезпечення фактичного дотримання встановлених правил роботи з інформацією, своєчасне виявлення порушень та реагування на них.

Стосовно діяльності органів прокуратури контрольні й наглядові методи в інформаційно-правовій сфері включають: а) внутрішні перевірки своєчасності внесення відомостей до ЄРДР, повноти статистичної звітності, коректності ведення електронних справ; б) моніторинг дотримання строків розгляду запитів на публічну інформацію та якості відповідей; в) аудит доступу до інформаційних систем (перевірка логів, виявлення несанкціонованих доступів, аналіз аномальної активності користувачів); г) службові розслідування щодо витоків інформації, втрати носіїв, порушення порядку класифікації інформації.

З огляду на концентрацію чутливої інформації в органах прокуратури (персональні дані, дані досудового розслідування, інформація з обмеженим

доступом), ми вважаємо, що контрольні методи є також елементом загальнонаціональної системи інформаційної безпеки. Тут вони перетинаються з вимогами законодавства про захист персональних даних та про державну таємницю, що ускладнює й водночас підвищує значущість відомчих контрольних процедур.

6. Стимулюючі та мотиваційні методи у сфері управління інформаційними ресурсами - поряд з традиційними для української правової системи «жорсткими» методами (регулювання, контроль, примус) дедалі більшого значення набувають стимулюючі та мотиваційні методи. Їх сутність полягає у використанні внутрішньо-організаційних механізмів заохочення працівників прокуратури до дотримання високих стандартів інформаційної культури, ініціювання інновацій у сфері інформатизації.

На нашу думку, у сфері інформатизації управлінської діяльності, стимулювання якісної роботи з інформаційними ресурсами через систему оцінювання, преміювання, кар'єрного просування є не менш важливим, ніж формальне регулювання.

У системі органів прокуратури це може проявлятися: а) у включенні показників якості ведення інформаційних баз та дотримання інформаційних режимів до критеріїв оцінювання діяльності прокурорів; б) у моральному та матеріальному заохоченні команд, які впроваджують успішні ІТ-рішення, оптимізують документообіг, підвищують прозорість відомства; в) у підтримці ініціатив, спрямованих на відкриття даних та покращення комунікації з громадськістю через цифрові платформи. Стимулюючі методи, будучи м'якими за характером впливу, дозволяють формувати середовище, у якому належна інформаційна поведінка сприймається не як обтяжливий обов'язок, а як елемент професійної культури прокурора.

7. Методи адміністративного примусу - залишається одним із ключових методів забезпечення законності у сфері інформаційних відносин, зокрема й у діяльності органів прокуратури. Йдеться не лише про притягнення до адміністративної відповідальності за порушення інформаційного законодавства,

а й про здійснення дисциплінарного впливу на працівників органів прокуратури у випадку порушення ними інформаційних обов'язків.

Метод примусу в публічному адмініструванні застосовується тоді, коли інші, «м'якші» методи (переконання, стимулювання) виявилися неефективними, і має завдання відновлення правопорядку, попередження нових порушень. У площині інформаційно-правового забезпечення прокурорської діяльності це означає: а) можливість притягнення до адміністративної відповідальності посадових осіб інших органів за ненадання інформації прокуратурі, за надання завідомо недостовірних даних або порушення строків їх подання, якщо такі обов'язки прямо встановлені законом; б) застосування дисциплінарних стягнень до працівників прокуратури за порушення правил роботи з інформацією; в) ініціювання кримінальних проваджень у випадках, коли порушення інформаційних режимів утворює склад злочину (несанкціоноване втручання в роботу інформаційних систем, розголошення державної таємниці тощо).

Як показує аналіз навчального посібника «Інформаційне право України», адміністративна відповідальність у сфері інформаційних правовідносин розглядається як важливий елемент загальної системи гарантій правопорядку в інформаційній сфері [54, с. 374-380]. Відтак метод адміністративного примусу органічно доповнює регулятивні, контрольні та стимулюючі методи, забезпечуючи реальність виконання інформаційно-правових обов'язків.

8. Інноваційно-цифрові методи управління інформацією та ризиками - останніми роками у практиці органів правосуддя, у тому числі прокуратури, виокремлюються інноваційно-цифрові методи, пов'язані з використанням автоматизованих інформаційних систем, аналітики великих масивів даних та елементів штучного інтелекту. СЕРЕJ у Європейській етичній хартії щодо застосування штучного інтелекту в судових системах наголошує, що впровадження таких технологій повинно супроводжуватися чіткими гарантіями прозорості, підконтрольності алгоритмів, можливості людського перегляду рішень [67].

З адміністративно-правового погляду до інноваційно-цифрових методів

інформаційно-правового забезпечення в органах прокуратури можна віднести: а) використання алгоритмів автоматизованого контролю якості введення даних (виявлення «прогалин», дублювання, логічних суперечностей); б) застосування систем ризик-орієнтованого моніторингу, що на основі аналізу масивів даних сигналізують про потенційні порушення або аномалії в роботі окремих підрозділів; в) тестування систем підтримки прийняття рішень (decision support systems), які пропонують прокуророві варіанти дій на підставі зіставлення наявних даних із типізованими сценаріями.

На нашу думку, такі технології можуть істотно підвищити ефективність і прозорість роботи прокуратури, але лише за умови, що вони вбудовані у чітко визначені правові процедури й супроводжуються належною підготовкою кадрів. Тому інноваційно-цифрові методи не скасовують традиційні адміністративно-правові методи (регулювання, контроль, примус), а доповнюють їх новими інструментами управління інформаційними ресурсами та ризиками.

Отже, основні адміністративно-правові методи інформаційно-правового забезпечення діяльності органів прокуратури України утворюють цілісну, багаторівневу систему впливу на інформаційні процеси. Кожен із них виконує власну функцію, але лише в сукупності вони забезпечують належний рівень законності, ефективності, прозорості та безпеки використання інформації у прокурорській діяльності. Їх подальше доктринальне осмислення і нормативна конкретизація, з урахуванням європейських стандартів цифрового правосуддя, є необхідною умовою модернізації інформаційно-правового забезпечення органів прокуратури України в умовах цифрової трансформації та війни.

У свою чергу, виходячи із аналізу адміністративно-правових форм та методів інформаційно-правового забезпечення діяльності органів прокуратури України, варто акцентувати увагу на питанні їх взаємодії, як на наш погляд має розглядатися не як механічне поєднання двох самостійних категорій, а як внутрішньо узгоджений «каркас» і «динаміка» одного й того самого управлінського процесу. У площині інформаційно-правового забезпечення діяльності органів прокуратури це означає, що жодна форма (наказ про порядок

ведення ЄРДР, відповідь на запит про доступ до публічної інформації, протокол аудиту інформаційної системи) не є формальною, у ній завжди конкретизується певний метод (регулятивно-нормувальний, координаційний, контрольний, примусовий чи стимулюючий). Водночас методи не існують «у повітрі» – вони матеріалізуються саме через форми: наказ як форма є носієм методу регулювання, внутрішня перевірка – методу контролю, дисциплінарне стягнення – методу адміністративного примусу.

З позицій адміністративного та інформаційного права й спеціальної прокурорської доктрини така єдність форм і методів набуває додаткового змісту, оскільки від правильного вибору і поєднання інструментів залежить не лише ефективність роботи з даними, а й дотримання інформаційних прав людини, режимів конфіденційності та вимог цифрової безпеки. Для органів прокуратури, які функціонують у середовищі інтенсивної цифровізації, це означає необхідність свідомого конструювання зв'язків «форма–метод» при розробленні внутрішніх регламентів, впровадженні ІТ-рішень, побудові системи контролю та відповідальності, аби кожна нова інформаційна процедура була одночасно юридично коректною, технологічно стійкою й підконтрольною з точки зору прав людини.

2.4. Адміністративно-правовий статус суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України

В українській адміністративно-правовій доктрині й практиці застосування права поняття «суб'єкти інформаційно-правового забезпечення» досі прямо не закріплене в законодавстві. Тому його зміст доводиться вибудовувати доктринально, спираючись на системний, функціональний та інституційний підходи.

У узагальненому розумінні під суб'єктами інформаційно-правового забезпечення доцільно розуміти правосуб'єктних учасників публічних відносин (органи державної влади, органи прокуратури, інші установи, посадових осіб, окремі інформаційні системи чи технологічні комплекси), яким на підставі

закону або внутрішньоорганізаційних приписів доручено збір, обробку, зберігання, передачу та захист інформації, необхідної для здійснення повноважень органів прокуратури.

Для їх характеристики принциповими є такі ознаки: а) правосуб'єктність – наявність визначеного правового статусу та нормативного закріплення відповідного органу, структурного підрозділу чи інформаційної системи; б) функціональна залученість – участь у ключових інформаційних процесах (збирання, оброблення, передача, аналіз, захист даних); в) нормативна регламентація – ґрунтування діяльності на положеннях законодавства про органи прокуратури, інформаційного та адміністративного права, а також на актах, що визначають правовий режим інформаційних систем; г) стала взаємодія з органами прокуратури – фактичне виконання функцій інформаційно-правового супроводу їх діяльності через відповідні системи, служби та підрозділи інформаційної безпеки.

За організаційно-правовою формою, статусом і рівнем підпорядкованості такі суб'єкти можуть істотно відрізнятися, однак їх інтегрує спільна ціль – створення належних правових і технологічних умов для повноцінного функціонування органів прокуратури в інформаційному вимірі.

Концептуальне наповнення цього поняття спирається на аналіз адміністративно-правових механізмів управління інформаційними процесами, ідеї публічного адміністрування, а також на норми Законів України «Про інформацію», «Про доступ до публічної інформації», «Про прокуратуру» та пов'язаних актів. У науковій літературі підкреслюється, що інформаційне забезпечення органів прокуратури охоплює не лише масив інформаційних ресурсів, а й спеціалізовані системи, канали комунікації та службові підрозділи, відповідальні за інформування, аналіз і оцінку відомостей.

З точки зору адміністративного права діяльність суб'єктів інформаційно-правового забезпечення органів прокуратури належить до сфери публічної адміністрації. Оскільки органи прокуратури здійснюють нагляд за додержанням законів, відповідна інформаційна інфраструктура виступає інструментом

адміністративно-правового забезпечення реалізації цієї наглядової, представницької та інших функцій.

Зміст суб'єктів інформаційно-правового забезпечення виявляється в їх ролі інституційних посередників між інформаційними ресурсами та органами прокуратури як носіями публічної влади. Фактично йдеться про організаційні структури й механізми, що трансформують розрізнену інформацію в юридично значимі та управлінськи придатні дані для прийняття рішень, виконання наглядових, представницьких та аналітичних повноважень.

Функціонально такі суб'єкти покликані забезпечувати реалізацію права на інформацію, організувати її обіг, обробку та захист у встановлених законом межах. Їх завданням є не тільки задоволення поточних інформаційних потреб органів прокуратури, а й підтримка стратегічного розвитку інформаційної складової їх діяльності, формування аналітичної бази для управлінських рішень, організація кіберзахисту, забезпечення відкритості та публічної підзвітності [68, с. 19].

У системі права зазначені суб'єкти виступають адресатами правового регулювання: норми визначають їх правосуб'єктність, межі компетенції, підпорядкованість і види юридичної відповідальності. Джерельну основу становлять галузеві закони, міжвідомчі угоди та внутрішні регламенти органів прокуратури.

Правова природа цих суб'єктів полягає в тому, що їх діяльність безпосередньо спрямована на забезпечення інформаційної складової реалізації функцій органів прокуратури: інформаційного обслуговування, цифрової підтримки управлінських процесів, аналітичної роботи, документування, комунікацій, оброблення персональних і службових даних. Вони виступають активними учасниками адміністративно-правових відносин з нормативно визначеною або делегованою компетенцією у сфері інформаційно-правового забезпечення. У адміністративно-правовому вимірі це проявляється через їх організаційно-правову форму, інституційне підпорядкування, обсяг повноважень, функціональні межі та закріплену відповідальність.

Статус суб'єктів інформаційно-правового забезпечення має ознаки публічно-правових утворень: вони діють за умов правового імперативу, реалізують повноваження, встановлені безпосередньо законом або внутрішніми актами, і несуть дисциплінарну, адміністративну, а в окремих випадках – і кримінальну відповідальність за неналежне виконання покладених функцій. Така модель забезпечує легітимність їх діяльності в системі органів прокуратури, дозволяє формувати прозору систему підконтрольності та підзвітності в інформаційній сфері [69, с. 35].

Комплексний характер їх правової природи зумовлює поєднання кількох галузевих начал. Провідним є адміністративно-правовий компонент, що регулює організацію, управління, субординацію та взаємодію, але вагомий вплив мають також норми інформаційного, кримінального процесуального, конституційного та міжнародного права [23, с. 88].

Функціонально-правовий аспект діяльності цих суб'єктів полягає в їх участі у формуванні та реалізації інформаційної політики органів прокуратури: забезпеченні постійного доступу до актуальної й достовірної інформації, її обробці, систематизації, збереженні та захисті від втрат, витоків чи несанкціонованого використання відповідно до законодавчих вимог.

Принциповим є відмежування суб'єктів інформаційно-правового забезпечення від суто технічних елементів інфраструктури або пасивних носіїв даних. Лише ті учасники, які мають юридично закріплений статус і певний обсяг адміністративної чи управлінської компетенції, можуть розглядатися як суб'єкти в адміністративно-правовому значенні. Це дозволяє уникати ототожнення допоміжних технологічних рішень (серверів, хмарних платформ, програмних інтерфейсів) з реальними суб'єктами правовідносин, що формують і підтримують інформаційний механізм діяльності органів прокуратури.

Узагальнюючи викладене, правову природу суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України доцільно розглядати як багатовимірну конструкцію, що поєднує інституційний, функціональний, адміністративно-компетенційний і нормативний компоненти.

Вони є не лише допоміжними ланками у внутрішній структурі органів прокуратури, а й самостійними елементами системи публічного управління, які забезпечують стабільність, ефективність та законність реалізації прокурорських повноважень в умовах інформаційного суспільства. Такий статус обумовлює потребу в чіткому й сучасному правовому регулюванні, методичному супроводі та інтеграції їх діяльності в цифрові процеси, що визначають якість публічної влади в Україні.

З огляду на це, суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України можна визначити як уповноважені публічно-правові утворення, структурні підрозділи, посадових осіб та техніко-інформаційні системи, які на основі нормативно визначених повноважень здійснюють збір, обробку, зберігання, передачу, захист і правову регламентацію інформації, необхідної для реалізації функцій органів прокуратури, забезпечення внутрішнього управління, публічної підзвітності та належного рівня інформаційної безпеки [70, с. 735].

У подальшому аналіз суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України доцільно вибудовувати на засадах методологічного плюралізму, тобто свідомого поєднання класичних і сучасних підходів до осмислення правових та управлінських явищ. У цьому контексті ключове значення мають такі методи:

1. Системно-структурний підхід дає змогу розглядати відповідних суб'єктів не як окремі, відокремлені ланки, а як взаємопов'язані елементи єдиного інформаційно-правового комплексу в межах органів прокуратури. До цього комплексу належать організаційні структури (служби, відділи, управління), технологічні рішення (реєстри, автоматизовані бази даних), кадровий потенціал (спеціалісти, аналітики), нормативно-правова основа (закони, інструкції, накази) та засоби інформаційної взаємодії (програмні інтерфейси, інформаційні шлюзи, системи електронного документообігу).

2. Функціональний підхід орієнтує на розподіл суб'єктів залежно від характеру покладених на них завдань: виділяються, зокрема, суб'єкти,

відповідальні за первинний збір відомостей; суб'єкти, що забезпечують захист інформації; суб'єкти, які безпосередньо формують акти прокурорського реагування та інші юридично значущі документи.

3. Інституціональний метод акцентує увагу на правовому становищі суб'єктів, формах їх створення, характері підпорядкованості та внутрішніх організаційних зв'язках. Завдяки цьому підходу можливо чітко розрізнити, з одного боку, внутрішніх суб'єктів (організаційно інтегрованих у систему органів прокуратури), а з іншого – зовнішніх суб'єктів (державних і недержавних інституцій, що взаємодіють із прокуратурою в інформаційній площині).

4. Компаративістський підхід передбачає зіставлення національної моделі з практикою окремих держав – членів Європейського Союзу (зокрема Франції та Польщі), де організація інформаційно-правового забезпечення прокуратури має детальну нормативну регламентацію, а статус відповідних суб'єктів визначається через вимоги цифрового врядування, відкритості діяльності та охорони персональних даних [71, с. 549].

5. Діалектичний метод дає змогу врахувати не лише «зріз» суб'єктів у певний момент, а й їхню трансформацію в умовах цифровізації, запровадження воєнного стану, зміни організаційно-штатної структури органів прокуратури. Саме завдяки діалектичному підходу простежується еволюція уявлень про суб'єкта під впливом технологічних новацій та оновлення законодавства.

З огляду на викладене, вважаємо виправданим для уніфікації підходів до виокремлення й дослідження суб'єктів інформаційно-правового забезпечення у діяльності органів прокуратури України застосування чітко окресленої системи критеріїв суб'єктності: а) наявність публічно-правового статусу, підтвердженого нормативно-правовим актом, положенням про орган (підрозділ) або посадовою інструкцією; б) закріплення повноважень у сфері роботи з інформацією – від її збирання й оброблення до захисту, використання чи поширення в межах компетенції органів прокуратури; в) зв'язок із функціональним призначенням органів прокуратури – забезпечення виконання їхніх завдань за допомогою інформаційних засобів (підтримання публічного обвинувачення, охорона

публічного інтересу, реагування на порушення закону); г) юридична відповідальність за результати діяльності, що передбачає існування механізмів контролю, нагляду, внутрішнього аудиту та підзвітності.

На наш погляд, така система критеріїв дає змогу не лише коректно ідентифікувати суб'єктів інформаційно-правового забезпечення, а й ранжувати їх за значущістю – залежно від обсягу компетенції, впливу на реалізацію прокурорських повноважень і критичності для безперервного функціонування інформаційної інфраструктури органів прокуратури.

У правовому полі України інституційна модель органів прокуратури як елементу публічної влади врегульована доволі чітко: за нею саме цей орган покликаний забезпечувати охорону прав і свобод людини, публічного інтересу та здійснювати підтримання державного обвинувачення. Стаття 7 Закону України «Про прокуратуру» № 1697-VII від 14 жовтня 2014 року визначає, що до системи органів прокуратури належать Офіс Генерального прокурора, обласні прокуратури, окружні прокуратури, а також Спеціалізована антикорупційна прокуратура, якій надано спеціальний статус у сфері протидії корупції [13].

Таке нормативне формулювання дає змогу розглядати окремі ланки прокурорської системи як самостійні суб'єкти публічного адміністрування, наділені повноваженнями у сфері інформаційно-правового забезпечення. Саме вони забезпечують організаційний каркас для функціонування внутрішніх і зовнішніх каналів інформаційної взаємодії, обміну правовою інформацією, ведення офіційних реєстрів та реалізації механізмів захисту інформаційних прав фізичних і юридичних осіб.

У площині адміністративного права Офіс Генерального прокурора виконує роль вищої управлінської ланки щодо обласних та окружних прокуратур. Обласні прокуратури, у свою чергу, здійснюють керівний вплив на окружні прокуратури, що діють у межах відповідної адміністративно-територіальної одиниці. Така побудова формує вертикаль організаційної підпорядкованості, окреслює межі компетенції кожної ланки та забезпечує дієвий внутрішній контроль, що є типовими рисами суб'єктів публічної адміністрації зі

спеціальною юрисдикцією [72, с. 151].

Окремої уваги заслуговує Спеціалізована антикорупційна прокуратура (САП), якій надано статус юридичної особи публічного права. Вона має відокремлене майно, самостійно відкриває рахунки в органах казначейського обслуговування, використовує власну печатку з Державним Гербом України та повним найменуванням, що свідчить про високий ступінь її інституційної автономії. У межах антикорупційної компетенції САП здійснює інформаційно-правове забезпечення у тісній координації з Національним антикорупційним бюро України, формуючи розгалужену мережу аналітичних, процесуальних та інформаційних підрозділів. Територіальне розміщення центрального апарату та підрозділів САП синхронізоване з інфраструктурою НАБУ, що забезпечує швидкий обмін даними, ефективну обробку й подальший аналіз інформації про корупційні правопорушення.

Принцип єдності системи органів прокуратури, закріплений у законодавстві, реалізується через спільні засади організації та діяльності, однаковий правовий статус прокурорів, уніфіковані підходи до організаційного забезпечення, централізоване фінансування з Державного бюджету України, а також через функціонування органів прокурорського самоврядування, які вирішують кадрові, дисциплінарні та методичні питання. Сукупність цих чинників створює нормативно-організаційне підґрунтя для формування єдиної інформаційної політики, у межах якої діють суб'єкти інформаційно-правового забезпечення на всіх рівнях прокурорської системи.

З урахуванням цієї інституційно-організаційної логіки доцільно проаналізувати кожен ланку органів прокуратури, виокремивши їх адміністративно-правові особливості та роль у забезпеченні інформаційно-правового режиму, зокрема:

1. Офіс Генерального прокурора як центральна ланка. У побудові сучасної системи органів прокуратури України, що функціонує як особливий суб'єкт публічної влади в межах єдиного державно-владного механізму, провідне місце в організаційному та інформаційному забезпеченні належить Офісу

Генерального прокурора та Спеціалізованій антикорупційній прокуратурі. Саме ці інституції задають основні вектори політики у сфері інформаційно-правового забезпечення, оскільки володіють повноваженнями з організації, координації, аналітичного опрацювання й нормативного регулювання діяльності всієї прокурорської вертикалі.

З адміністративно-правового погляду Офіс Генерального прокурора виступає ключовим центральним елементом прокурорської системи, на який покладено здійснення повноважень найвищого рівня. Його внутрішня побудова ґрунтується на поєднанні функціональної та предметної спеціалізації: створюються департаменти, управління, відділи, а також Генеральна інспекція. Окремі управління й відділи можуть діяти як самостійні структурні одиниці або входити до складу департаментів, формуючи багаторівневу систему адміністративної підпорядкованості. Така організаційна конструкція забезпечує цілісність інформаційної діяльності та дозволяє чітко розмежувати повноваження у сферах діловодства, аналітики, інформаційного супроводу та внутрішнього електронного управління.

У площині нормативного керівництва Генеральний прокурор реалізує свою адміністративну компетенцію шляхом видання наказів, якими упорядковуються внутрішні організаційні процеси в органах прокуратури, у тому числі регламентується електронний документообіг, порядок зберігання й використання інформації, функціонування інформаційних систем, організація захисту даних. Такі відомчі акти приймаються на підставі та на виконання Конституції й законів України й виступають важливими засобами регулювання діяльності суб'єктів інформаційно-правового забезпечення в межах прокурорської системи.

З огляду на вимоги правової визначеності, прозорості та відкритості публічного управління, накази Генерального прокурора нормативного характеру підлягають офіційному оприлюдненню державною мовою на вебсайті Офісу Генерального прокурора не пізніше наступного робочого дня після підписання, з урахуванням обмежень щодо інформації з обмеженим доступом. Як загальне

правило, такі акти набувають чинності з дня оприлюднення, якщо інший момент вступу в дію не встановлено самим наказом, але в будь-якому разі не раніше фактичного опублікування. Це забезпечує доступність та передбачуваність нормативних приписів, що впорядковують інформаційну складову діяльності органів прокуратури.

Спеціалізована антикорупційна прокуратура посідає особливе місце в структурі суб'єктів прокурорської системи. Формально будучи елементом єдиної системи органів прокуратури, вона водночас має окремий правовий статус юридичної особи публічного права. У межах САП функціонують спеціалізовані підрозділи, зорієнтовані на виконання завдань інформаційно-правового забезпечення, зокрема: канцелярія (включно з підрозділом електронного документообігу), служба режимно-секретної роботи, підрозділ з питань персоналу, відділ внутрішнього контролю, а також інші структурні одиниці, необхідні для належного здійснення антикорупційних повноважень. Їх діяльність будується на основі внутрішніх положень і наказів, обов'язкових для всіх працівників САП, а адміністративне керівництво здійснює заступник Генерального прокурора – керівник САП або уповноважена ним особа. Це поєднує організаційну самостійність САП із її включеністю до загальної системи прокуратури.

Просторова відокремленість Спеціалізованої антикорупційної прокуратури від адміністративних будівель Офісу Генерального прокурора, обласних та окружних прокуратур має не лише організаційне, а й інституційно-правове значення. Окремі службові приміщення слугують додатковою гарантією функціональної незалежності, зменшують ризики адміністративного впливу та сприяють зміцненню суспільної довіри до антикорупційного сегменту прокурорської діяльності.

Порядок організації роботи САП, зокрема у сфері інформаційно-правового забезпечення, визначається відомчими актами керівника САП. Такі накази обов'язкові для виконання всіма працівниками, що здійснюють функції в межах антикорупційної юрисдикції. У контексті адміністративного права це приклад

локального нормотворення в межах публічного органу, що спирається на делеговані повноваження і дозволяє оперативно реагувати на управлінські потреби.

Важливо, що принцип незалежності прокурорів САП має безпосередній і реальний зміст. Генеральний прокурор, його перший заступник та інші заступники не можуть давати їм вказівки щодо здійснення процесуальних повноважень у конкретних кримінальних провадженнях. Будь-які адміністративно-організаційні рішення, що стосуються діяльності САП, приймаються лише за погодженням з її керівником, що додатково закріплює автономний статус цього суб'єкта в умовах вертикально організованої прокурорської системи.

У підсумку, і Офіс Генерального прокурора, і Спеціалізована антикорупційна прокуратура сформували власні адміністративно-правові механізми здійснення інформаційно-правових функцій. Їх внутрішня структура, система підпорядкування, нормативне регулювання та порядок внутрішнього управління дозволяють розглядати ці органи як ключові елементи багаторівневої системи суб'єктів інформаційного забезпечення в органах прокуратури України, через які реалізуються інформаційні повноваження, підтримується правовий режим інформації та функціонує електронне управління.

Узагальнюючи ми вважаємо, що Офіс Генерального прокурора постає системним «ядром» механізму інформаційно-правового забезпечення: саме тут формується нормативна та організаційна рамка, що охоплює видання відомчих актів, архітектуру підпорядкування й спеціалізацію підрозділів, а також адміністрування ключових інформаційних систем (ЄРДР, ІАС «ОСОП», ІС «СЕД»). Концентрація компетенції в Департаменті інформаційних технологій, Департаменті документального забезпечення та в управлінні організаційного забезпечення Єдиного реєстру досудових розслідувань і інформаційно-аналітичної роботи забезпечує єдність стандартів діловодства, безперервність електронного документообігу, узгодженість статистики та відповідальне володіння даними на всіх рівнях прокурорської системи. Саме через ці

інституційні «вузли» механізм набуває реальної дії: від визначення правил і процедур - до технічної підтримки, моніторингу, доступу та захисту інформації.

Що стосується ролі САП саме в межах інформаційно-правового забезпечення, то варто відзначити, що цей орган прокуратури як юридична особа публічного права організує власний документообіг (у т.ч. електронний), режимно-секретну роботу, управління персоналом і внутрішній контроль через підрозділи, що утворюються окремо від Офісу Генерального прокурора. Ввідповідні питання врегульовуються локальними наказами заступника Генерального прокурора - керівника САП, обов'язковими для всіх прокурорів і працівників САП. Територіальне розміщення САП у відокремлених приміщеннях і пряма підпорядкованість її керівника Генеральному прокурору поєднуються з процесуальною незалежністю. Таким чином, дотичність САП до механізму інформаційно-правового забезпечення є «внутрішньо-організаційною», САП самостійно встановлює та забезпечує режим роботи з інформацією в межах власної юрисдикції (документообіг, захист, доступ, контроль), водночас інтегруючись у загальносистемні стандарти прокуратури через обов'язкове погодження адміністративних рішень і методичну сумісність.

2. Обласні прокуратури - посідають проміжний, але визначальний рівень: саме вони забезпечують стабільність територіальної організації, здійснюють прокурорський нагляд, координують діяльність підпорядкованих окружних прокуратур і, що принципово в умовах цифровізації, відповідають за належний стан інформаційно-правового забезпечення на регіональному рівні.

Стаття 10 Закону України «Про прокуратуру» встановлює, що до обласних прокуратур належать прокуратури областей, прокуратура Автономної Республіки Крим і міста Севастополя, а також Київська міська прокуратура [13]. Кожен із цих органів виступає окремим елементом єдиної системи прокуратури України з власною адміністративно-управлінською компетенцією в межах визначеної територіальної юрисдикції.

Очолює обласну прокуратуру керівник відповідного рівня – прокурор області, прокурор Автономної Республіки Крим і міста Севастополя або керівник

Київської міської прокуратури. Їх діяльність організаційно підтримується першим заступником і кількома заступниками (але не більше трьох), що дає змогу раціонально розподілити функціональні обов'язки у сферах організаційного, адміністративного та аналітичного управління.

У середині обласних прокуратур формуються структурні підрозділи – управління та відділи, які забезпечують документування, опрацювання та аналіз відомостей, систематизацію правозастосовної практики, а також координацію діяльності окружних прокуратур. У такий спосіб вони виконують роль безпосередніх суб'єктів інформаційно-правового забезпечення, оскільки саме через ці підрозділи здійснюється збір, оброблення, аналітичне опрацювання й передача інформації, необхідної для виконання прокурорських повноважень у межах конкретного регіону.

У функціональному вимірі керівник обласної прокуратури реалізує комплекс повноважень, що мають ознаки публічного управління, у тому числі й в інформаційно-правовій сфері. До його адміністративної компетенції належать: а) представництво обласної прокуратури у взаємодії з органами державної влади, місцевого самоврядування, підприємствами, установами та організаціями; б) загальна організація поточної роботи обласної прокуратури та координація діяльності її структурних підрозділів; в) призначення й звільнення прокурорів обласного й окружного рівнів, а також прокурорів-стажистів за процедурою, визначеною Законом України «Про прокуратуру»; г) затвердження внутрішніх адміністративних актів (наказів, розпоряджень, положень), що регулюють організацію роботи обласної прокуратури, у тому числі порядок обігу, зберігання та захисту інформації; г) організація контролю за веденням та аналізом статистичних показників, вивченням і узагальненням правозастосовної практики для забезпечення належного інформаційно-аналітичного супроводу діяльності прокурорів.

Зазначені повноваження дозволяють розглядати обласну прокуратуру як відносно самостійного суб'єкта інформаційно-правового забезпечення, який діє в межах делегованих повноважень, але має простір адміністративної автономії

щодо організації доступу до інформації, її обігу та захисту. Керівник обласної прокуратури, видаючи накази в межах своєї компетенції, формує обов'язкові для працівників правила внутрішньої організації, у тому числі в інформаційній сфері.

У площині інформаційно-правового забезпечення такі накази, зокрема, можуть стосуватися: а) затвердження внутрішніх регламентів, що визначають порядок руху інформації в обласній прокуратурі; б) організації та підтримання систем електронного документообігу; в) призначення відповідальних осіб за зберігання та актуальність електронної доказової бази; г) встановлення процедур доступу до інформаційно-аналітичних ресурсів прокуратури; г) визначення заходів із забезпечення інформаційної безпеки та охорони службової чи конфіденційної інформації.

Отже, обласні прокуратури як проміжний рівень у ієрархії органів прокуратури України виконують подвійну функцію в інформаційно-правовій площині. З одного боку, вони імплементують політику, сформульовану на рівні Генерального прокурора, реалізуючи відповідні нормативні та методичні акти. З іншого боку, виступають самостійними нормо-утворюючими та координуючими суб'єктами в межах власної територіальної юрисдикції, розробляючи локальні підходи до організації інформаційних процесів і забезпечуючи їх реалізацію в підпорядкованих окружних прокуратурах.

3. Окружні прокуратури - у розбудові системи органів прокуратури України саме окружні прокуратури формують її «основу», оскільки діють безпосередньо на місцевому рівні й забезпечують реалізацію завдань прокуратури в межах конкретної адміністративно-територіальної одиниці. Стаття 12 Закону України «Про прокуратуру» передбачає, що перелік окружних прокуратур і межі їх територіальної юрисдикції затверджуються наказом Генерального прокурора України [73]. Той самий суб'єкт публічного управління ухвалює рішення щодо створення, реорганізації чи ліквідації окружних прокуратур, а також визначає їх структуру, компетенцію та штат, що є черговим підтвердженням централізованої побудови прокурорської системи.

Орган очолює керівник окружної прокуратури, якому підпорядковані

перший заступник та, як правило, не більше двох заступників. Така модель управління відповідає засадам адміністративної субординації й забезпечує оптимальний розподіл управлінських функцій усередині органу. За потреби в структурі окружної прокуратури можуть створюватися окремі відділи, які виконують спеціалізовані функції (процесуальні, організаційні, аналітичні тощо).

З адміністративно-правової точки зору керівник окружної прокуратури здійснює сукупність управлінських і організаційно-розпорядчих повноважень, значна частина яких прямо пов'язана з інформаційно-правовим забезпеченням. До таких повноважень належать, зокрема: а) офіційне представництво окружної прокуратури у взаєминах з органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями; б) організація поточної діяльності окружної прокуратури на основі затверджених регламентів, положень та внутрішніх інструкцій; в) забезпечення належного ведення й аналізу статистичних показників як елементу системи адміністративної звітності та внутрішнього контролю за інформаційними процесами; г) організація вивчення та узагальнення правозастосовної практики з метою відстеження відповідності між приписами законодавства й реальними результатами їх застосування; г) створення умов для повноцінного інформаційно-аналітичного супроводу діяльності прокурорів, що сприяє підвищенню якості реалізації процесуальних і наглядових повноважень.

З огляду на те, що окружні прокуратури є найближчою до населення та місцевих органів влади ланкою, саме через них проходить значний обсяг правової інформації, яка циркулює в системі публічного управління. У цьому контексті адміністративно-правовий статус керівника окружної прокуратури охоплює, серед іншого, організацію внутрішнього документообігу, встановлення режиму доступу до службової інформації, координацію впровадження електронних систем обліку та обміну даними.

Таким чином ми вважаємо, що окружні прокуратури формують «операційний контур» механізму інформаційно-правового забезпечення, як

базова ланка вони безпосередньо реалізують політики й стандарти, визначені вищими рівнями, організовують внутрішній документообіг (у т.ч. електронний), ведення та верифікацію статистики, узагальнення практики, адміністрування доступів і захист службової інформації. За потреби утворюють відділи, а керівник, діючи в межах делегованої компетенції, видає обов'язкові внутрішні акти та координує інформаційно-аналітичну підтримку прокурорів. У цьому контексті суб'єктний склад на місцевому рівні охоплює дві категорії: прокурорів (як носіїв публічно-владних повноважень і користувачів ЄРДР) та державних службовців (які забезпечують діловодство, ІТ-супровід, облік і звітність із застосуванням ІС «СЕД» та ІАС «ОСОП»). Функціонування окружної ланки додатково підкріплюється наявністю фахівців з інформаційних технологій, що підтримують прикладне програмне забезпечення.

Отже, окружна прокуратура є не лише структурною одиницею, а й первинним осередком, у якому норми та регламенти перетворюються на повсякденні інформаційні процедури - від реєстрації й обігу даних до їхнього аналізу й передачі за вертикаллю.

Крім того, у контексті з'ясування ролі Офісу Генерального прокурора як провідного суб'єкта інформаційно-правового забезпечення діяльності органів прокуратури України доцільно зосередити увагу на тих структурних підрозділах, через які реалізуються повноваження Генерального прокурора у сфері інформаційного та інформаційно-технічного супроводу. Вирішальне значення для такого аналізу мають накази Генерального прокурора, якими затверджено Положення про самостійні структурні підрозділи Офісу Генерального прокурора, оскільки саме в них деталізуються напрями спеціалізації працівників, що забезпечують інформаційно-аналітичний, документальний і технічний супровід виконання функцій органів прокуратури загалом. Йдеться, зокрема, про низку відомчих актів, кожен з яких регламентує діяльність конкретного структурного елемента Офісу Генерального прокурора. Сукупно ці та інші нормативно-організаційні акти охоплюють понад три десятки структурних підрозділів, серед яких – підрозділи інформаційно-аналітичного, кадрового,

кібербезпекового, міжнародного та іншого профілю [74].

У структурі Офісу Генерального прокурора особливий інтерес для дослідження становлять три утворення, що безпосередньо забезпечують інформаційно-технічний та документальний вимір діяльності всієї прокурорської системи:

1. Департамент інформаційних технологій - виконує провідну роль у цифровій трансформації органів прокуратури, відповідаючи за впровадження сучасних інформаційно-комунікаційних технологій, організацію технічного захисту інформації та підтримання стабільного функціонування ключових інформаційних систем.

У його структурі виокремлюються: 1) відділ впровадження та супроводження інформаційних систем, який опікується розробленням, адаптацією та супроводженням прикладного програмного забезпечення, адмініструє основні інформаційні платформи – інформаційну систему «ЄРДР» (Єдиний реєстр досудових розслідувань), інформаційно-аналітичну систему «ОСОП» (облік суб'єктів оперативно-розшукової діяльності та процесу), систему електронного документообігу «СЕД» тощо, а також відповідає за підготовку користувачів і функціонування електронних довірчих послуг; 2) відділ адміністрування мереж та технічного захисту інформації, який забезпечує безперебійну роботу ІТ-інфраструктури, обслуговує апаратно-програмні комплекси, організовує захист персональних даних, контролює мережі електронного зв'язку та відповідає за підтримання належного рівня кібербезпеки; 3) відділ забезпечення функціонування центрів обробки даних та мультимедійних систем, що здійснює технічну підтримку серверних потужностей, супроводжує мультимедійні комплекси та забезпечує технічну складову комунікаційних процесів у межах Офісу Генерального прокурора.

2. Департамент документального забезпечення - виконує функцію «ядра» системи документообігу органів прокуратури. Він відповідає за уніфікацію правил роботи з документами, організацію і підтримання електронного документообігу (інформаційна система «СЕД»), належне зберігання службової

кореспонденції, її облік, своєчасне знищення чи передачу до архівних установ. Особливий акцент робиться на дотриманні вимог законодавства щодо обробки персональних даних, охорони службової інформації та організації взаємодії з обласними прокуратурами в частині документообігу.

До функціональних завдань департаменту, зокрема, належать: узгодження форматів електронної взаємодії з іншими органами державної влади; редагування та технічне опрацювання службових документів; ведення та поповнення документаційного фонду; організація передачі документів до Центрального державного архіву вищих органів влади та управління України (ЦДАВО України).

3. Управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи - виконує функцію «центрів тяжіння» для кримінальної статистики й аналітики. Його основним завданням є організація ведення Єдиного реєстру досудових розслідувань, формування статистичних показників щодо кримінальної протиправності, узгодження національних статистичних підходів із міжнародними стандартами, а також підготовка узагальнених інформаційно-аналітичних матеріалів для керівництва та інших зацікавлених суб'єктів.

Структурно управління складається з чотирьох відділів: а) відділу організаційного забезпечення ведення ЄРДР; б) відділу інформаційно-аналітичної роботи; в) відділу інформаційного забезпечення учасників кримінального провадження та інноваційного розвитку; г) відділу організаційного забезпечення статистики кримінальної протиправності.

До кола його завдань належать: координація заходів щодо статистичного обліку кримінальних правопорушень; контроль за повнотою й достовірністю внесення даних до відповідних реєстрів; взаємодія з органами досудового розслідування та судами; інтеграція національної звітності з європейськими електронними платформами (зокрема е-платформами Європейської комісії); розроблення цифрових інструментів для автоматизації збору й обробки статистичних даних; моніторинг кримінальної ситуації; аналіз правозастосовної практики; впровадження стандартів статистичної конфіденційності.

З огляду на викладене можна стверджувати, що система суб'єктів інформаційно-правового забезпечення в органах прокуратури України має складну багаторівневу побудову та значний ступінь функціональної спеціалізації. Адміністративно-правові механізми, які її регламентують, дозволяють цілісно реалізовувати завдання цифровізації, забезпечувати інформаційну безпеку, упорядковувати документообіг, організовувати ведення ЄРДР і формувати аналітичний супровід прокурорської діяльності. У кожному підрозділі формується власна адміністративно-правова компетенція, що в підсумку забезпечує системність функціонування прокуратури як інституту публічного права.

Окремо слід зазначити, що прокурори та державні службовці згаданих підрозділів здійснюють свої повноваження з використанням електронного цифрового підпису (ЕЦП) та працюють із базовими інформаційними системами прокуратури України – системою електронного документообігу «СЕД», інформаційно-аналітичною системою «ОСОП» та Єдиним реєстром досудових розслідувань, доступ до якого мають виключно прокурори.

Узагальнення змісту наказів Генерального прокурора дає підстави констатувати, що в межах Офісу Генерального прокурора сформовано розгалужену мережу спеціалізованих структур, які виступають невід'ємними суб'єктами інформаційно-правового забезпечення. Саме їх діяльність гарантує інформаційний суверенітет, належний рівень захисту даних, дієвий внутрішній контроль, можливість повноцінної електронної взаємодії та належну технологічну підтримку всієї системи органів прокуратури України.

Підсумовуючи викладене, адміністративно-правовий статус суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України постає як багаторівнева, але внутрішньо узгоджена система, що поєднує інституційну, функціональну та нормативно-компетенційну складові. Офіс Генерального прокурора, Спеціалізована антикорупційна прокуратура, обласні й окружні прокуратури та їх спеціалізовані підрозділи діють як публічно-правові утворення, наділені чітко визначеними повноваженнями у сфері роботи з

інформацією. Поєднання централізованого керівництва з елементами адміністративної автономії на різних рівнях дозволяє забезпечити належний правовий режим даних, сталу роботу електронних систем та підзвітність органів прокуратури. Саме через призму адміністративно-правового статусу цих суб'єктів розкривається реальний зміст інформаційно-правового забезпечення прокуратури як інституції публічної влади, від якого безпосередньо залежить ефективність, прозорість і легітимність здійснення прокурорських повноважень в умовах сучасних трансформацій державного управління.

Висновки до розділу 2

1. Система видів інформаційно-правового забезпечення, поєднана з їх науково обґрунтованою класифікацією, дозволяє розглядати інформаційну діяльність прокуратури як цілісний, багатовимірний комплекс, а не як сукупність розрізнених процесів. Виокремлення процесуального, організаційно-управлінського, комунікаційного, аналітичного та безпекового блоків у взаємозв'язку з такими критеріями, як джерело формування інформації, правовий режим доступу, спосіб фіксації та форма реалізації, створює чіткий методологічний каркас для подальшої уніфікації практики. Такий підхід дає змогу узгодити відомчі стандарти роботи з інформацією з вимогами законодавства, мінімізувати дублювання інформаційних потоків і підвищити прозорість прийняття прокурорських рішень.

2. Розмежування рівнів та напрямів інформаційно-правового забезпечення (від нормативно-правового та інституційного до організаційно-процесуального, інфраструктурно-технологічного й індивідуально-посадового) демонструє багат шаровість адміністративно-правового механізму в цій сфері. З одного боку, це дозволяє чітко визначити, на якому рівні виникають ключові інформаційні ризики та де саме слід посилювати регулювання чи контроль. З іншого боку, виділення процесуального, управлінського, аналітико-прогнозного, комунікаційного та безпекового напрямів забезпечує керованість інформаційних потоків, раціональний розподіл ресурсів і можливість адресної відповідальності

суб'єктів за результати інформаційної діяльності. У підсумку підвищується передбачуваність та стабільність функціонування всієї прокурорської системи в інформаційному вимірі.

3. Адміністративно-правові форми та методи інформаційно-правового забезпечення виступають інструментами, через які воля держави трансформується у конкретні правила організації інформаційних процесів у прокуратурі. Нормативні акти, індивідуальні адміністративні рішення, внутрішні регламенти, процедурні стандарти контролю та відповідальності задають рамки законності, відтворюваності та підконтрольності руху інформації. Вони забезпечують єдність підходів до ведення електронного документообігу, роботи з реєстрами, аналітичними системами й захисту даних, водночас залишаючи простір для адаптації під конкретні умови функціонування органів прокуратури. Саме завдяки поєднанню імперативних і диспозитивних методів управлінського впливу формується збалансований режим інформаційної діяльності, у якому поєднуються вимоги законності, ефективності та доцільності.

4. Запропоноване бачення адміністративно-правового статусу суб'єктів інформаційно-правового забезпечення прокуратури, засноване на критеріях публічно-правового статусу, чітко закріплених повноваженнях, зв'язку з функціями органів прокуратури та юридичній відповідальності за результати діяльності, дозволяє уникнути розмитості суб'єктного складу в цій сфері. Розмежування між органами, структурними підрозділами, посадовими особами та техніко-інформаційними системами як елементами інфраструктури унеможливорює підміну реальних суб'єктів адміністративно-правових відносин суто технологічними компонентами. Це, у свою чергу, створює підґрунтя для належного застосування заходів відповідальності, побудови системи внутрішнього контролю та формування адресних управлінських рішень у сфері роботи з інформацією.

5. Ієрархія суб'єктів інформаційно-правового забезпечення – від Офісу Генерального прокурора та Спеціалізованої антикорупційної прокуратури до

обласних і окружних прокуратур, а також спеціалізованих ІТ, документальних та аналітичних підрозділів – створює складну, але керовану багаторівневу систему. Високий ступінь централізації забезпечує єдність стандартів, політики та технічних рішень, тоді як надання адміністративної автономії на регіональному й місцевому рівнях дозволяє враховувати специфіку конкретної територіальної юрисдикції та навантаження. Водночас цифровізація, розбудова ЄРДР, «СЕД», «ОСОП» та інших інформаційних платформ актуалізують потребу в подальшому вдосконаленні вторинного нормативного регулювання – від чіткого визначення статусу електронних доказів до стандартизації процедур доступу, зберігання й кіберзахисту. Усе це свідчить про динамічний характер адміністративно-правового механізму, який має постійно адаптуватися до технологічних і безпекових викликів.

РОЗДІЛ 3

НАПРЯМИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО- ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

3.1. Зарубіжний досвід інформаційно-правового забезпечення діяльності прокуратури країн ЄС

В умовах сучасної цифрової трансформації публічної влади виникає об'єктивна потреба у глибокому теоретико-методологічному оновленні підходів до інформаційно-правового забезпечення діяльності органів прокуратури. Особливої ваги набуває порівняльно-правове вивчення моделей європейських держав, насамперед Франції та Польщі, з орієнтацією на вироблення придатних для імплементації в українське адміністративно-правове середовище рішень.

Методологічний фундамент такого аналізу ґрунтується на поєднанні кількох взаємодоповнюваних підходів. Насамперед ідеться про чітке розмежування об'єкта і предмета: об'єктом виступає загальна система правового регулювання інформаційних процесів у діяльності прокуратури, тоді як предметом є конкретні адміністративно-правові норми, інститути та процедури, що забезпечують збирання, опрацювання, захист і використання інформації у межах прокурорської діяльності. При цьому провідним має залишатися саме адміністративно-правовий підхід, оскільки органи прокуратури функціонують як суб'єкти публічного адміністрування, а значна частина їх діяльності врегульована нормами адміністративного права.

Застосування порівняльного методу дає можливість виявити як спільні риси, так і відмінності у підходах до інформаційно-правового забезпечення, оцінити результативність відповідних адміністративних рішень, співвіднести функціональне навантаження прокуратур із практиками інформаційного обміну. Важливим є також використання нормативно-інституційного підходу, який зосереджується не лише на змісті правових приписів, а й на особливостях побудови інформаційної інфраструктури, рівні технологічної підтримки, кадрових ресурсах та механізмах взаємодії з іншими суб'єктами публічної влади.

Окремого наголосу потребує етичний і правозахисний вимір. Оскільки органи прокуратури оперують значними масивами персональних даних, завжди існують ризики посягання на права людини, насамперед на право на приватність. Тому доцільним є залучення міждисциплінарного інструментарію, який поєднує юридичний аналіз із соціологічним та інформаційно-технологічним баченням. Саме такий комплексний підхід дає змогу коректно інтерпретувати європейський досвід з урахуванням особливостей української правової системи.

Європейська модель інформаційно-правового забезпечення діяльності органів прокуратури вибудовується на поєднанні принципів публічності, підзвітності, відкритості інформації, захисту персональних даних та інституційної незалежності. Її вихідним положенням є розуміння прокуратури як органу публічної влади, що покликаний не лише забезпечувати законність, а й діяти відповідно до вимог адміністративної ефективності, прозорості та цифрової відкритості. Важливим елементом виступає розвинена інформаційна інфраструктура, яка дає змогу органам прокуратури держав – членів Європейського Союзу забезпечувати належний електронний документообіг, аналітичну обробку даних і комунікацію з судами, поліцією та іншими органами влади.

У межах такої моделі доцільно виокремити три взаємопов'язані рівні: 1) нормативний – систему загальноєвропейських актів; 2) інституційний – організацію діяльності європейських і національних прокуратур на засадах автономності та цифрової взаємодії (зокрема, діяльність Європейської прокуратури – European Public Prosecutor's Office (EPPO)) [75]; 3) організаційно-технологічний – упровадження автоматизованих інформаційних систем і механізмів обміну даними між органами публічної влади. При цьому європейська модель має системний характер, вона не обмежується технічними інформаційно-технологічними рішеннями, а інтегрує адміністративно-правові, етичні та процедурні вимоги, спрямовані на досягнення балансу між результативністю діяльності органів прокуратури та гарантіями прав людини.

Джерела європейського інформаційного права у сфері діяльності органів прокуратури. Система джерел, на яких ґрунтується інформаційно-правове забезпечення діяльності органів прокуратури в європейських державах, має багаторівневу структуру й охоплює: 1) нормативно-правові акти Європейського Союзу; 2) акти Ради Європи та практику Європейського суду з прав людини; 3) національне законодавство держав – членів ЄС; 4) внутрішньоорганізаційні акти прокуратур, що регламентують інформаційні процедури, стандарти та політики.

На рівні права Європейського Союзу базовим актом є Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних (General Data Protection Regulation – GDPR) [21]. Попри те, що він не спрямований безпосередньо на регулювання діяльності прокуратури, його норми є обов'язковими для всіх публічних інституцій, які обробляють персональні дані, у тому числі в сфері правосуддя. Особливе значення мають приписи статті 5 GDPR щодо принципів обробки даних: законності, прозорості, визначеності цілей, мінімізації та обмеження строків зберігання.

Для органів, що здійснюють правоохоронні функції, зокрема прокуратури, діє спеціальна Директива (ЄС) 2016/680 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування злочинів [41]. Вона безпосередньо стосується діяльності прокуратур, встановлюючи додаткові гарантії прав суб'єктів даних (право на інформацію, обмеження доступу до даних) і вимоги до зберігання, точності та безпеки інформації.

У площині наднаціональної співпраці важливим джерелом є Регламент (ЄС) 2017/1939 від 12 жовтня 2017 року про впровадження тіснішої співпраці щодо створення Європейської прокуратури (European Public Prosecutor's Office – EPPO) [76]. Створений на його основі орган, уповноважений розслідувати злочини проти фінансових інтересів ЄС, діє за загальними принципами права ЄС

та функціонує із використанням розгалужених інформаційних систем обліку, звітності й обміну доказами між прокурорами держав-членів.

На рівні актів Ради Європи та практики Європейського суду з прав людини джерелами інформаційно-правового забезпечення є, зокрема: 1) Рекомендація Rec (2000)19 Комітету міністрів Ради Європи державам-членам щодо ролі прокуратури в системі кримінального правосуддя [77], де підкреслюється необхідність дотримання принципів прозорості, відповідальності та відкритості, у тому числі в інформаційному вимірі; 2) Конвенція Ради Європи №108+ про захист осіб у зв'язку з автоматизованою обробкою персональних даних [78], що створює правову основу взаємного визнання права на захист персональних даних у транскордонному обміні, включно з правоохоронною діяльністю. 3) Європейська Етична Хартія про використання штучного інтелекту в судових системах та їх середовищі (European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment), прийнята 03.12.2018 Європейською комісією з ефективності правосуддя Ради Європи (CEPEJ – European Commission for the Efficiency of Justice, Європейська комісія з питань ефективності правосуддя) [67], яка містить зведення принципів, якими мають керуватися політики, законодавці та фахівці в галузі правосуддя, коли їм доводиться стикатися зі швидким розвитком штучного інтелекту в національних судових процесах, зокрема: принцип поваги основних прав, недискримінації, якості та безпеки, прозорості, неупередженості та справедливості, «під контролем користувача».

Практика ЄСПЛ у справах щодо доступу до інформації, права на повагу до приватного життя (ст. 8 Конвенції) та права на ефективний засіб юридичного захисту (ст. 13) доповнює цю систему, формуючи стандарти прозорості й допустимого втручання прокуратури в інформаційну сферу [39]. Так, у справі «M.M. v. the United Kingdom» (2012) Суд визнав, що зберігання інформації про особу в базах даних, пов'язаних з діяльністю прокуратури, може становити втручання в право на приватність за відсутності належного правового регулювання [79].

Отже, джерельна база європейського інформаційного права у сфері діяльності органів прокуратури має багаторівневий характер - від актів ЄС до національного законодавства й рекомендацій Ради Європи, що забезпечує уніфікацію правових стандартів та посилює довіру до прокуратури як суб'єкта публічної влади.

Що стосується досвіду Франції, насамперед слід підкреслити, що у системі прокуратури немає єдиного «загального прокурора». Її вершину становить Procureur général près la Cour de cassation (Генеральний прокурор при Касаційному суді), який очолює прокуратуру при Cour de cassation – найвищій судовій інстанції Франції [80]. На рівні апеляційних судів діють Procureur général при кожній cour d'appel, які керують ministère public (органами публічного обвинувачення) у межах відповідного апеляційного округу [81], (ministère public, або parquet) побудована за чіткою ієрархією, що повторює судову систему: місцевий рівень – апеляційний – касаційний. На кожному рівні функціонує орган публічного обвинувачення зі своїм керівником, а розмежування компетенції та внутрішня «субституція» (взаємозамінність прокурорів) прямо закріплені у законодавстві. Це забезпечує безперервність підтримання обвинувачення, єдність застосування права та стандартизовані інформаційні процедури.

У судах першої інстанції (tribunal judiciaire) публічне обвинувачення здійснює прокурор Республіки (procureur de la République). Він особисто або через субститута представляє ministère public у справах, що належать до юрисдикції суду, та керує процесуальними діями поліції у своєму окрузі. На цьому рівні концентруються прийняття скарг, рішення про початок чи відмову від переслідування, застосування альтернатив та підтримання обвинувачення в суді. Стаття L122-2 Code de l'organisation judiciaire (Кодекс судочинства) прямо закріплює: «Le ministère public est exercé... par le procureur de la République», а розділ «Des attributions du procureur de la République» КПП деталізує його повноваження.

На апеляційному рівні над місцевими прокуратурами стоїть *procureur général* при апеляційному суді, який очолює *parquet général* та координує діяльність усіх підпорядкованих прокурорів республіки. Він забезпечує єдність кримінальної політики й практики застосування закону в окрузі, у тому числі й у сфері інформаційних потоків (звітність, статистика, методичні вказівки). Нормативну основу цього рівня також закріплено у розділі L122 *Code de l'organisation judiciaire* (Кодекс судочинства) [82].

На касаційному рівні (*parquet général près la Cour de cassation*) функціонує прокурор Касаційного суду. На відміну від місцевих та апеляційних прокуратур, він не здійснює публічного переслідування в класичному розумінні й не побудований за жорсткою дисциплінарно-ієрархічною моделлю. Його головне завдання – сприяти єдності тлумачення права та належному функціонуванню найвищої судової інстанції. Це підкреслено на сайті *Cour de cassation*: «*Le parquet général de la Cour de cassation se distingue... en ce qu'il n'est pas hiérarchisé, ni en charge de l'action publique*» [80].

Важливою рисою внутрішньої організації французької прокуратури є принцип взаємозамінності будь-який магістрат одного *parquet* може здійснювати функції публічного обвинувачення в його межах. Згідно зі ст. L122-4 *Code de l'organisation judiciaire* (Кодекс судочинства) «*Tout magistrat d'un parquet... peut exercer les fonctions du ministère public au sein de ce parquet*» (Будь-який магістрат прокуратури... може виконувати функції державного обвинувача в цій прокуратурі). На практиці це означає, що у разі вибуття конкретного прокурора інший безперешкодно підміняє його у справі, а функція *ministère public* залишається безперервною. В інформаційному вимірі це підтримується тим, що документообіг, реєстрація рішень, облік та статистика не «прив'язані» до однієї особи й можуть безпечно делегуватися в межах офісу [82].

Доброю ілюстрацією структури великої прокуратури є Паризька прокуратура. Офіційний ресурс *Tribunal de Paris* вказує, що офіс складається з кабінету прокурора, 6 дивізій, 16 секцій та окремого підрозділу з альтернатив переслідуванню. Це демонструє високий рівень функціональної спеціалізації та

організацію внутрішніх інформаційних каналів (керуваність потоків, стандартизовані шаблони, єдині регламенти) [83].

У французькій публічній доктрині (портал *vie-publique*) прокуратура визначається як «сукупність магістратів міністерства публічного обвинувачення, відповідальних за застосування закону від імені суспільного інтересу», які «перебувають під владою міністра юстиції» з адміністративного боку [84]. Поєднання процесуальної ролі в системі правосуддя та адміністративної залежності (через кадрову політику, ресурси, ІТ-системи) формує «подвійну природу» прокуратури, що має ключове значення для розуміння її організації й інформаційного адміністрування.

Що стосується досвіду Франції у сфері інформаційно-правового забезпечення діяльності органів прокуратури, він демонструє тісну взаємодію адміністративно-правового регулювання, технологічної інфраструктури та принципів публічного управління. У французькому контексті прокуратура (*procureur de la République* та інші публічні прокурори) виступає не лише кримінально-правовим суб'єктом, а й публічним адміністративним органом, що здійснює функції суспільного контролю, координації правоохоронної діяльності, моніторингу та інформаційної взаємодії.

У наукових і публіцистичних оглядах, зокрема в циклі матеріалів «*L'e-Administration avance*», підкреслюється, що французька прокуратура розвивається як елемент ширшої «цифрової держави», де електронні системи правосуддя інтегруються в загальну політику е-урядування та визначають реальний зміст її інформаційної компетенції [85].

Функцію публічного обвинувачення у Франції виконує прокуратура, визначена в Кримінально-процесуальному кодексі (*Code de procédure pénale*). У розділі про *procureur de la République* закріплено його повноваження та організаційні засади діяльності, включно з інформаційними функціями, звітністю й координацією з іншими органами [86].

З погляду інформаційно-правового забезпечення ключовим є положення ст. 230-8 Кодексу кримінального провадження, яке регламентує обробку

персональних даних під наглядом прокурора: «The processing of personal data is carried out under the supervision of the public prosecutor with territorial jurisdiction ... the public prosecutor will decide within two months on the appropriate action ...» (Обробка персональних даних здійснюється під наглядом державного прокурора з територіальною юрисдикцією... державний прокурор протягом двох місяців приймає рішення про відповідні дії...) [87]. Прокурор здійснює правове керівництво такими обробками і може вимагати видалення, доповнення чи виправлення даних, що особливо актуально після завершення або закриття справи. Це свідчить про вбудованість прокуратури в інформаційно-правове поле, де робота з даними є елементом її адміністративного статусу.

Важливу роль відіграє й технологічна інфраструктура, створена для інформаційного забезпечення прокурорської діяльності. Одна з центральних систем – CASSIOPEE (Chaine Applicative Supportant le Système d'Information Orienté Procédure pénale Et Enfants), призначена для реєстрації скарг, заяв, процесуальних дій і ведення кримінальних проваджень у єдиному інформаційному контурі [88].

Функціонування CASSIOPEE передбачене статтями 48-1 и R15-33-66-4 Кримінального-процесуального кодексу. Міністерство Юстиції Франції несе відповідальність за роботу Cassiopée, при цьому право внесення виправлень та доповнень інформації, зазначеної у програмному комплексі, належить прокурору. Інформація в Cassiopée зберігається від 10 до 30 років в залежності від вчиненого правопорушення та строків давності притягнення до відповідальності, передбачених ст. 706-25-1 и 706-31 Кримінального-процесуального кодексу. Для роботи в CASSIOPEE, окрім прокурорів та слідчих мають право зареєструватись мирові судді, секретарі та уповноважені особи судових інстанцій [89].

ЗМІ та аналітичні огляди відзначають, що Cassiopée охоплює дані про заяви, клопотання, рішення, документи, забезпечує зберігання, архівування й підвищує ефективність обробки кримінальних справ та швидкість обміну інформацією між прокуратурою, судами та іншими учасниками кримінального судочинства [90].

Автоматизація поєднується з правовими гарантіями захисту даних і контролю за їх обробкою відповідно до ст. 230-8, що демонструє синергію технологій, права та адміністративної практики.

За даними офіційних джерел, Cassiopée поетапно впроваджувалася в судах та підрозділах прокуратури починаючи з 2008 року як єдина платформа, покликана замінити різноманітні локальні програми й паперовий документообіг. До 2013 року програмне забезпечення Cassiopée було впроваджено в усіх державних прокуратурах, кримінальних судах та судах у справах неповнолітніх, проте, це впровадження не було завершено для апеляційних судів та судів присяжних.

Її функціонал охоплює повний життєвий цикл кримінального провадження – від первинної реєстрації заяви в поліції до винесення вироку – із фіксацією всіх процесуальних подій, автоматизованим формуванням процесуальних документів, інтеграцією з реєстрами осіб та можливістю формувати статистичні вибірки для потреб кримінальної політики.

Водночас у професійній пресі та публічних оглядах (зокрема в рамках серії «L'e-Administration avance») наголошується, що Cassiopée стала не лише символом цифровізації, а й джерелом низки проблем: тривале неперенесення інформації з застарілих програмних комплексів до Cassiopée про результати судового розгляду в Апеляційних судах, значне ускладнення інтерфейсу для користувачів, часті технічні збої, підвищене навантаження на прокурорських та судових клерків, суттєве зростання вартості проєкту (від 45 мільйонів євро на етапі планування до понад ста мільйонів євро за даними Рахункової палати). Саме тому Cassiopée у французькому дискурсі часто описується як «необхідний, але проблемний» інструмент, що вимагає постійної оптимізації, доопрацювання модулів та інвестицій у навчання користувачів.

Мова йде про широку реформу «justice numérique» (цифрове правосуддя) у складі загальноурядового курсу «e-administration», впроваджену Міністерством юстиції у вигляді Планів цифрової трансформації на 2017-2022, 2023-2027 роки, затверджених законами, що включає дематеріалізацію кримінального процесу

(ноль паперу до 2027, Le projet “Zero papier 2027”), уніфікацію довідників і форматів даних, покращення мережі, створення модульної та розрізної інформаційної системи, а також міжфункціональних сховищ даних, запровадження електронного обміну процесуальними документами та відкритих статистичних показників; Cassiopée є ядром саме «кримінальної» гілки цієї реформи. План цифрової трансформації спрямований на ретельне оновлення технічної бази, яке включає, зокрема, перенесення всіх додатків міністерства в хмару, поступову ліквідацію локальних серверів та масове збільшення швидкості завдяки підключенню до Державної міжвідомчої мережі усіх сайтів міністерства. Для успішного втілення вказаної масштабної реформи створено Стратегічний комітет цифрової трансформації (Comité stratégique de la transformation numérique - CSTN) [91].

Зміст реформи Франції простими словами можна визначити: 1) стандартизація даних та процесів у всіх ланках (поліція – прокуратура – суд – пенітенціарна система); 2) «одне вікно» для реєстрації й супроводу справ; 3) наскрізне журналювання доступів і дій; 4) автоматичне формування процесуальних документів і статистики; 5) інтеграція з суміжними сервісами (е-подання, кабінети учасників процесу, відкриті дані судових рішень).

У згаданих матеріалах «L’e-Administration avance» цифрове середовище французького правосуддя розглядається не лише через призму Cassiopée, а й у зв’язку з іншими електронними системами – платформами електронного обміну між судами та адвокатами, сервісами подання заяв і скарг онлайн, порталами доступу громадян до інформації про хід проваджень. Підкреслюється, що ці інструменти створюють «цифровий ланцюг» правосуддя, в якому прокуратура виступає одним із ключових вузлів: вона отримує, опрацьовує й передає дані в електронній формі, а якість її інформаційної роботи безпосередньо впливає на швидкість і прозорість усього кримінального процесу. Водночас автори звертають увагу на типові виклики е-адміністрування: фрагментарність IT-рішень, необхідність уніфікації форматів даних, ризики перевантаження

кінцевих користувачів складними інтерфейсами та потребу в системній політиці навчання й підтримки персоналу.

Значення цієї реформи для України полягає в низці практичних уроків і організаційно-правових орієнтирів. По-перше, це уроки інтеоперабельності - перед запуском необхідно запровадити уніфіковані класифікатори, стандартизовані формати обміну даними (XML/JSON), правила версійності та чітко визначені API-шлюзи для повної інтеграції зв'язки «прокуратура – поліція/ДБР/БЕБ/НАБУ – суд». По-друге, це керовані міграції - перехід від розрізнених відомчих баз до єдиної платформи слід здійснювати поетапно, через пілотні впровадження, використання еталонних наборів даних та проведення незалежного аудиту якості міграції на кожному кроці. По-третє, це повне управління вартістю володіння і змінами - потрібно завчасно планувати весь життєвий цикл витрат (обладнання, ліцензії, навчання персоналу, технічна підтримка), встановлювати обов'язкові KPI - Key Performance Indicator(s) (ключовий(-і) показник(-и) ефективності) та Service-Level-Agreements і резервувати бюджет на безперервні оновлення систем. По-четверте, це забезпечення доказової цілісності - від початку слід закласти правові й технічні вимоги до наскрізного журналювання дій, фіксації хеш-сум, часових міток і ролей користувачів, аби електронні сліди були допустимими та переконливими доказами. По-п'яте, це повне підключення всіх інстанцій - необхідно запобігти «вузьким горлечкам» на рівні апеляційних і спеціалізованих судів та прокуратур, забезпечивши або синхронний запуск, або чіткий обов'язковий графік підключення з проміжними інтеграційними рішеннями.

Франція також послідовно розвиває прозорість і відкритість прокурорської та судової діяльності. Через портал Міністерства юстиції реалізовано проєкт «Open data of court decisions» – публікацію судових рішень у цифровому форматі з анонімізованими даними, що забезпечує широкий доступ до результатів правосуддя [92]. Судові рішення у справах, пов'язаних із кримінальним переслідуванням, стають доступними онлайн із дотриманням вимог захисту персональних даних, що підсилює підзвітність системи кримінального

правосуддя, у тому числі прокуратури. У поєднанні з електронними системами управління справами це означає, що значна частина інформаційного циклу – від введення даних у Cassiopée до публікації анонімізованих рішень – здійснюється в цифровому середовищі, де кожен етап спирається на чітко визначені правові режими доступу, обробки й оприлюднення інформації.

У системі інформаційно-правового забезпечення діяльності органів прокуратури Франції визначальним є баланс між захистом прав людини (насамперед права на приватність) і потребами правосуддя. Закон № 78-17 від 6 січня 1978 р. («Law relating to data processing, files and civil liberties») (Закон щодо обробки даних, файлів та громадянських свобод) та запроваджений ним санкційний режим щодо неправомірної обробки персональних даних сформували основу правової відповідальності за порушення у цій сфері [93]. У поєднанні з положеннями ст. 230-8 КПП це створює рамки, в яких прокурор не лише контролює автоматизовану обробку даних, а й несе юридичну відповідальність за порушення права на приватність, що структурує внутрішню інформаційну політику прокуратури.

Отже, цифрові інструменти французької прокуратури функціонують не ізольовано, а в режимі жорсткого нормативного «обрамлення»: запуск нових ІТ-систем супроводжується оцінкою впливу на приватність, погодженням із національним органом з питань захисту даних (CNIL), визначенням строків зберігання, категорій доступу та процедур виправлення інформації [94].

Звіти Міністерства юстиції Франції («Key Figures of Justice, 2023 Edition») засвідчують, що прокуратура щороку отримує аналітичні зведення щодо кримінальної політики та статистики проваджень, що відображає становлення інформаційної політики як сталого елементу її діяльності [95].

Отже, французький досвід має кілька рис, важливих для порівняльного аналізу: по-перше, інтеграцію технологій (автоматизованих систем) із правовим регулюванням, коли ІТ-рішення функціонують у чітко визначеному нормативному полі; по-друге, однозначне закріплення повноважень прокурора в обробці даних (зокрема ст. 230-8 КПП), що підкреслює його роль як

адміністративного органу з інформаційною відповідальністю; по-третє, наявність інструментів відкритості та підзвітності (open data, статистичні звіти), які відповідають принципам публічного адміністрування й сучасного інформаційного права; по-четверте, орієнтацію на баланс між правами особи та публічною безпекою як ключовий елемент інформаційно-правового забезпечення прокуратури.

Додатково важливим для України є те, що французький кейс демонструє не лише переваги, а й «вартість помилки» в е-адмініструванні: складні, дорого втілені системи на кшталт Cassiopée потребують одночасно якісної нормативної бази, продуманої архітектури даних і реалістичної оцінки навантаження на персонал, інакше цифровізація ризикує перетворитися на фактор додаткової бюрократизації процесів.

Для України використання французького досвіду може означати формування такого правового режиму, за якого прокуратура отримує чітко окреслені інформаційні функції, повноваження й обов'язок контролювати обробку даних, діяти в умовах електронних систем та бути підзвітною через публічні дані. Водночас необхідно враховувати національні особливості – історію інституту прокуратури, рівень цифрової трансформації, юридичний статус органів прокуратури. Управління IT-інфраструктурою прокурорських органів має спиратися на чітке нормативне регулювання, подібно до французької моделі.

У свою чергу, польська прокуратура функціонує як публічна служба, організована в ієрархічну систему органів, що здійснюють кримінальне переслідування, охороняють законність і публічний інтерес. Її сучасну модель визначає Закон від 28 січня 2016 р. «Prawo o prokuraturze» (Dz.U. poz. 177) (Закон про прокуратуру), який кодифікує структуру, компетенції та підпорядкованість органів прокуратури й став нормативною основою реформи 2016 р., що істотно змінила інституційний дизайн та механізми управління всередині системи [96].

У ст. 16 цього Закону закріплено чотирирівневу систему загальних (публічних) організаційних одиниць прокуратури: Prokuratura Krajowa

(Національна прокуратура), прокуратури регіональні, окружні та районні. У розділі про органи та структуру прямо вказано, що саме ці одиниці становлять мережу поширених органів прокуратури, що забезпечує чітку управлінську вертикаль і територіальну компетенцію на всій території держави. На вершині системи перебуває Prokurator Generalny, поруч із яким Закон 2016 р. передбачає посади Prokurator Krajowy, інших заступників та корпус прокурорів загальних підрозділів, що вибудовує одночасно і управлінську, і процесуально-наглядову ієрархію.

Офіційний портал Prokuratura Krajowa (Національна прокуратура) демонструє фактичну географію мережі: підтверджено функціонування 11 регіональних прокуратур (Білосток, Гданськ, Катовіце, Краків, Люблін, Лодзь, Познань, Жешув, Щецин, Варшава, Вроцлав) із окремими сторінками та реквізитами, що наочно підтверджує реальність цього рівня в структурі [97]. Ієрархія будується не лише територіально, а й функціонально-процесуально: нормативно визначено, яка одиниця є «вищого рівня» щодо іншої (для районних – окружна, регіональна і Крайова; для окружних – регіональна і Крайова; для регіональних – Крайова), що забезпечує тяглість нагляду, узгодженість кримінальної політики й уніфікацію внутрішніх стандартів роботи [98].

У внутрішній структурі Prokuratura Krajowa виокремлено спеціалізовані департаменти та бюро (з питань досудового провадження, судового провадження, боротьби з організованою злочинністю і корупцією, кіберзлочинності та інформатизації, конституційних та військових справ тощо), що свідчить про високий рівень функціональної диференціації та дає змогу формувати методичні підходи й координацію для нижчих ланок системи [99]. Типову матрицю компетенцій і підпорядкування демонструють також сайти окружних та регіональних прокуратур: наприклад, Prokuratura Okręgowa w Nowym Sączu (Окружна прокуратура м. Новий Сонч) вказує на підпорядкування Краківській регіональній прокуратурі та Prokuratura Krajowa, що має значення як для процесуального контролю, так і для управління персоналом та інформаційними потоками [100].

Ключовою новацією реформи 2016 р. стало поєднання посад Міністра юстиції та Генерального прокурора. Венеційська комісія у Висновку щодо Закону про прокуратуру CDL-AD(2017)028 підкреслила, що суть змін полягала у «поверненні» до моделі, за якої Генеральний прокурор одночасно є діючим Міністром юстиції, що викликало занепокоєння з огляду на стандарти деполітизації та інституційної незалежності прокуратури, оскільки концентрація повноважень в руках члена уряду може впливати на автономію прокурорського корпусу [101].

Водночас у 2024 р. Венеційська комісія, оцінюючи проєкт подальших поправок, прямо вказала, що їх головною метою є роз'єднання ролей Міністра юстиції та Генерального прокурора, що відповідає рекомендаціям 2017 р. щодо деполітизації прокуратури. Попри те, що проєкт ще перебуває у процесі доопрацювання, сам факт такої офіційної оцінки свідчить про рух у бік інституційного відокремлення та балансування ієрархії управління. Водночас Комісія наголошує на необхідності подальшого посилення гарантій незалежності прокуратури, зокрема у частині процедур призначення та звільнення [102].

Що стосується інформаційно-правового забезпечення діяльності органів прокуратури Польщі, його нормативне підґрунтя насамперед формує Закон «Prawo o prokuraturze» (Закон про прокуратуру) 2016 р., який виступає базовою «опорною нормою», на якій вибудовується інфраструктура обробки, обміну та відкритості даних у прокурорській діяльності. Паралельно діють загальні акти публічної адміністрації, зокрема Закон від 6 вересня 2001 р. «Про доступ до публічної інформації», що гарантує кожному право на доступ до публічної інформації та встановлює строки її надання (як правило, до 14 днів), у тому числі й щодо органів прокуратури як суб'єктів публічної влади [103]. Стаття 8 закону покладає обов'язок оприлюднення інформації через «Biuletynem Informacji Publicznej - VIP» (Бюлетень публічної інформації) – єдину телекомунікаційну систему сторінок публічних інституцій.

У практиці це означає, що кожна ланка прокурорської системи (Prokuratura Krajowa, регіональні, окружні та районні прокуратури) має власну сторінку в «Biuletynem Informacji Publicznej - BIP» (Бюлетень публічної інформації), де в стандартизованих розділах розміщуються: структура органу, перелік підрозділів, контактні дані, описи реєстрів, що ведуться, зразки форм звернень, умови прийому громадян, оголошення про конкурси на посади, а також щорічні звіти про діяльність [104]. Доступ до цих даних є відкритим, а оновлення інформації контролюється як внутрішніми правилами, так і наглядом з боку органів, відповідальних за дотримання закону «Про доступ до публічної інформації». Таким чином «Biuletynem Informacji Publicznej - BIP» (Бюлетень публічної інформації) виступає «публічним вікном» прокуратури, через яке реалізуються як обов'язок прозорості, так і базові інформаційні права громадян.

Окрім цього, Польща застосовує Закон від 10 травня 2018 р. «Про захист персональних даних» [105] та спеціальний Закон від 14 грудня 2018 р. щодо обробки персональних даних у зв'язку із запобіганням і протидією злочинності [106]. Кримінально-процесуальний вимір інформаційних повноважень закріплено в Кодексі кримінального процесу (КПК), який підтверджує керівну роль прокурора в досудовому розслідуванні (зокрема можливість доручати його проведення поліції), що обумовлює інтенсивний інформаційний обмін між прокуратурою й органами розслідування та формування відповідних документопотоків і реєстрів рішень [107, с. 333].

На рівні організації роботи це проявляється в тому, що прокурор виступає ключовим вузлом інформаційних потоків у кримінальному провадженні. Поліція та інші органи досудового розслідування зобов'язані передавати йому матеріали в електронній або змішаній формі. Прокурор, у свою чергу, ініціює внесення змін до електронних реєстрів, погоджує або відхиляє слідчі дії, формує обвинувальні акти, які надалі потрапляють до судових ІТ-систем. Усі ці операції супроводжуються фіксацією в інформаційних системах Міністерства юстиції та пов'язаних реєстрах, що забезпечує простежуваність рішень і контроль за дотриманням процесуальних строків.

Разом із організаційною вертикаллю, практику інформаційно-правового забезпечення прокуратури Республіки Польща формують низка державних електронних реєстрів та сервісів, які забезпечують доступ, верифікацію та обмін даними, зокрема:

1. Krajowy Rejestr Karny (KRK) та електронний сервіс e-KRK – базовий довідковий реєстр відомостей про судимість де електронні довідки доступні через портал Міністерства юстиції e-KRK (офіційний вхід: ekrk.ms.gov.pl). Цей інструмент використовується для перевірок у кримінальних провадженнях і кадрових процедурах, у т.ч. прокуратурою [108].

2. Krajowy Rejestr Sądowy (KRS / e-KRS) – Національний судовий реєстр юридичних осіб, фондів та підприємців, корисний для ідентифікації контрагентів, бенефіціарів і зв'язків у справах про економічні злочини; діє електронний модуль e-KRS [109]. 3. Krajowy Rejestr Zadłużonych (KRZ) – Національний реєстр боржників (неплатоспроможність, реструктуризація, банкрутство), що забезпечує офіційну публічність проваджень і використовується для верифікації процесуального статусу учасників у справах економічного спрямування [110].

4. Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG) – реєстр фізичних осіб-підприємців; дозволяє підтвердити реєстраційні дані, види діяльності (PKD) та історію змін [111].

5. PESEL (Powszechny Elektroniczny System Ewidencji Ludności) – базовий демографічний реєстр, доступ до якого регламентовано; для громадян доступні електронні довідки про власні дані, для органів – міжвідомчий обмін [112].

6. Rejestr sprawców przestępstw na tle seksualnym – спеціальний реєстр з обмеженим доступом (розширена частина лише для уповноважених органів, зокрема прокуратури та поліції); відкритий сегмент доступний громадянам [113].

7. Portal Informacyjny Sądów Powszechnych – електронний кабінет для доступу до матеріалів справ, графіків засідань і стану провадження; використовується сторонами, захисниками та іншими уповноваженими особами, що полегшує інформаційну взаємодію з судами [114].

8. VIP (Biuletyn Informacji Publicznej) органів прокуратури – обов’язкові сторінки публічної інформації (організація, компетенції, оголошення, статистика тощо), через які забезпечується прозорість і пасивний доступ [104].

9. ePUAP – національна платформа електронних послуг публічної адміністрації, що надає канали подання електронних звернень/документів та автентифікацію користувачів; застосовується і у взаємодії з юстицією [115].

Сукупно ці реєстри та платформи забезпечують: 1) стандартизовані джерела перевірених даних (KRK/e-KRK, KRS/e-KRS, KRZ, CEIDG); 2) демографічну ідентифікацію учасників (PESEL); 3) доступ до процесуальної інформації та документів (Портал Інформаційний судів); 4) офіційну публічність та прозорість (VIP); 5) уніфіковані канали електронної комунікації (ePUAP). Це формує передумови для належного інформаційно-правового режиму діяльності органів прокуратури, сумісного з вимогами захисту персональних даних і відкритості публічної інформації.

Ключовою інституцією довідково-правового забезпечення є (Krajowy Rejestr Karny – KRK), створений Законом від 24 травня 2000 р. Він визначає категорії відомостей, що накопичуються (дані про засуджених, умовне припинення, види покарань тощо) та порядок надання інформації уповноваженим органам, у тому числі прокуратурі [116]. Офіційний портал KRK та електронна платформа e-KRK Міністерства юстиції дають змогу органам влади й громадянам подавати запити та отримувати довідки в цифровій формі, забезпечуючи єдині правила перевірки судимостей і процесуального статусу у взаємодії прокуратури, судів, поліції та інших органів [117].

Функціонування e-KRK Міністерства юстиції на практиці можна описати як багаторівневу систему електронного доступу. По-перше, органи прокуратури мають спеціальний, розширений доступ до реєстру через захищені телекомунікаційні канали. Уповноважені працівники (прокурори або визначені клерки) можуть у режимі реального часу отримувати інформацію про судимість підозрюваних, обвинувачених чи свідків, а також про застосовані до них покарання й обмеження. Запит формується в електронній формі, підписується

кваліфікованим електронним підписом і автоматично логінується в системі. Відповідь KRK повертається у вигляді структурованого електронного документа, який може бути приєднаний до матеріалів провадження.

По-друге, суди, органи місцевого самоврядування, ліцензійні органи та інші суб'єкти публічної адміністрації використовують е-KRK для перевірки осіб у зв'язку з призначенням на посади, отриманням дозволів, участю в публічних закупівлях тощо. Для прокуратури це створює єдиний інформаційний простір, в якому одна й та сама інформація про судимість доступна всім уповноваженим органам за однаковими правилами, що зменшує ризик суперечностей та дублювання даних.

По-третє, громадяни й підприємства можуть звертатися до KRK за довідками про відсутність судимості через електронну форму е-KRK або особисто. Ці довідки, у свою чергу, використовуються в провадженнях, що розглядаються прокурором, як офіційне підтвердження статусу особи. Таким чином KRK поєднує внутрішньо-відомчий та «зовнішній» вимір, забезпечуючи як оперативну роботу прокуратури, так і реалізацію прав зацікавлених осіб.

Польське інформаційне право передбачає також проактивне оприлюднення на сторінках VIP відомостей про структуру, компетенцію, керівництво, реєстри та процедури набору, що прямо впливає зі ст. 8 закону «Про доступ до публічної інформації», та приписів щодо переліку інформації, обов'язкової для розміщення. Паралельно забезпечується й «пасивний» доступ – через розгляд індивідуальних запитів у встановлені строки з можливістю їх продовження за визначеною процедурою. Для адміністративної практики прокуратури це означає налагоджені канали прийому запитів, стандартизовані форми й постійну взаємодію з реєстрами.

Якщо узагальнити механіку системи, то типовий інформаційний цикл у взаємодії громадянина з прокуратурою Польщі виглядає так: 1) громадянин або організація знаходить на сторінці VIP відповідної прокуратури зразок заяви чи електронної форми й подає звернення (наприклад, про доступ до публічної інформації або скаргу на дії органів правопорядку); 2) звернення реєструється в

електронній системі діловодства прокуратури, йому присвоюється унікальний номер, фіксуються строки розгляду; 3) у разі потреби прокурор або уповноважений працівник звертається до КРК та е-КРК чи інших реєстрів для перевірки даних; 4) відповідь формується в установленій законом формі та, за наявності такої можливості, надсилається заявнику в електронному вигляді; інформація про виконання запиту фіксується в інформаційній системі. Таким чином, закон «Про доступ до публічної інформації», і «Biuletynem Informacji Publicznej - BIP» (Бюлетень публічної інформації) задають загальні правила відкритості й форми комунікації, тоді як КРК та інші реєстри забезпечують змістовне наповнення цієї взаємодії даними, які прокуратура отримує й використовує в межах своєї компетенції.

Важливим елементом є включеність прокуратури Польщі в екосистему правосуддя ЄС. У 2024 р. Європейська комісія підтвердила приєднання Польщі до Європейської прокуратури (EPPO), а Міністерство юстиції оголосило про створення офісів європейських прокурорів у Варшаві та Катовіце [118]. Це означає появу нових каналів транскордонного обміну даними, уніфікованих вимог до збирання доказів і координації з європейською колегією прокурорів у межах Регламенту 2017/1939. Якщо раніше Польща залишалася поза EPPO (що відображалось у джерелах 2021–2023 рр.), то з 2024 р. вона долучилася до посиленого співробітництва, надавши процедурам взаємної правової допомоги новий інституційний контекст [76].

Інформаційно-правовий аспект участі в EPPO полягає в тому, що польська прокуратура має забезпечити сумісність своїх інформаційних систем із каналами обміну даними Європейської прокуратури, уніфікацію форматів звітності, а також дотримання європейських стандартів захисту персональних даних у транскордонних провадженнях (зокрема у справах про шахрайство з коштами ЄС, транскордонні ПВК тощо). Це ще більше підсилює роль внутрішніх реєстрів та електронних систем Польщі як джерел достовірних, структурованих даних для європейських партнерів.

Отже, аналіз польського досвіду дає підстави стверджувати, що поєднання ієрархічної структури (Prokuratura Krajowa → регіональні → окружні → районні), уніфікованих реєстрів (K RK/e-KRK) та загальних правил відкритості (UDiP/ViP) забезпечує прокуратурі інструменти для: а) стандартизації записів та форм документів; б) функціонування єдиних каналів отримання довідок (цифрові запити, міжвідомчі інтерфейси); в) контролю строків і повноти відповідей на публічні запити; г) здійснення аудиту законності обробки персональних даних. Іншими словами, система працює як цілісний інформаційно-правовий механізм. Нормативні акти задають правила гри, електронні платформи ViP та e-KRK забезпечують технічну реалізацію цих правил, а прокуратура, перебуваючи в центрі цих потоків, одночасно є і користувачем, і виробником даних, і суб'єктом відповідальності за їх належне оброблення.

У підсумковому порівняльному вимірі можна говорити про дві працездатні, але концептуально різні моделі інформаційно-правового забезпечення діяльності органів прокуратури. Франція сформувала процесно-орієнтовну систему, у якій цифрове «ядро» поєднує всі ланки кримінальної юстиції – від фіксації події до виконання вироку – та одночасно генерує уніфіковану статистику. Польща ж використовує реєстрово-сервісний підхід: довідково-верифікаційні інструменти та режим доступу до публічної інформації створюють стабільні й передбачувані канали даних для прокуратури й суспільства.

Організаційні вертикалі функціонують також по-різному. У Франції ієрархія органів прокуратури органічно пов'язана з єдиною судовою IT-інфраструктурою та класифікаторами, що забезпечує методичну уніфікацію обліку й аналітики. У Польщі центральний рівень координує нижчі прокуратури через стандартизовані реєстри, механізми відкритості ViP та регламентовані процедури розгляду запитів, коли керованість досягається не за рахунок єдиної платформи, а через формалізовані потоки «запит – відповідь».

У сфері прозорості простежуються різні акценти. Франція робить наголос на публікації судових рішень і детальному регулюванні їх обробки (анонімізація,

запобігання профайлінгу), фактично перетворюючи результати правосуддя на відкритий аналітичний ресурс. Польща підкреслює універсальне право на інформацію та обов'язковість VIP-сторінок – від відомостей про структуру й керівництво до статистики та документів за запитами. Обидві моделі орієнтовані на зміцнення довіри, але потребують різних комплаєнс-налаштувань.

У блоці захисту даних обидві системи прагнуть зберегти баланс між ефективним переслідуванням і повагою до приватності. У Франції органи контролю вбудовані в судову цифрову екосистему, у Польщі – охоплюють як правоохоронні обробки, так і ширший адміністративний обіг даних. Додатковий європейський вимір – участь Польщі в Європейській прокуратурі та стандарти Ради Європи – стимулює зближення підходів щодо класифікаторів, трасованості доступів і кібербезпеки.

Сильні сторони кожної моделі досить очевидні: французька наскрізна платформа зменшує транзакційні витрати й підвищує якість статистичних даних, тоді як польські реєстрові сервіси та правила відкритості забезпечують швидкий, прогнозований сервіс і сталі механізми підзвітності.

Додатково для Франції фіксуються типові технічні й організаційні ризики, пов'язані з експлуатацією Cassiopée та суміжних судово-прокурорських систем: використання застарілих серверних рішень і фрагментованої інфраструктури, що призводить до перевантажень, повільної роботи та ускладнює впровадження оновлень; складні й тривалі процеси перенесення даних із попередніх реєстрів, які спричиняють дублювання записів, неповноту або помилки в масивах справ; неповну функціональну інтеграцію всіх ланок судової системи, зокрема затримки з повноцінним підключенням окремих апеляційних і спеціалізованих судів, що зумовлює «розриви» у цифровому ланцюгу провадження та змушує частину процедур виконуватися поза єдиною платформою.

Узагальнюючи, можна стверджувати, що результативність обох підходів тримається на чотирьох ключових опорах: 1) чіткій правовій підставі кожної обробки; 2) технічній сумісності (класифікатори, формати, API); 3) організаційній підзвітності (стандарти звітності, VIP/open data); 4) дієвому

зовнішньому нагляді за дотриманням приватності. Для законодавця й органів прокуратури це означає потребу поєднати належну нормативну базу, уніфіковану «мову даних», сервісні канали з можливістю трасування доступів і незалежний контроль, перетворюючи цифрові інструменти на реальний інституційний ресурс, а не формальність.

Підсумовуючи порівняльне дослідження, можна ствердити, що Франція та Польща демонструють взаємодоповнювані моделі цифрової організації прокуратури: від «наскрізних» процесних платформ до реєстрово-сервісних механізмів відкритості та верифікації даних. Їх поєднання з урахуванням українських реалій дозволяє окреслити практичні вектори модернізації, які доцільно оформити як системні рекомендації – своєрідну нормативну, інституційну та технологічну «дорожню карту» для України, зокрема:

1. Створення спеціалізованого цифрового агентства для інформаційно-правової інфраструктури прокуратури за аналогією з французьким Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) [119]. Доцільно заснувати, наприклад, «Агентство цифрових технологій прокуратури» при Офісі Генерального прокурора України або Міністерстві юстиції, уповноважене на розроблення, впровадження та супровід платформи електронного документообігу, міжсистемної інтеграції, обміну даними, аналітики та кібербезпеки. Ключові функції: а) централізація технічних рішень; б) стандартизація даних; в) інтеграція «прокуратура – правоохоронні органи – суд» із поширенням єдиного цифрового середовища на всі органи досудового розслідування та фінансової безпеки (Національну поліцію, Державне бюро розслідувань, Бюро економічної безпеки, Національне антикорупційне бюро України, інші спеціалізовані органи), що унеможливить «острівні» ІТ-рішення, забезпечить єдині стандарти збирання й передачі доказової інформації та дозволить будувати повний електронний ланцюг «виявлення – розслідування – підтримання обвинувачення – судовий розгляд; г) підготовка кадрів; г) аудит кібербезпеки. Французький досвід (до 92 % електронних перехоплень через

платформу PNIJ) свідчить, що централізована структура дозволяє уникнути фрагментарних рішень, дублювання та посилює безпеку [120].

2. Законодавче закріплення принципів відкритих даних та електронної публічності для прокуратури за орієнтиром французького закону *Loi pour une République numérique* 2016 р. [121]. Доцільно: а) ухвалити спеціальний закон або підзаконний акт щодо прокуратури, який передбачатиме електронний документообіг, відкритість статистики, публічну звітність і механізми доступу громадськості до певних даних із дотриманням конфіденційності; б) визначити перелік оприлюднюваних показників (кількість проваджень, строки їх розгляду, ключові цифрові індикатори); в) закріпити обов'язковість відкритих форматів та інтеоперабельності, за аналогією з французькими вимогами до форматів, вихідних кодів ПЗ та оприлюднення адміністративних документів. Це підвищить прозорість і довіру до прокуратури та спростить зовнішній контроль [122].

3. Розбудова інтегрованої цифрової платформної інфраструктури «прокуратура – суд – правоохоронні органи» за зразком французьких систем віддалених слухань та дематеріалізації процесів [123]. Для України доцільно: 1) розробити платформу «Е-прокуратура» / «Прокурорський цифровий простір», що забезпечуватиме: а) електронний документообіг між прокурором, слідчим і судом; б) реєстр проваджень із відображенням статусів у реальному часі (з урахуванням обмежень доступу); в) аналітичний модуль оцінки ефективності (строки розгляду, електронні звернення, інтенсивність обміну інформацією); 2) встановити стандарти безпеки, шифрування, резервування та інтерфейси для взаємодії з правоохоронними органами й судовими системами; 3) реалізувати поетапне впровадження – від пілоту в кількох регіонах до загальнонаціонального масштабу.

4. Посилення кібербезпеки та захисту даних у прокурорських ІТ-системах за орієнтиром французького закону *Lois SREN* 2024 р. (Про безпеку та регулювання цифрового простору) [124]. Для України доцільно: а) установити спеціальні нормативні вимоги до інформаційних систем прокуратури (сертифікація, щорічний аудит, управління інцидентами, шифрування, резервне

копіювання, розмежування доступу); б) запровадити програму «Прокуратура + кібербезпека» з навчанням прокурорів, слідчих та ІТ-персоналу щодо кіберзлочинності, цифрових доказів, ризик-менеджменту; в) створити системи моніторингу кіберзагроз і реагування, особливо в сегменті обміну даними між прокуратурою, судами й правоохоронними органами.

5. Етапна реалізація реформ із пріоритетом інтероперабельності та міжнародної інтеграції [125]. Для України доцільно: 1) підготувати дорожню карту: а) короткостроковий етап (1–2 роки) – створення агентства, закріплення правових рамок, пілот цифрової платформи у 2–3 областях; б) середньостроковий (3–5 років) – масштабування платформи, повноцінна інтеграція з судовими та правоохоронними системами, запуск аналітичних модулів; в) довгостроковий (5+ років) – підключення до міжнародних систем (ЄС, ЕРРО) та створення інструментів прогнозу аналітики; 2) забезпечити інтероперабельність: стандарти даних (XML - eXtensible Markup Language (розширювана мова розмітки), JSON - JavaScript Object Notation (нотація об'єктів JavaScript), API - Application Programming Interface (програмний інтерфейс застосунків), наближення до вимог GDPR - General Data Protection Regulation (Загальний регламент захисту даних ЄС), підключення до міжнародних платформ обміну.

6. Урахування ризиків та адаптація до української специфіки. Досвід Франції та Польщі потребує не механічного перенесення, а адаптації. Перші кроки: 1) оцінити ресурси й спроможності (ІТ-інфраструктура, кадри, бюджет, законодавство); 2) реалізувати пілотний проєкт у форматі «цифрової лабораторії» в одному регіональному управлінні; 3) запровадити керування змінами (change management): комунікація з персоналом, навчання, мотивація, подолання опору; 4) визначити KPI - Key Performance Indicator(s) (ключовий(-і) показник(-и) ефективності), як частка електронного документообігу, кількість міжвідомчих обмінів, час обробки звернень; 5) підготувати резервні сценарії на випадок технічних чи організаційних збоїв [126, с. 406-408].

Водночас модернізація української прокуратури не починається «з нуля». Уже сформовано нормативну та організаційну основу інформаційно-правового забезпечення: функціонує Єдиний реєстр досудових розслідувань (ЄРДР) і системи електронного документообігу (СЕД) органів прокуратури. Кримінальний процесуальний кодекс (ч. 2 ст. 214) встановлює, що досудове розслідування починається з моменту внесення відомостей до ЄРДР, а порядок формування й ведення Реєстру затверджується Офісом Генерального прокурора за погодженням із профільними органами. Інституційно ЄРДР функціонує на підставі наказу Офісу Генерального прокурора від 30.06.2020 № 298, яким затверджено Положення про ЄРДР, визначено суб'єктів наповнення, ролі та права доступу, обов'язкові реквізити, процедури виправлення й обміну відомостями [127]. Офіс Генерального прокурора веде окрему сторінку з добіркою чинних документів щодо організації Реєстру, що полегшує уніфікацію практики [128].

Інформування громадськості здійснюється через цифрові канали Офісу Генерального прокурора: на офіційному вебсайті оприлюднюються статистичні дані, аналітичні звіти, новини, роз'яснення та актуальні нормативні акти [129]. Для уповноважених суб'єктів діє спеціалізований інтернет-портал доступу до ЄРДР [130]. Це забезпечує елемент відкритості та адміністративної впорядкованості, хоча повна публічність Реєстру обмежена вимогами процесуального законодавства й захисту персональних даних.

Найбільшою вразливістю є вузол «прокуратура – суд». Під система «Електронний суд» (у складі Єдиної судової інформаційно-телекомунікаційної системи — ЄСІТС) хоч і розвивається, але впроваджується нерівномірно, що зумовлює часткову «ручну» синхронізацію процесуальних документів і ризик розбіжності статусів справ у різних системах, тобто в окремих випадках прокурор змушений дублювати передачу матеріалів: надсилати документи до суду в електронній формі та додатково – поштою чи особисто, самостійно звіряти, чи відображено їх надходження в ЄСІТС, і порівнювати дані про стан провадження в судовій системі з даними внутрішніх облікових систем

прокуратури, що створює можливість «розходження» дат надходження, стадій розгляду та навіть складу матеріалів справи [131]. Попри наявність національної інформаційної шини «Трембіта» (X-Road) – (державна система взаємодії електронних ресурсів України, що базується на естонській платформі X-Road (безпечний шар обміну даними між реєстрами), як стандартного каналу обміну реєстровими даними, для правосуддя бракує обов'язкових API-процедур (Application Programming Interface (програмний інтерфейс застосунків) із чіткими SLA (Service Level Agreement (угода про рівень послуг) та SLI (Service Level Indicator (показник рівня послуг), наскрізним журналюванням та паспортами наборів даних. Це створює простір для обхідних практик (просто листування, ручне завантаження файлів) і послаблює доказовий ланцюг [132]. Отже, електронне адміністрування взаємодії у сфері інформаційно-правового забезпечення прокуратури України потребує невідкладної модернізації з урахуванням апробованого досвіду держав – членів ЄС.

Узагальнюючи зарубіжний досвід інформаційно-правового забезпечення діяльності прокуратури країн ЄС, слід зазначити, що його основу становлять багаторівневе нормативне регулювання, високий рівень цифровізації процедур, прозорість та належний захист персональних даних. Французька процесно-орієнтована модель єдиних цифрових платформ і польський реєстрово-сервісний підхід з акцентом на уніфікованих реєстрах та відкритих даних демонструють різні, але взаємодоповнювані формати організації інформаційного простору прокуратури. Спільними для них є чітке закріплення повноважень прокурора щодо обробки даних, інтегрованість інформаційних систем і поєднання публічної підзвітності з ефективним кримінальним переслідуванням. Для України цей досвід є цінним орієнтиром для формування власної моделі інформаційно-правового забезпечення органів прокуратури із урахуванням європейських стандартів та національної специфіки.

3.2. Перспективи формування інформаційно-правових технологій діяльності органів прокуратури України

Сучасний етап розвитку української державності характеризується одночасною дією трьох взаємопов'язаних факторів: цифрової трансформації публічного управління, євроінтеграційного курсу та функціонування органів публічної влади в умовах повномасштабної агресії. Для органів прокуратури України це означає перехід від традиційно «паперової» моделі організації діяльності до комплексного використання інформаційно-комунікаційних та інформаційно-правових технологій як системного інструменту реалізації конституційно визначених функцій. У цьому контексті питання про перспективи формування інформаційно-правових технологій діяльності органів прокуратури набуває не лише техніко-організаційного, а насамперед адміністративно-правового виміру.

У вітчизняній доктрині інформаційного права акцентовано, що якість правового регулювання інформаційних відносин визначається здатністю права інтегрувати технічні рішення у чіткі юридичні конструкції, забезпечуючи баланс між ефективністю публічного управління та гарантіями прав людини [54, с. 354]. Для органів прокуратури це проявляється у переході від фрагментарного використання окремих інформаційних систем (окремих локальних електронних журналів реєстрації заяв і повідомлень про кримінальні правопорушення, відомчих баз даних руху кримінальних проваджень на рівні окремих прокуратур, автономних систем внутрішнього діловодства й обліку кореспонденції, які не були взаємопов'язані між собою та вимагали дублювання паперових процедур) до концептуальної побудови «цифрової екосистеми» прокурорської діяльності – Єдиного реєстру досудових розслідувань (ЄРДР), інформаційно-телекомунікаційної системи досудового розслідування (зокрема «іКейс»), як інтегрованої платформи електронного кримінального провадження, що забезпечує формування електронної справи, автоматизоване фіксування слідчих та процесуальних дій, обмін документами між слідчим, прокурором і слідчим суддею, контроль процесуальних строків та уніфікацію форм процесуальних

рішень а також систем електронного документообігу. Наприклад, внутрішніх систем типу СЕД органів прокуратури, що забезпечують реєстрацію, маршрутизацію, погодження, накладення електронного підпису та архівування управлінських і організаційно-розпорядчих документів), аналітичних модулів, реєстрів статистичної звітності (зокрема інтегрованої інформаційно-аналітичної системи ІАС «ОСОП», електронних форм звітності про стан злочинності, результати досудового розслідування, показники підтримання публічного обвинувачення та ефективності прокурорського нагляду), які функціонують за єдиними класифікаторами та дозволяють отримувати порівнювану статистику в режимі реального часу.

Нормативно-правові передумови такої трансформації вже закладено у базових законах інформаційного циклу, зокрема: Законах України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про електронні документи та електронний документообіг», а також у відомчих актах Офісу Генерального прокурора, передусім Наказі від 30.06.2020 № 298, яким затверджено Положення про ЄРДР [127]. У сукупності вони формують правове ядро майбутніх інформаційно-правових технологій в діяльності органів прокуратури, визначаючи вимоги до електронних документів, режиму доступу до інформації, захисту персональних даних, процедур автентифікації та електронного підпису тощо.

Зарубіжний досвід підтверджує, що цифровізація органів публічного обвинувачення та судової системи загалом є сталим трендом європейського простору. Програми цифровізації правосуддя Європейського Союзу, розвиток Європейського порталу електронного правосуддя (e-Justice), стандарти Ради Європи щодо використання інформаційно-комунікаційних технологій у діяльності прокуратури та судів демонструють, що цифрові інструменти розглядаються не як допоміжний ресурс, а як структурний елемент належного правосуддя та верховенства права [133, с. 149]. У роботах, присвячених цифровій трансформації органів правосуддя, підкреслюється, що саме інформаційно-правові технології дозволяють перевести процесуальні процедури, обіг доказів,

комунікацію із учасниками провадження у прогнозовані, стандартизовані цифрові процеси при збереженні їх юридичної значущості [134, с. 422].

Таким чином, перспективи формування інформаційно-правових технологій діяльності органів прокуратури України слід розглядати як поетапний процес, від нормативного закріплення базових вимог до інформаційних систем – до розбудови цілісної моделі електронного кримінального провадження і цифрового прокурорського менеджменту [135, с. 258].

У цьому процесі ключовим є не лише технічне оснащення, а й вироблення адміністративно-правових підходів до організації інформаційних потоків, розмежування відповідальності суб'єктів, встановлення процедурних гарантій від зловживань та помилок.

У контексті досліджуваного питання важливим є питання впливу процесу цифровізації публічного управління на трансформацію прокурорської діяльності, що на нашу думку розглядається, як комплексна реформа, що охоплює електронні послуги, електронну демократію, відкриті дані, автоматизацію регуляторної та контрольної діяльності. У теоретичному плані цифровізацію розглядають як якісний етап розвитку державності, пов'язаний зі зміною способів прийняття рішень, організації управлінських процесів та взаємодії держави з суспільством [136, с. 37-43].

У такій рамці органи прокуратури будучи елементом системи органів публічної влади й одночасно учасником кримінального провадження, інтегруються у цей цифровий процес у двох вимірах. По-перше, як суб'єкти загальних процесів цифрової трансформації публічного управління - через запровадження електронного документообігу, використання електронного підпису, інтеграцію з іншими державними реєстрами, відкритими даними тощо. По-друге, як спеціалізовані учасники кримінальної юстиції, що здійснюють процесуальне керівництво в електронному кримінальному провадженні, взаємодіють із інформаційно-телекомунікаційною системою досудового розслідування та ЄРДР.

У науковій літературі справедливо підкреслюється, що цифровізація

наглядової діяльності прокурора змінює саму «архітектуру» його повноважень. Р. Левочко, Л. Гандзюк та А. Потинський показують, що використання електронних інформаційних систем, реєстрів та аналітичних модулів у досудовому розслідуванні трансформує модель нагляду від постфактум-перевірки паперових матеріалів до безперервного моніторингу цифрових слідів процесуальних дій, автоматизованого контролю строків, типових помилок, дублювання процесуальних документів [137, с. 120-123]. Це, у свою чергу, вимагає від прокурора нових компетентностей – здатності працювати з даними, розуміти логіку інформаційних систем, оцінювати ризики кібербезпеки та захисту персональної інформації.

Важливим елементом трансформації є розвиток електронного кримінального провадження та пов'язаних із ним інформаційно-правових технологій. Дослідження М. Поповича демонструє, що впровадження інформаційно-телекомунікаційної системи досудового розслідування, інтегрованої з ЄРДР та комп'ютерною програмою "Д-3", створює передумови для майже повної відмови від паперових носіїв на стадії досудового розслідування, а також для забезпечення безперервності та прозорості процесуальних дій [138, с. 395]. Комп'ютерна програма «Д-3» — це частина інформаційної системи, яка використовується в судових органах України, зокрема у Державному підприємстві «Інформаційні судові системи», для ведення електронного документообігу та автоматизованого розподілу судових справ між суддями. Вона є однією з комп'ютерних програм (разом з КП «Діловодство спеціалізованого суду») для зовнішніх користувачів, таких як учасники судового процесу [139].

У цьому ракурсі прокурор виступає не лише правозастосовцем, але й адміністратором інформаційних процесів – суб'єктом, який уповноважений ініціювати, контролювати та верифікувати цифрові сліди кримінального провадження.

Європейська практика підтверджує, що аналогічні процеси відбуваються в інших правопорядках. Дослідження, присвячені цифровізації цивільного й

кримінального правосуддя у державах – членах ЄС, відзначають перехід до електронного обміну процесуальними документами, створення спільних платформ для прокурорів, суддів та адвокатів, використання електронних доказів, онлайн-засідань, відео конференцій. Для органів публічного обвинувачення це означає зміщення акценту з «кабінетно-паперової» моделі роботи до моделі «цифрового офісу», в якій більшість процесуальних рішень ініціюється, фіксується й оскаржується у цифровому середовищі.

Цифровізація публічного управління у поєднанні з реформою прокуратури в Україні також підсилює вимоги до прозорості та підзвітності органів прокуратури перед суспільством. Впровадження електронних реєстрів, відкритих даних, механізмів електронних звернень, онлайн-звітності, оприлюднення статистичних показників діяльності органів прокуратури об'єктивно зменшує простір для «відомчої закритості» і водночас формує попит на нові інформаційно-правові технології, що забезпечують належний баланс між публічністю та захистом персональної й службової інформації.

Отже, цифровізація публічного управління виступає ключовим детермінантом трансформації прокурорської діяльності. Вона не просто накладає електронні інструменти на чинні адміністративно-правові форми й методи, а змушує по-новому вибудовувати систему правових, організаційних та технологічних рішень, що у своєму поєднанні становлять зміст інформаційно-правових технологій діяльності органів прокуратури України.

У свою чергу, розгляд перспектив формування інформаційно-правових технологій у діяльності органів прокуратури України доцільно здійснювати як аналіз можливих напрямів еволюції всієї моделі прокурорської діяльності, від правового статусу прокуратури й організації внутрішніх процесів до характеру взаємодії з іншими суб'єктами кримінальної юстиції, публічною адміністрацією та суспільством. Формування та впровадження таких технологій є перспективою, яка включає ряд взаємопов'язаних напрямів: нормативно-правового формування, організаційно-управлінської адаптації, технічного забезпечення, кадрового і освітнього супроводу, а також міжнародної співпраці. Так

наприклад:

1. Нормативно-правові перспективи включають:

1) Удосконалення правової бази - це подальша розбудова нормативно-правової бази, яка регламентує створення, функціонування й захист інформаційних систем органів прокуратури. У цьому контексті, розділяючи позицію С. Гайдая необхідним є систематизації правових норм, що регулюють інформатизацію діяльності органів прокуратури, що формулюється як правова основа, яка включає інформаційні технології, інформаційну безпеку, інформаційно-аналітичну діяльність [1, с. 122].

2) Забезпечення сумісності з європейськими стандартами - враховуючи бажання вступу України до європейського правового простору, органам прокуратури варто враховувати стандарти Європейського Союзу, Ради Європи та інших міжнародних організацій щодо цифровізації правозастосовної діяльності, захисту персональних даних та відкритості державних інформаційних ресурсів. Це означає перспективу гармонізації національного законодавства з європейськими директивами та виконання міжнародних зобов'язань у сфері інформаційного права. Цей підхід сприятиме підвищенню довіри до діяльності органів прокуратури, їхньої прозорості та ефективності.

3) Інтеграція міжнародно-правового виміру - перспективним є включення в правове забезпечення інформаційно-правових технологій органів прокуратури міжнародно-правових норм, угод і стандартів, зокрема у сфері обміну даними з міжнародними органами, кібербезпеки, кримінального судочинства та електронного правосуддя. Такий підхід дасть змогу органам прокуратури більш ефективно діяти в глобалізованих інформаційних просторах, брати участь у міжнародному співробітництві з розслідування транснаціональних злочинів, використання аналітики великих даних, штучного інтелекту та інших технологій.

2. Організаційно-управлінські перспективи включають:

1) Удосконалення інформаційно-аналітичної діяльності – яка становить специфічний вид інтелектуальної діяльності, що передбачає алгоритм пошуку, накопичення, обробки, аналізу інформації, формування нової аналітичної

продукції (довідки, звіти, прогнози). Перспектива полягає у впровадженні сучасних аналітичних технологій (зокрема Big Data, AI-інструментів, автоматизованих систем аналітики) для підвищення якісної основи ухвалення процесуальних чи управлінських рішень органами прокуратури. Також можлива централізація аналітичних підрозділів чи створення міжрегіональних мереж аналітики у складі органів прокуратури з метою підвищення масштабності та швидкості реагування.

2) Електронний документообіг і цифрова трансформація - це повне або часткове переведення документообігу та діловодства органів прокуратури в електронну форму, створення електронних баз даних, систем цифрового підпису, платформи взаємодії із громадськістю. Прикладом, такої розподіленої мережі є прокуратура Одеської області [140]. Де ще у 2006 році, згідно з відкритими даними, було реалізовано пілотну модель регіональної інформаційно-телекомунікаційної інфраструктури: створено захищені канали зв'язку між місцевими прокуратурами, запроваджено систему електронної реєстрації вхідних і вихідних документів, автоматизовано розподіл кореспонденції між виконавцями, контроль строків виконання доручень, електронне погодження проєктів процесуальних документів та формування електронних номенклатурних справ. Така модель демонструє, як у межах однієї області може функціонувати «розподілений офіс» прокуратури, коли більшість управлінських операцій із документами здійснюється в цифровій формі з можливістю віддаленого доступу уповноважених працівників. Це відкриває перспективу для:

- а) впровадження єдиної корпоративної інформаційної системи органів прокуратури;
- б) інтеграції з державними інформаційними системами (зокрема, з Єдиним державним реєстром судових рішень, Єдиною судовою інформаційно-телекомунікаційною системою «Електронний суд», Єдиним державним реєстром юридичних осіб, фізичних осіб-підприємців та громадських формувань, Державним реєстром речових прав на нерухоме майно, Державним реєстром фізичних осіб – платників податків, окремими галузевими реєстрами, які містять відомості, що використовуються прокурорами в їхній діяльності);
- в)

забезпечення мобільного доступу та роботи з віддаленим режимом, що є особливо актуальним в умовах воєнного стану чи надзвичайних ситуацій.

3. Технічні та технологічні перспективи включають:

1) Побудова сучасної інфраструктури ІТ – це модернізація ІТ-інфраструктури органів прокуратури (серверні рішення, хмарні сервіси, безпечні мережеві середовища, резервне зберігання, аналітичні платформи). Це дозволить забезпечити високу доступність, надійність і захищеність інформаційних ресурсів. З наукового дослідження виходить, що інформатизація органів прокуратури передбачає створення оптимальних умов (організаційних, правових, соціально-економічних, технічно-наукових) для комплексного використання інформаційно-комунікаційних технологій.

2) Використання аналітичних технологій і штучного інтелекту - для прогнозування тенденцій злочинності, аналізу великих обсягів даних, виявлення закономірностей у криміногенній обстановці, автоматичного генерування аналітичних звітів. Хоча безпосередньо українські дослідження поки ще не містять глибоко розроблених моделей ШІ для прокуратури, натомість вони підкреслюють перспективність аналітичної діяльності.

3) Забезпечення кібербезпеки та захисту інформації - це захист персональних даних, забезпечення конфіденційності, цілісності та доступності інформації, відповідно до вимог міжнародних стандартів. Технологічні перспективи включають створення систем управління інформаційною безпекою, сертифікацію ІТ-систем, впровадження систем раннього виявлення кіберзагроз, навчання персоналу з кібергігієни, а також участь у міжвідомчих платформах обміну кіберінформацією.

4. Кадрово-освітні перспективи включають:

1) Підвищення кваліфікації та підготовка фахівців - для реалізації інформаційно-правових технологій потрібні компетентні кадри, це юристи, які володіють знаннями в інформаційному праві, так і ІТ-спеціалісти, що орієнтуються у правовій сфері. Перспективами є: а) запровадження програм підвищення кваліфікації працівників органів прокуратури з питань

інформаційного права, цифрової грамотності, кібербезпеки; б) створення міждисциплінарних навчальних комплексів (юридичні + ІТ); в) відкриття курсів і тренінгів із застосування ІТТ у правозахисній діяльності.

2) Формування інформаційної культури та правосвідомості - важливо формувати в середовищі органів прокуратури інформаційну культуру, тобто, усвідомлення значення даних, аналітики, інформаційних процесів, відповідальності за інформаційні ресурси та їхній правовий режим. Це важлива складова успішного впровадження ІТТ. Перспективами є: а) створення систем внутрішньої комунікації, що підсилюють інформаційну правосвідомість; б) розробка етичних стандартів роботи з інформацією; в) впровадження заходів, які стимулюють активне користування аналітичними ресурсами, електронним документообігом та платформами обміну.

5. Перспективи щодо правового статусу і взаємодії включають:

1) Правовий статус інформаційно-правових технологій - це визначення в правовому полі статусу інформаційно-правових технологій як елементу системи діяльності органів прокуратури. Це передбачає уточнення функцій, прав і обов'язків суб'єктів, відповідальності за інформаційні процеси, алгоритмів взаємодії та контролю.

2) Взаємодія між органами прокуратури та іншими суб'єктами - це розвиток взаємодії органів прокуратури з іншими державними та міжнародними інституціями, приватним сектором, громадськими організаціями у сфері інформаційно-правового забезпечення. Така взаємодія сприяє обміну даними, координації дій, реалізації спільних аналітичних проєктів і створенню інформаційних платформ мульти-секторного призначення.

6. Перспективи впровадження в умовах воєнного стану та післявоєнної трансформації включають:

1) Адаптація ІТТ до умов надзвичайного режиму - в умовах воєнного стану та високої динаміки загроз інформаційно-правові технології органів прокуратури потребують особливого врахування, наприклад: мобільність, стійкість, безперервність діяльності, захищеність інформаційних потоків, можливість

дистанційної роботи. У цих обставинах перспективним є розгортання автономних систем, резервних центрів, мобільних робочих місць, що забезпечують безперебійну роботу органів прокуратури. Це означає, впровадження технології блокчейн для забезпечення незмінності даних, система криптозахисту, віддалені підключення для органів прокуратури та ін.

2) Післявоєнна трансформація і цифрове відновлення - після стабілізації ситуації в державі органам прокуратури доведеться брати участь у процесах цифрового відновлення, трансформації правосуддя, відбудови інституційних процесів. Інформаційно-правові технології можуть відіграти ключову роль у модернізації системи прокуратури, а саме: створення розумних платформ для обміну даними, інтеграція з системами міжнародної гуманітарної допомоги, відновлення архівів в електронному форматі, створення єдиних репозиторіїв доказів злочинів війни.

Проте при формуванні перспектив інформаційно-правових технологій органів прокуратури необхідно враховувати низку викликів: 1) технологічний розрив між органами, регіонами, кадровий дефіцит ІТ-фахівців; 2) правова неврегульованість частини інформаційних процесів, що може призвести до правового вакууму або зловживань; 3) загрози кібербезпеки, витоки, знешкодження інформаційних систем; 4) опір змінам на рівні організаційної культури, недостатня інформаційна правосвідомість працівників; 5) необхідність значних фінансових ресурсів, що в умовах обмеженого бюджету можуть стати перепорою.

Узагальнюючи, хочемо відзначити, що формування інформаційно-правових технологій діяльності органів прокуратури України відкриває значні перспективи для модернізації їхньої функціональної діяльності, підвищення ефективності, прозорості, професійності та інтеграції із сучасними міжнародними правовими та технологічними стандартами. Особливо актуальними перспективи стають в умовах воєнного стану та післявоєнної трансформації, коли цифрові рішення та інформаційні технології стають ключовими в правозастосовній діяльності.

Однак успіх цих перспектив залежить від спроможності органів прокуратури адаптуватися до змін, забезпечення адміністративно-правового та технологічного середовища, підготовки персоналу для адміністрування інформаційно-правових технологій, управління ризиками та ефективної взаємодії з іншими гілками влади та міжнародного середовища. Науково-методичне супроводження цього процесу, зокрема через подальші дослідження, розробку стандартів, моніторинг результатів, є невід'ємною складовою. Отже, інформаційно-правові технології мають стати не просто інструментом, а складовою стратегії розвитку системи прокуратури України, що відповідає викликам ХХІ століття.

3.3. Напрями вдосконалення законодавчої бази з інформаційно-правового забезпечення діяльності органів прокуратури України

Аналіз чинної законодавчої бази інформаційно-правового забезпечення діяльності органів прокуратури України дає змогу окреслити ключові напрями її вдосконалення. Насамперед ідеться про посилення обов'язковості та визначеності правових приписів, які регулюють створення, збирання, обробку, зберігання, захист і розкриття інформації в діяльності органів прокуратури, – шляхом чіткого формулювання прав та обов'язків посадових осіб і закріплення дієвих механізмів відповідальності. Важливим напрямом є модернізація чинного законодавства, що регламентує інформаційні процеси, з урахуванням пріоритету актів вищої юридичної сили з використанням досвіду країн ЄС.

Окремого вдосконалення потребує системність і комплексність законодавчої бази: вона має цілісно охоплювати всі стадії інформаційного циклу (збирання, обробка, захист, зберігання, доступ) саме в діяльності органів прокуратури [23, с. 88]. У зв'язку з цифровізацією, розвитком технологій обробки великих масивів даних та зростанням кіберзагроз законодавство має бути більш динамічним, оперативно адаптуючись до нових форматів електронної взаємодії, електронного кримінального провадження, кібербезпеки. Нарешті, напряду модернізації потребує правозахисний вимір законодавчої

бази: норми, що регулюють доступ до інформації, захист персональних даних, конфіденційність і режим державної таємниці, мають узгоджуватися з європейськими стандартами прав людини та публічними інтересами, на чому акцентується й у сучасних наукових дослідженнях інформаційного права [141, с. 44]. Таким чином, удосконалення законодавчої бази розглядається не лише як її оновлення, а як системний напрям реформування інформаційно-правового забезпечення діяльності органів прокуратури України.

У контексті визначення напрямів вдосконалення законодавчої бази з інформаційно-правового забезпечення діяльності органів прокуратури України важливо насамперед уточнити її зміст і структуру. Під такою законодавчою базою доцільно розуміти сукупність нормативно-правових актів та інших юридичних джерел, які регулюють діяльність органів прокуратури у сфері створення, збирання, обробки, зберігання, захисту та розкриття інформації. У межах удосконалення цієї бази ключовими залишаються такі елементи: вид джерела права, суб'єкт його прийняття, юридична сила акта, предмет регулювання (доступ до інформації, зберігання службових відомостей, захист конфіденційної інформації, технологічні процедури) та механізми контролю й відповідальності.

Подальший розвиток законодавчої бази вимагає логічно вибудованої структури та чіткої ієрархії актів. В адміністративно-правовій доктрині традиційно наголошується, що джерела адміністративного права України охоплюють Конституцію України, закони України, міжнародні договори, підзаконні акти Кабінету Міністрів України, міністерств, відомчі нормативно-правові акти (накази, інструкції), рішення Конституційного Суду України та інші підзаконні акти [142, с. 115].

З позицій адміністративного права одним із ключових напрямів вдосконалення є посилення зв'язку законодавчої бази з інститутами адміністративної відповідальності та службової дисципліни. Нормативні акти мають не лише встановлювати обов'язки посадових осіб органів прокуратури у сфері інформаційно-правового забезпечення, а й чітко визначати правові

наслідки їх порушення: дисциплінарну відповідальність за недодержання службових обов'язків та процедур, адміністративну відповідальність за правопорушення, пов'язані з інформацією, а також можливість застосування інших організаційно-правових заходів. Удосконалення законодавства в цьому вимірі спрямоване на зміцнення механізмів державного примусу та контролю в адміністративній площині.

З метою підвищення керованості й прозорості доцільно розвивати законодавчу базу за модульним принципом: а) модуль «доступ і розкриття»; б) модуль «захист і зберігання»; в) модуль «контроль і аудит»; г) модуль «відповідальність». Кожен модуль має охоплювати акти різного рівня – від закону до внутрішньої інструкції, – що дозволить структуровано впорядкувати регулювання інформаційних процесів у діяльності органів прокуратури. Такий підхід відображає один із пріоритетних напрямів вдосконалення законодавчої бази, орієнтований на її системність, узгодженість та практичну ефективність.

Конституційний рівень задає вихідні орієнтири для подальшого вдосконалення законодавства: стаття 34 Конституції України гарантує право кожного «вільно збирати, зберігати, використовувати і поширювати інформацію» та допускає його обмеження лише законом і за умов, пов'язаних із національною безпекою, територіальною цілісністю, громадським порядком тощо [5].

Закон України «Про прокуратуру» № 1697-VII визначає правовий статус органів прокуратури, їхні завдання та обов'язки, у тому числі щодо збереження охоронюваної законом інформації. Для подальшого розвитку законодавчої бази важливим є те, що норми про організацію діяльності, повноваження й процесуальні гарантії формують загальну «рамку компетенції», у межах якої підзаконні акти деталізують процедури доступу, зберігання, захисту, обліку та розкриття відомостей. Зокрема, стаття 19 прямо покладає на прокурора обов'язок не розголошувати відомості, які становлять таємницю, що охороняється законом [13].

Законодавчі акти нашої держави задають змістовне наповнення таких змін. Закон України «Про інформацію» визначає базові дефініції, класифікацію інформації та загальні правила доступу й обмеження [31], а Закон України «Про захист персональних даних» – принципи та підстави обробки, обов’язки володільців і розпорядників, права суб’єктів даних [33].

На рівні підзаконних актів та відомчих документів визначаються практичні напрями вдосконалення законодавчої бази з інформаційно-правового забезпечення діяльності органів прокуратури України. Йдеться про накази, інструкції, положення про підрозділи інформаційного забезпечення, внутрішні політики захисту інформації, процедури доступу до публічної інформації, журнали обліку доступу та резервного копіювання – саме їх оновлення та узгодження забезпечує реальну дію законодавчих вимог.

Зокрема, у сфері кримінальної юстиції діє наказ Генерального прокурора від 30.06.2020 № 69 «Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення», який встановлює порядок реєстрації відомостей, ролі користувачів та контроль строків у ЄРДР [127]. Процедури доступу до публічної інформації в системі органів прокуратури унормовано Інструкцією Офісу Генерального прокурора щодо опрацювання запитів (наказ ОГП від 25.06.2024 № 153) [143] та оновленнями до Інструкції про доступ до публічної інформації (наказ ОГП від 17.07.2024 № 171), що конкретизують строки, форми відповідей і роботу через офіційні канали [144]. Організацію діловодства й електронного документообігу в органах прокуратури забезпечують внутрішні інструкції, що кореспондують із «Типовою інструкцією з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну» (постанова КМУ від 17.01.2018 № 55), яка визначає реєстрацію, маршрутизацію, архівне зберігання та облік службових документів (у т.ч. електронних) [145]. Вимоги до журналювання доступу, резервного копіювання та технічного захисту інформації впроваджуються відповідно до постанови КМУ

від 19.06.2019 № 518 і загальних вимог до кіберзахисту, затверджених урядом для об'єктів критичної інфраструктури [146].

Важливим орієнтиром є Наказ Генерального прокурора від 06.08.2020 № 363, яким затверджено Інструкцію про порядок забезпечення доступу до публічної інформації в органах прокуратури України та консолідовано попередні акти [147]. Це показує, що один з ключових напрямів удосконалення законодавчої бази полягає в оновленні відомчих процедур доступу до інформації з урахуванням сучасних електронних форматів.

На відомчому рівні значення має й Кодекс професійної етики та поведінки прокурорів, який закріплює імперативи збереження та нерозголошення охоронюваної інформації та фактично орієнтує застосування дисциплінарної відповідальності за порушення інформаційних стандартів [148].

Окремим напрямом є нормативне закріплення електронної взаємодії з іншими органами публічної влади. Показовим є спільний наказ Державної судової адміністрації України та Офісу Генерального прокурора від 02.05.2024 № 189/98 щодо електронного обміну процесуальними документами в Єдиній судовій інформаційно-телекомунікаційній системі [149].

Також слід підкреслити, що важливим орієнтиром для напрямів вдосконалення законодавчої бази з інформаційно-правового забезпечення діяльності органів прокуратури України є міжнародно-правові джерела. Йдеться про конвенції, рекомендації та стандарти (зокрема Конвенцію Ради Європи про кіберзлочинність – «Будапештську конвенцію», директиви Європейського Союзу з кібербезпеки, стандарти Організації Об'єднаних Націй). Їх імплементація сприяє наближенню українського регулювання до міжнародних вимог у частині обробки електронних доказів, реагування на кіберінциденти та забезпечення доступу до інформації в умовах воєнного стану [150].

Окремі проєкти Ради Європи для України (CyberEast/CyberEast+) акцентують увагу на узгодженості національного законодавства з Будапештською конвенцією та практиками обміну даними, що безпосередньо стосується інформаційно-правового забезпечення прокуратури. Їх практичне

значення полягає у напрацюванні типових процедур і доказових стандартів, які надалі інтегруються у відомчі акти органів прокуратури [151]. Зокрема, у вигляді методичних рекомендацій щодо збирання, фіксації та зберігання електронних доказів, стандартів «ланцюга збереження» (chain of custody), типових форм звернень до іноземних провайдерів і компетентних органів, а також внутрішніх інструкцій щодо використання результатів цифрової експертизи у кримінальному провадженні. Таким чином, напрацьовані в межах проєктів Ради Європи підходи поступово трансформуються у конкретні правила службової поведінки прокурорів та ІТ-фахівців, закріплені у наказах, регламентах і методичних листах.

Крім того, для окреслення напрямів вдосконалення законодавчої бази з інформаційного-правового забезпечення діяльності органів прокуратури України доцільно мати узагальнену «карту процесів і ролей», яка показує, як на практиці здійснюється обробка інформації, де виникають ризики витоку чи несанкціонованого доступу і які запобіжники мають бути нормативно закріплені.

У спрощеному вигляді така карта включає принаймні п'ять блоків: 1) надходження та первинну реєстрацію відомостей (заяви, повідомлення, матеріали ДБР, НАБУ, БЕБ, Нацполіції тощо); 2) формування та ведення електронних кримінальних проваджень і внутрішнього службового документообігу; 3) обмін інформацією з іншими органами публічної влади та судами; 4) аналітичну обробку й статистичну звітність; 5) архівування, обмеження доступу та знищення інформації після спливу визначених строків зберігання.

Основні процеси охоплюють: збирання інформації (у тому числі доказової й аналітичної), її обробку та зберігання, визначення кола осіб, уповноважених на доступ, розкриття чи передачу відомостей, реагування на інциденти (несанкціонований доступ, витік, пошкодження), аудит і контроль (журнали доступу, логи, внутрішні перевірки) та притягнення до дисциплінарної, адміністративної чи кримінальної відповідальності.

Наприклад, на стадії первинної реєстрації відомостей про кримінальне

правопорушення ключову роль відіграють канцелярія, черговий прокурор і реєстратор ЄРДР, які працюють із персональними даними заявників, відомостями про подію, можливих підозрюваних тощо. На цьому етапі точками ризику є: несвоєчасне або неповне внесення відомостей до ЄРДР, паралельне ведення «тіньових» журналів, передання інформації через незахищені канали (звичайна електронна пошта, месенджери). Формальними запобіжниками виступають відомчі інструкції щодо реєстрації заяв і повідомлень, обов'язкове журналювання всіх операцій у ЄРДР, персоніфікований доступ реєстраторів та періодичні перевірки повноти внесених даних.

На стадії внутрішнього документообігу й підготовки процесуальних документів (постанов, клопотань, обвинувальних актів) основним інструментом є система електронного документообігу, з якою працюють прокурори, помічники, працівники діловодства. Тут ризики пов'язані з обігом «обхідних» документів поза СЕД (через обмін файлами напряму), масовим друком і винесенням конфіденційних матеріалів, дублюванням документів на особистих носіях. Відповідні запобіжники включають вимоги щодо обов'язкової реєстрації всіх документів у СЕД, обмеження можливостей копіювання й друку, політики використання зовнішніх носіїв інформації та внутрішні перевірки дотримання цих правил. При взаємодії з іншими органами – судами, органами досудового розслідування, СБУ, ДБР, НАБУ, БЕБ – використовуються як електронні канали (інтеграція з державними реєстрами, системами на кшталт «Електронного суду»), так і традиційний обіг паперових документів.

У цих процесах беруть участь посадові особи органів прокуратури, відповідальні за інформаційне забезпечення, служби внутрішньої безпеки, підрозділи ІТ-безпеки та контролю доступу, а також зовнішні органи, що надають інформацію. Точки ризику пов'язані з несанкціонованим доступом до службових і конфіденційних даних, помилковою класифікацією чи зберіганням, витоками через електронні канали, недостатнім журналюванням доступу, слабким контролем служб безпеки та «сірими зонами» у розподілі повноважень.

Запобіжники охоплюють законодавчі та відомчі норми щодо доступу й

захисту інформації, внутрішні політики органів прокуратури, системи журналювання і резервного копіювання, багатофакторну автентифікацію, регулярні перевірки й внутрішній аудит, процедури реагування на інциденти, навчання персоналу та розвиток інформаційної правосвідомості та внутрішніх актів органів прокуратури України.

Разом із тим аналіз чинних підзаконних актів дає підстави вважати, що ці запобіжники не завжди відповідають сучасним кіберризикам. Зокрема: 1) Дисциплінарний статут прокуратури та відомчі накази переважно описують загальні порушення службової дисципліни, але не містять розгорнутої типології проступків, пов'язаних із роботою в інформаційних системах (компрометація ключів доступу, маніпулювання записами в ЄРДР, несанкціоноване копіювання баз даних тощо); 2) внутрішні регламенти часто хоча і встановлюють обов'язковості багатофакторної автентифікації для доступу до критичних інформаційних систем, обмежуючись логіном/паролем, що не відповідає найкращим практикам кібербезпеки; 3) порядок документування та розслідування інцидентів інформаційної безпеки залишається фрагментарним: відсутні уніфіковані форми актів, строкові стандарти реагування (наприклад, 24/72 години), чітко прописані вимоги до технічної фіксації подій (форензик-копії, збереження логів); 4) частина інформаційної взаємодії з іншими органами публічної влади досі здійснюється через незахищені або частково захищені канали (звичайна електронна пошта, месенджери), що зумовлено відсутністю детально регламентованих вимог до технічних засобів обміну. Саме ці приклади дозволяють обґрунтовано стверджувати про розрив між формальною наявністю відомчих політик і їх відповідністю актуальному рівню кіберзагроз та міжнародним стандартам інформаційної безпеки.

Отже, така карта процесів і ролей демонструє, що законодавча база має не лише визначати загальні правила, а й забезпечувати інтеграцію технологічних та організаційних механізмів, які реально гарантують дотримання режимів обробки інформації та мінімізацію ризиків витоку й несанкціонованого доступу.

На нашу думку, потребує оновленого підходу з вирішення наступні

проблеми:

1. Відсутність єдиного системного підходу породжує прогалини, дублювання норм та правову невизначеність, зокрема щодо службової інформації, електронних доказів, правил обробки даних. Так, наприклад, режим «службової інформації» одночасно впливає із Закону України «Про інформацію», типових інструкцій із діловодства та відомчих наказів Генерального прокурора, які не завжди узгоджуються між собою за критеріями віднесення відомостей до обмеженого доступу. Окремими блоками врегульовано ЄРДР, системи електронного документообігу, режимно-секретну роботу, але відсутній єдиний рамковий акт, що комплексно описував би «цифрову екосистему» прокуратури (перелік систем, ролі користувачів, базові принципи обробки даних, єдині підходи до журналювання й зберігання інформації). У результаті одна й та сама операція – наприклад, внесення відомостей до ЄРДР на підставі процесуального рішення прокурора та паралельна реєстрація документів у СЕД – регулюється різними інструкціями, які не завжди узгоджені за термінологією та вимогами до строків, що створює «сіру зону» для помилок та зловживань.

2. Колізії між загальним інформаційним законодавством і спеціальними актами. Закони «Про інформацію» та «Про захист персональних даних» регламентують обіг інформації загалом, але майже не враховують специфіку прокуратури. Водночас Закон «Про прокуратуру» не містить чітких приписів щодо обов'язків і відповідальності працівників у сфері інформаційної безпеки. Це створює колізії при визначенні меж конфіденційної інформації, порядку її класифікації та доступу. Зокрема, загальне інформаційне законодавство виходить із презумпції відкритості публічної інформації та права особи на доступ до своїх персональних даних, тоді як процесуальні норми й відомчі акти прокуратури оперують категоріями таємниці досудового розслідування, службової інформації, внутрішніх аналітичних матеріалів. На практиці це проявляється, наприклад, у ситуаціях, коли запитувач вимагає надати копії процесуальних документів або витяги з ЄРДР, посилаючись на Закон «Про

доступ до публічної інформації», тоді як прокурор змушений обмежувати доступ, керуючись КПК та внутрішніми інструкціями, які прямо не співвіднесені з режимами публічної інформації. Аналогічно, Закон «Про захист персональних даних» встановлює загальні строки зберігання та принцип мінімізації даних, але спеціальне кримінальне й архівне законодавство передбачає значно триваліші строки зберігання матеріалів проваджень. При цьому спеціальний механізм узгодження цих вимог для органів прокуратури законодавчо не деталізований. Це зумовлює різночитання щодо того, які саме персональні дані можуть і повинні зберігатися в ЄРДР, внутрішніх базах і статистичних масивах, а які мають бути знеособлені або видалені.

3. Проблеми застосування Дисциплінарного статуту прокуратури України, зокрема: а) Статут містить лише загальні положення й не передбачає спеціальних складів дисциплінарних проступків, пов'язаних із витоком службової чи конфіденційної інформації, порушенням правил доступу до реєстрів, ведення інформаційних систем, збереження електронних документів; б) відсутній механізм «ескалації» стягнень за повторні порушення: не закріплено прогресивної відповідальності (від першого дисциплінарного заходу до більш суворих наслідків за системні порушення інформаційної безпеки); в) не врегульовано порядок фіксації цифрових інцидентів (несанкціонований доступ, втрата даних тощо), що ускладнює кваліфікацію таких випадків як дисциплінарних проступків в умовах цифрової інфраструктури прокуратури.

4. Недоліки Кодексу України про адміністративні правопорушення (КУпАП), зокрема: а) відсутні окремі склади правопорушень, пов'язаних з інформаційними проступками у публічній службі – немає спеціальних норм щодо порушення інформаційного законодавства службовими/посадовими особами органів прокуратури та правоохоронних органів; б) не передбачено адміністративної відповідальності за недодержання внутрішніх інструкцій щодо обробки електронних доказів або доступу до реєстрів, тому працівники БЕБ, ДБР, Нацполіції, СБУ, НАБУ та прокуратури можуть грубо порушувати режим інформаційного поводження без наслідків у публічно-правовій площині; в)

відсутні норми про «повторне правопорушення» у сфері інформаційної дисципліни як обтяжуючу обставину або окремий склад, що послаблює превентивний ефект регулювання.

5. Проблеми інформаційного законодавства, зокрема: а) немає спеціального закону про службову чи конфіденційну інформацію, Закон України «Про інформацію» пропонує лише загальну класифікацію, згідно з якою виокремлюються: відкрита інформація та інформація з обмеженим доступом, а остання поділяється на конфіденційну, службову та таємну. Водночас у законі не встановлено вичерпних критеріїв, які саме відомості органи прокуратури мають відносити до службової чи конфіденційної інформації, не деталізовано порядок зміни режиму доступу, строки зберігання тощо. Тоді як у реальній практиці прокуратури використовуються внутрішні класифікації, закріплені у відомчих інструкціях з діловодства, переліках відомостей, що становлять службову інформацію в Офісі Генерального прокурора, типових переліках документів, на які накладається гриф «Для службового користування», а також у режимно-секретних інструкціях (зокрема, із використанням грифів «Таємно», «Цілком таємно», «Для службового користування» залежно від змісту матеріалів досудового розслідування, оперативних розробок, внутрішньої аналітики). Ці класифікації фактично визначають режим доступу до інформації, однак мають суто відомчий характер і не кодифіковані в єдиному законі, що зумовлює правову невизначеність і відсутність чітких орієнтирів для працівників, особливо при вирішенні колізій між вимогами відкритості та режимом обмеженого доступу.

б) неврегульоване поводження з цифровою інформацією – законодавство не встановлює належні способи фіксації, зберігання, передавання й архівування електронних даних у кримінальному та інших видах проваджень, зокрема електронних доказів (листування в месенджерах, даних з мобільних пристроїв, логів інформаційних систем, відеозаписів із камер спостереження, цифрових даних аграрних реєстрів тощо). Не визначено на рівні закону обов'язкові процедури технічної фіксації (створення форензик-копій, хеш-суми, формат

збереження), стандарти передачі таких даних між органами (прокуратура – ДБР – БЕБ – НАБУ – суд), правила довгострокового архівування та збереження цілісності електронних масивів. На практиці це призводить до використання різнорідних носіїв (флеш-накопичувачів, оптичних дисків, хмарних сховищ) без єдиних вимог до захисту й перевірки автентичності, що ускладнює доказування, формування цифрових слідів, верифікацію джерел та посилює ризик оскарження допустимості електронних доказів.

в) відсутні механізми «технічного обов'язку» для органів прокуратури (обов'язковість багатофакторної автентифікації, журналювання доступу, резервного копіювання тощо), які є стандартними для міжнародної практики, зокрема відповідно до стандартів ISO/IEC 27001 [152]. Тобто на рівні закону прямо не передбачено мінімальні технічні вимоги до функціонування інформаційних систем прокуратури. Нині питання застосування багатофакторної автентифікації при доступі до ЄРДР та інших реєстрів, обов'язкового централізованого логування всіх операцій користувачів, періодичного резервного копіювання баз даних, проведення регулярних тестів на вразливості та аудиту інформаційної безпеки вирішуються переважно відомчими наказами, а не імперативними законодавчими приписами. Через це технічні гарантії захисту інформації можуть істотно відрізнятись між окремими регіональними прокуратурами, а невиконання таких вимог нерідко сприймається як внутрішнє порушення дисципліни, а не як невід'ємний елемент публічно-правового обов'язку, що підлягає посиленій юридичній відповідальності.

З огляду на виявлені проблеми інформаційно-правового забезпечення, в умовах цифровізації державного управління та зростання кіберзагроз законодавча база, що регламентує діяльність органів прокуратури, потребує не лише технічної адаптації, а й глибинного переосмислення. Фрагментарність регулювання, відсутність спеціалізованих механізмів відповідальності за порушення режиму обігу інформації та слабкі процедурні гарантії фіксації інцидентів об'єктивно зумовлюють потребу у системному оновленні законодавчих і відомчих актів. Основні напрями такого вдосконалення можна

окреслити так:

1. Зміни до Дисциплінарного статуту прокуратури України - доцільно запровадити окремий розділ про дисциплінарну відповідальність за проступки у сфері обігу інформації та роботи в інформаційних системах, чітко визначивши види проступків (витік, неналежне зберігання, порушення правил доступу, класифікації, ведення ІС, ЄРДР тощо), їх типологію та ступені тяжкості, а також процедуру фіксації й доказування цифрових інцидентів.

Так, наприклад новий розділ № IV Статуту можна сформулювати з наступних статей:

- Стаття 1. Поняття інформаційного дисциплінарного проступку - умисне порушення встановленого порядку доступу, зберігання, класифікації, обліку, розкриття чи передачі службової або конфіденційної інформації (у т.ч інформації, що міститься в інформаційних системах прокуратури), невиконання обов'язкових техніко-організаційних заходів під час роботи з інформаційними системами, перешкоджання інцидент-менеджменту.

- Стаття 2. Типологія проступків: а) доступ без правової підстави; б) неналежне зберігання (відсутність шифрування, зберігання на неавторизованих носіях тощо); в) розголошення/витік; г) ігнорування процедур інцидент-менеджменту; г) маніпуляції журналами доступу; д) несвоєчасний облік відомостей в ІС; неповний, недостовірний облік відомостей в ІС.

- Стаття 3. Категорії тяжкості: а) легкі (без наслідків, усунуті одразу); б) значні (ризик шкоди правам людини/інтересам правосуддя); в) грубі (реальний витік, порушення таємниці, істотна шкода).

- Стаття 4. Процедура фіксації інциденту: акт виявлення; строк повідомлення керівництва (напр., 24 години); обов'язкове збереження електронних логінів; первинне блокування доступів до особистих ключів для доступу; внутрішній аналітичний звіт, службова перевірка.

- Стаття 5. Докази: допустимість і належність електронних журналів, технічних логінів, форензик-знімків; вимоги до «ланцюга збереження».

Також, важливо закріпити ескалаційну шкалу стягнень – від зауваження до

звільнення – та доповнити ст. 9 Статуту новим видом дисциплінарного стягнення у вигляді тимчасової заборони доступу до службової інформації як гнучкого інструмента персональної відповідальності. Запропоновані зміни до статуту представлені у вигляді законопроекту до роботи.

2. Зміни до Кодексу України про адміністративні правопорушення – на наш погляд КУпАП має деякі прогалини, які підлягають усуненню, з метою модернізації існуючої нормативно-правової бази для діяльності органів прокуратури з інформаційно-правового забезпечення.

Наразі в КУпАП відсутні окремі склади правопорушень щодо інформаційних проступків у публічній службі. КУпАП не містить статей, які прямо передбачають відповідальність за порушення інформаційного законодавства з боку службових і посадових органів прокуратури та правоохоронних органів; не містить спеціалізованих норм щодо складів проступків, пов'язаних із порушенням правил роботи у відомчих інформаційних системах (ЄРДР, система електронного документообігу, аналітичні підсистеми).

Відсутність адміністративної відповідальності за невиконання вимог інформаційної безпеки у разі порушення внутрішніх інструкцій, що встановлюють режим обробки електронних документів або доступу до реєстрів створює ситуацію, коли працівники правоохоронних органів (БЕБ, ДБР, Нацполіції, СБУ, НАБУ), працівники прокуратури можуть грубо порушити режим інформаційного поведіння без наслідків у публічному правовому полі.

З метою посилення адміністративної відповідальності з інформаційної безпеки необхідно у Загальній частині КУпАП запровадити узагальнений конструкт «спеціальне право доступу до інформаційних (автоматизованих) систем» як унормовану правову категорію, яка може бути об'єктом адміністративного тимчасового обмеження на визначений строк та визначити його як додаткове адміністративне стягнення.

З огляду на викладене, доцільним вбачається внесення змін до КУпАП, шляхом доповнення його окремих статей:

- 1) Доповнити ч. 1 ст. 24 КУпАП (види адміністративних стягнень) пунктом

9 - позбавлення спеціального права доступу до інформаційних (автоматизованих) систем.

2) Також, доцільно доповнити Загальну частину КУпАП статтею 32-2 КУпАП «позбавлення спеціального права доступу до інформаційних (автоматизованих) систем» у якій розкрити поняття «інформаційні (автоматизовані) системи» та поняття «спеціальне право доступу до інформаційних систем».

У ч.1 ст. 32-2 КУпАП визначити, що інформаційні (автоматизовані) системи» - це інформаційно-комунікаційні системи, які забезпечують збір, обробку, зберігання, систематизацію інформації, що становить державну таємницю, службову інформацію та іншу інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом, із застосуванням технічних засобів електронних комунікацій і засобів криптографічного захисту інформації.

У ч. 2 ст. 32-2 КУпАП окреслити, що спеціальне право доступу до інформаційних систем – службово зумовлена, персоніфікована можливість посадової чи службової особи виконувати операції з інформацією, що має спеціальний правовий режим (таємна, службова, конфіденційна, інша охоронювана законом інформація), у тому числі шляхом доступу до відповідних інформаційних систем, реєстрів у межах посадової компетенції за допомогою спеціального обладнання та особистих ключів доступу.

Ч. 3 ст. 32-2 КУпАП також необхідно доповнити наступним: що адміністративна відповідальність у вигляді позбавлення спеціального права доступу до інформаційних (автоматизованих) систем може застосовуватись до державних службовців, посадових та службових осіб органів державної влади, місцевого самоврядування, правоохоронних органів та суду, строком від одного до шести місяців.

У ч.4 ст.32-2 КУпАП передбачити обов'язок для адміністраторів безпеки органів державної влади, місцевого самоврядування, правоохоронних органів та суду, після набрання чинності постанови суду, якою накладено на правопорушника стягнення у вигляді позбавлення спеціального права доступу

до інформаційних систем, невідкладно виконати рішення шляхом блокування особистих ключів доступу, деактивування облікових записів, анулювання сертифікатів.

Відділи роботи з кадрами органів державної влади, місцевого самоврядування, правоохоронних органів та суду, зобов'язані внести до відомчого реєстру відомості про факт застосування такого стягнення до правопорушника для контролю повторності.

Особливу частину КУпАП пропонуємо доповнити окремими складами правопорушень у сфері роботи з інформаційними системами, зокрема:

1) Ст.212-5 КУпАП (Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію) частиною третьою наступного змісту: «Не забезпечення Реєстратором повного, всебічного та достовірного обліку обов'язкових до внесення відомостей про кримінальне правопорушення до ЄРДР; невнесення, несвоєчасне (понад 24 години) внесення Реєстратором відомостей до ЄРДР про рух кримінальних проваджень, - тягне за собою накладення штрафу на посадових осіб - від шістдесяти до ста неоподатковуваних мінімумів доходів громадян».

2) Ст.212-5 КУпАП частиною четвертою наступного змісту: «Безпідставне редагування (зміна) Реєстратором зафіксованих у ЄРДР відомостей, внесення Реєстратором оновлених даних до електронних форм ЄРДР, які не підтверджені матеріалами досудового розслідування, що призвело до порушення прав учасників кримінального провадження, - тягне за собою накладення штрафу на посадових осіб - від ста до ста шестидесяти неоподатковуваних мінімумів доходів громадян».

3) Ст.212-5 КУпАП частиною п'ятою наступного змісту: «Повторне протягом року вчинення порушень, передбачених частинами третьою або четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу на посадових осіб - від ста шестидесяти до двохсот шістдесяти неоподатковуваних мінімумів доходів громадян».

Крім того, доцільним вбачається доповнення ст.212-6 КУпАП (Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем), частиною 7 наступного змісту, - «Компрометація Реєстратором чи Користувачем особистих ключів для доступу до інформаційних (автоматизованих) систем, втрата або пошкодження носія ключової інформації, розголошення ідентифікаторів, - тягне за собою накладення штрафу від двадцяти до ста неоподатковуваних мінімумів доходів громадян».

Також ст. 212-5 та 212-6 КУпАП необхідно доповнити приміткою, у якій навести поняття: а) реєстратор; б) користувач; в) інформаційні (автоматизовані) системи.

Під реєстратором, слід розуміти - службову особу органу досудового розслідування або органів прокуратури, уповноважену на внесення, зміну та облік відомостей в Єдиному реєстрі досудових розслідувань чи іншій службовій інформаційній (автоматизованій) системі.

Під користувачем інформаційної (автоматизованої) системи, слід розуміти - службову особу органу прокуратури, органу досудового розслідування чи іншого органу публічної влади, якій надано персональні ідентифікатори та (або) особисті ключі для доступу до такої системи з метою виконання службових повноважень.

Під інформаційними (автоматизованими) системами, про які йдеться у статті 212-6 КУпАП слід розуміти державні інформаційні ресурси - систематизовану інформацію, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, правоохоронним органам, прокуратурі, суду та військовим формуванням, утвореним відповідно до законів України.

З метою забезпечення об'єктивності під час складення протоколів про адміністративні правопорушення необхідно доповнити статтю 255 КУпАП (Особи, які мають право складати протоколи про адміністративні

правопорушення), - протоколи про правопорушення мають право складати уповноважені на те посадові особи органів Державної служби спеціального зв'язку та захисту інформації України, - за ч.ч. 4,5 ст.212-5, ст. 212-6 КУпАП.

3. Щодо новел до інформаційного законодавства - пропонується доповнити Закон України «Про інформацію» спеціальним розділом щодо службової та конфіденційної інформації надавши їй законодавче визначення. Для посадових і службових осіб публічних органів, чітко визначивши їх обов'язки щодо зберігання, недопущення витоку, обмежень повторного використання зазначеної інформації (у тому числі після звільнення).

4. Відносно розвитку інституту дисциплінарної відповідальності - варто сформулювати в його межах окремих підінститут інформаційної дисциплінарної відповідальності, що базується на особливому режимі службової інформації, встановлює стандарти обов'язкової поведінки й передбачає спеціальні види стягнень (обмеження доступу, тимчасове блокування акаунтів, тимчасову заборону виконання повноважень) без автоматичного застосування звільнення.

5. Запровадження системи обліку повторності інформаційних проступків. Офіційне запровадження механізму ескалації стягнень залежно від кількості та характеру порушень (перше – зауваження, друге – догана або обмеження доступу, третє – довгострокова заборона або звільнення) має бути відображене у Дисциплінарному статуті, КУпАП і відомчих інструкціях через ведення реєстру порушень.

6. Правове визначення мінімального технічного профілю безпеки - доцільно ухвалити рамковий урядовий акт, що встановить для всіх органів публічної влади обов'язкові мінімальні вимоги до кібербезпеки (багатофакторна автентифікація, централізоване журналювання, шифрування, сегментація доступу, резервування та перевірка відновлення, періодичний аудит), які відомчі акти прокуратури деталізують з урахуванням власної специфіки.

7. Проведення заходів з уніфікації документування інцидентів – це запровадження стандартизованих форм фіксації інцидентів (акт, чек-лист дій, технічний звіт, матриця впливу) і єдиного таймлайна реагування (24 години –

повідомлення, 72 години – первинний звіт, 10 днів – фінальний висновок) забезпечить порівнюваність практики між регіонами, зменшить ризики процесуальних помилок і створить спільний «мовний код» для ІТ-фахівців, юристів і керівництва.

8. Щорічне здійснення підвищення кваліфікації з інформаційної безпеки – у формі теоретичного тестування та практичних кейсів, які пов’язані з користуванням і збереженням доступу до інформаційних систем.

У сукупності запропоновані напрями вдосконалення законодавчої бази з інформаційно-правового забезпечення діяльності органів прокуратури мають формувати сучасну систему інформаційної безпеки, чітку ієрархію відповідальності, належні гарантії конфіденційності даних, узгодженість із міжнародними стандартами та стали практику коректного поводження з інформацією в органах прокуратури [153, с. 382-385].

3.4. Особливості юридичної відповідальності суб’єктів інформаційно-правового забезпечення діяльності органів прокуратури України

У сучасних умовах, коли інформація перетворилася на ключовий ресурс держави й суспільства, суттєво зростає значення юридичної відповідальності у сфері інформаційно-правових відносин. Особливе значення це питання набуває в діяльності органів прокуратури, де інформаційно-правове забезпечення охоплює доступ до публічної інформації, захист персональних даних, обіг службових відомостей тощо. Забезпечення інформаційної безпеки й правового режиму інформації вимагає високих стандартів відповідальності за порушення у цій сфері.

Юридична відповідальність у сфері інформаційних відносин є державно-примусовою реакцією на протиправну поведінку, що порушує встановлений порядок обігу інформації. Вона виконує каральну, відновлювальну, превентивну й виховну функції, але в умовах цифровізації має власні специфічні риси. Йдеться про порушення, пов’язані з несанкціонованим доступом до баз даних, витоками інформації, порушенням режимів її захисту [154, с. 79].

Термін «інформаційно-правова відповідальність» розглядається як самостійний різновид юридичної відповідальності, що формується на перетині правового регулювання та цифрових технологій. Вона характеризується специфічним об'єктом (інформація, інформаційні відносини, інформаційні системи), залежністю від технологічного середовища, високим динамізмом порушень та суспільною значущістю наслідків [155, с. 88].

Основними складовими інформаційно-правової відповідальності є: 1) Підстава відповідальності - це протиправна дія або бездіяльність, що спричиняє шкоду інформаційним правам або ресурсам. Наприклад: незаконне розголошення службової інформації чи порушення порядку обробки персональних даних [156, с. 44]; 2) Умови застосування – це наявність норми, яка встановлює відповідальність, вина суб'єкта, причинно-наслідковий зв'язок між діями та шкодою. У сфері інформації ці умови ускладнені технологічними чинниками та складністю доведення порушення; 3) Ефект відповідальності - це наслідки у вигляді санкцій (штраф, обмеження доступу, дисциплінарні заходи). Можливе застосування заборони на доступ до службової інформації або відключення від інформаційної системи [157, с. 83].

Специфіка відповідальності суб'єктів інформаційно-правового забезпечення органів прокуратури зумовлена такими особливостями: 1) Технологічна динаміка - це стрімкий розвиток ІТ спричиняє появу нових правопорушень, складність їх виявлення та ідентифікації винних; 2) Мультигалузевість - це інформаційні делікти охоплюють сфери адміністративного, дисциплінарного, кримінального та цивільного права; 3) Превентивний характер – це адміністративно-правові заходи (попередження, штраф, обмеження доступу) слугують інструментом упередження правопорушень і є засобом управління ризиками; 4) Баланс публічності та безпеки - відповідальність охоплює як порушення права на доступ до публічної інформації, так і загрози інформаційній безпеці.

На сьогоднішній день на нормативному рівні Дисциплінарний статут прокуратури України (Постанова Верховної Ради № 1796-ХІІ від 06.11.1991)

формально визначає підстави дисциплінарної відповідальності, але не адаптований до викликів цифрового середовища. Він не містить положень щодо специфіки правопорушень у сфері електронного документообігу, ведення ЄРДР, роботи з персональними даними чи дотримання режимно-секретних вимог. Внаслідок цього спостерігається розрив між актуальними цифровими ризиками та наявним регулюванням дисциплінарної відповідальності в органах прокуратури [158].

На практиці інформаційно-правове забезпечення прокуратури охоплює всі етапи обігу інформації - від її збору, обробки й передачі до зберігання та захисту. Порушення на будь-якому з цих етапів можуть кваліфікуватися як дисциплінарні проступки, адміністративні або інші правопорушення, що й вимагає чіткого нормативного регулювання [159, с. 93].

У класичному розумінні юридична відповідальність передбачає наявність суб'єкта, об'єкта, підстав настання, санкції (наслідків) та процедури її застосування. Ці елементи повною мірою проявляються й щодо суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури.

Суб'єктами відповідальності є фізичні та юридичні особи, які організують або здійснюють таке забезпечення: працівники органів прокуратури, інформаційні підрозділи, адміністратори баз даних, оператори інформаційних систем, зовнішні підрядники, тобто уповноважені особи, що мають доступ до інформаційних ресурсів і здійснюють з ними юридично значимі дії [23, с. 90].

Об'єктом відповідальності виступають порушення встановлених правил у сфері інформаційно-правового забезпечення: несанкціонований доступ до даних, неналежний захист інформації, порушення порядку її обробки чи передачі, витоки й розголошення службової інформації, недотримання процедур контролю та аудиту інформаційно-аналітичної діяльності.

Підставою відповідальності є протиправна дія чи бездіяльність суб'єкта, на якого покладено обов'язки щодо забезпечення інформаційної діяльності органів прокуратури, що тягне юридично визначені наслідки. Відповідне правове підґрунтя утворюють Дисциплінарний статут прокуратури України,

законодавство про доступ до публічної інформації, захист персональних даних, а також норми, що регулюють роботу інформаційно-аналітичних підрозділів [160, с. 75].

За характером порушень застосовуються дисциплінарна, адміністративна, у певних випадках матеріальна, а за тяжких наслідків – кримінальна відповідальність. Окреме значення має адміністративна відповідальність за порушення інформаційного законодавства, зокрема за незаконне використання інформації, одержаної у зв'язку з виконанням службових повноважень (ст. 172-8 Кодексу України про адміністративні правопорушення) [161].

Таким чином, система юридичної відповідальності у сфері інформаційно-правового забезпечення діяльності органів прокуратури спирається на загальні засади юридичної відповідальності, але водночас формує спеціалізовану підсистему, зумовлену специфікою інформаційних правовідносин.

Також варт о відзначити, що у контексті функціонування органів прокуратури України інформаційно-правове забезпечення поступово набуває рис відносно автономного організаційно-правового напрямку, який перетинається з публічним управлінням, цифровою трансформацією та забезпеченням верховенства права. У цьому вимірі особливого значення набуває теоретико-правове осмислення та структуризація правового статусу суб'єктів інформаційного забезпечення діяльності органів прокуратури як ключового елементу їх функціонального потенціалу та міри юридичної відповідальності.

З урахуванням завдань, закріплених у внутрішніх положеннях і наказах, доцільно розмежовувати загальних і спеціальних суб'єктів інформаційного забезпечення. Загальні суб'єкти – це всі прокурори та державні службовці органів прокуратури, які щоденно створюють, обробляють і використовують інформацію, працюють з відомчими інформаційними системами та несуть персональну відповідальність за коректність і правомірність таких дій. Спеціальні суб'єкти – це працівники підрозділів, на які покладено організацію, адміністрування, методичний супровід і контроль інформаційних систем та діловодства: Департамент інформаційних технологій Офісу Генерального

прокурора, Департамент документального забезпечення, управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи разом із відповідними структурами в обласних прокуратурах [162]. Саме вони формують «ядро» спеціальної інформаційної компетенції та концентрують підвищений обсяг юридичної відповідальності.

Правовий статус загальних суб'єктів ґрунтується на єдності статусу прокурора незалежно від рівня, що в інформаційній площині означає обов'язок правомірно створювати, фіксувати, захищати й передавати дані з дотриманням установлених законом і внутрішніми актами режимів доступу (у т.ч. в електронному документообігу та роботі з державними реєстрами). Для державних службовців органів прокуратури компетенція визначається законодавством про державну службу та внутрішніми положеннями, які деталізують діловодні, архівні, комунікаційні й технічні операції в межах інформаційних систем «СЕД», ІАС «ОСОП» та інших. Невиконання цих обов'язків трансформується у дисциплінарну чи іншу юридичну відповідальність.

Натомість спеціальні суб'єкти мають розширений адміністративно-правовий статус, зокрема: 1) Департамент інформаційних технологій - забезпечує інформатизацію діяльності органів прокуратури, функціонування та захист відомчих інформаційних систем, експлуатацію програмно-апаратних комплексів, мережеву інфраструктуру й електронні довірчі послуги; 2) Департамент документального забезпечення - встановлює єдиний порядок документування управлінської інформації, обліку, зберігання та знищення носіїв, організовує електронний документообіг і взаємодію у системі електронної взаємодії органів влади; 3) Управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи - відповідає за організацію ведення ЄРДР, статистику кримінальної протиправності, інтеграцію Реєстру з іншими державними базами даних і надання відомостей. Ці підрозділи не лише виконують операційні функції, а й установлюють обов'язкові правила для інших, утворюючи центр відповідальності за повноту й достовірність даних,

що безпосередньо впливають на реалізацію прокурорських повноважень.

Адміністративно-правовий статус суб'єктів інформаційно-правового забезпечення нерозривно пов'язаний з режимом функціонування відомчих інформаційних систем – передусім ЄРДР, а також «СЕД», «ОСОП», «Кадри-WEB» тощо. Визначальними елементами є: регламентований доступ на підставі службових ролей, технічний і криптографічний захист (у тому числі в сегменті кваліфікованих електронних довірчих послуг), процедури тестування, впровадження та навчання користувачів, інтеграція з іншими державними реєстрами. На кожному рівні системи (Офіс Генерального прокурора, Спеціалізована антикорупційна прокуратура, обласні й окружні прокуратури) статус конкретизується через внутрішні акти - від нормотворчих і координаційних повноважень Офісу до первинної роботи з даними на окружному рівні.

У свою чергу варто відзначити, що оскільки інформаційно-правове забезпечення реалізується через юридично значущі операції з даними (внесення відомостей до ЄРДР, ведення діловодства, збереження носіїв, оприлюднення відкритих даних, застосування кваліфікованого електронного підпису), то міра юридичної відповідальності органічно впливає з посадових інструкцій, положень про підрозділи, наказів, режимних вимог (державна таємниця, службова інформація, персональні дані) та обов'язків користувача (доступ, збереження ключів, коректність внесення даних, дотримання строків). Для спеціальних суб'єктів підстави відповідальності посилюються їх організаційно-управлінською роллю, вони відповідають не лише за власні дії, а й за методичне керівництво й контроль інформаційних процесів, що запобігає розмиванню відповідальності та забезпечує простежуваність управлінських рішень.

Підсумовуючи, адміністративно-правовий статус суб'єктів інформаційного забезпечення органів прокуратури доцільно розглядати як інтегральну систему чотирьох взаємопов'язаних блоків: 1) норма – зовнішні та внутрішні регулятори, які визначають завдання й процедури; 2) організація – рівні, підрозділи, ролі та підпорядкованість; 3) інформаційно-правові технології – як інструменти захисту

від витоків і зловживань; 4) відповідальність – персоніфікована, організаційна, процедурна та режимна. Інформаційно-правові технології (системи запобігання витокам, шифрування, автентифікація й контроль доступу, моніторинг активності користувачів, політики безпеки) переводять технічні вимоги у площину службових обов'язків і дисциплінарної відповідальності, створюючи прямий зв'язок між обсягом повноважень, ризиками витоку інформації та мірою юридичної відповідальності суб'єктів інформаційно-правового забезпечення органів прокуратури України.

У свою чергу варто відзначити, що юридична відповідальність суб'єктів, які забезпечують інформаційно-правову діяльність органів прокуратури, ґрунтується на комплексі нормативно-правових актів, що визначають їх статус, повноваження, обов'язки та порядок притягнення до відповідальності у разі порушення встановлених вимог.

Базу становить Закон України «Про прокуратуру» № 1697-VII, який визначає систему органів (Офіс Генерального прокурора, обласні, окружні прокуратури, Спеціалізована антикорупційна прокуратура), єдиний статус прокурорів і загальні організаційні засади [13]. Саме в цих інституційних межах конкретизуються повноваження посадових осіб, процедури видання й оприлюднення внутрішніх актів, що слугують передумовою правомірної діяльності та основою для подальшого притягнення до відповідальності у разі відхилення від установлених стандартів.

До зовнішнього регулювання, на яке безпосередньо спираються внутрішні положення та інструкції, належать Кодекс України про адміністративні правопорушення, Кодекс адміністративного судочинства України, Кримінальний процесуальний кодекс України, закони «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про державну таємницю», «Про електронні документи та електронний документообіг». Їх приписи інтегруються у відомчі процедури роботи з ЄРДР, електронним документообігом, кваліфікованими електронними довірчими послугами, захистом інформації, визначаючи допустимі моделі поведінки та

типові порушення.

Важливу роль відіграє Дисциплінарний статут прокуратури України (постанова Верховної Ради України № 1796-XII від 06.11.1991), який задає загальні підстави й процедури дисциплінарної відповідальності, але майже не містить спеціальних складів проступків, пов'язаних із порушенням правил роботи у відомчих інформаційних системах чи режимно-секретних вимог. Тому деталізація відповідальності за такі порушення переноситься у внутрішній блок – систему організаційно-розпорядчих актів Генерального прокурора та керівників нижчих рівнів, що конкретизують завдання, функції, доступ і адміністрування інформаційних систем, правила документообігу та режимної роботи. Саме ці акти виступають безпосередніми «носіями» юридичних обов'язків працівників, а їх невиконання або неналежне виконання формує підставу відповідальності.

У свою чергу, залежно від характеру порушення суб'єкти інформаційно-правового забезпечення діяльності органів прокуратури України можуть нести такі види юридичної відповідальності:

1. Дисциплінарна відповідальність - застосовується за порушення внутрішніх регламентів, наказів і посадових інструкцій щодо роботи з інформацією (неналежне внесення відомостей до ЄРДР, порушення строків і правил реєстрації документів у СЕД, недотримання режимно-секретних вимог, політик доступу, правил використання кваліфікованого електронного підпису тощо). Її підстави випливають із Закону України «Про прокуратуру» та деталізуються у відомчих актах, положеннях про підрозділи й посадових інструкціях [163, с. 11].

2. Адміністративна відповідальність - виникає за порушення загальнообов'язкових правил інформаційної діяльності поза межами внутрішньої підлеглості, зокрема за порушення порядку обліку, зберігання й використання документів та інших носіїв, що містять службову інформацію (ст. 212-5 КУпАП) [161]. Йдеться, наприклад, про неналежну реєстрацію й архівацію документів, неправильне проставлення грифів, самовільне копіювання чи

винесення носіїв. Підстави та межі такої відповідальності визначаються законами про інформацію, державну таємницю, електронні документи та внутрішніми регламентами.

3. Матеріальна відповідальність - настає у разі заподіяння майнової шкоди внаслідок протиправних дій з інформацією (розголошення відомостей з обмеженим доступом, що спричинило збитки; несвоєчасне чи некоректне внесення даних із негативними майновими наслідками). Внутрішні положення й накази фіксують стандарти належної поведінки, які слугують критерієм оцінки професійних дій.

4. Кримінальна відповідальність - пов'язана з найбільш небезпечними порушеннями – незаконним втручанням у роботу інформаційних систем, розголошенням державної таємниці, підробленням електронних підписів/документів тощо (зокрема, ст. 361–364 КК України) [164]. Відомчі акти щодо ЄРДР, СЕД, ІАС «ОСОП», використання КЕП і режимних вимог у цьому разі виконують превентивну та доказову функції, фіксуючи обсяг обов'язків і факт їх порушення.

5. Інформаційно-правова відповідальність - у законодавстві прямо не виокремлена, однак у доктрині описується як міждисциплінарний вид відповідальності, що враховує особливості захисту інформації в цифровому середовищі. У практиці органів прокуратури вона простежується у відносинах між володільцями/розпорядниками службової інформації (Офіс Генерального прокурора, обласні, окружні прокуратури, САП, адміністратори систем) і користувачами; між розпорядниками персональних даних і суб'єктами цих даних; між керівниками та підлеглими, які зобов'язані дотримуватися встановлених режимів доступу, зберігання, передачі й архівації відомостей. Саме в цих «точках дотику» виникають підстави притягнення до відповідальності за порушення внутрішніх регламентів, режимно-секретних вимог, правил роботи з персональними даними та експлуатації ЄРДР/СЕД/ІАС «ОСОП».

У практичному вимірі юридична відповідальність реалізується через внутрішні механізми контролю (щорічні звіти, перевірки, службові

розслідування). Порушення правил збереження конфіденційності чи роботи з реєстрами, особливо за наявності шкідливих наслідків, тягнуть дисциплінарні та інші санкції. Система наказів Генерального прокурора про затвердження положень структурних підрозділів (Департамент інформаційних технологій, Департамент документального забезпечення, управління організаційного забезпечення ЄРДР та інформаційно-аналітичної роботи, режимно-секретні, кадрові, комунікаційні та інші підрозділи) виконує три ключові функції: 1) нормативізує обов'язки щодо роботи з даними; 2) розмежовує повноваження й відповідальність (адміністратор, користувач, контролер, методист); 3) забезпечує контрольованість через звітність, моніторинг, аудит і статистику [165, с. 344-345].

З урахуванням структури компетенцій та технічної організації найвищий ризик утворення деліктів зосереджується у таких сегментах: 1) ЄРДР – несвоєчасне, неповне чи недостовірне внесення відомостей, порушення методики обліку й правил надання інформації, несанкціоновані дії з Реєстром, неналежне адміністрування доступів; 2) СЕД – порушення строків реєстрації та маршрутизації документів, відсутність належної реєстрації, недоліки оформлення, втрата/псування носіїв, порушення правил архівування й знищення; 3) ІАС «ОСОП» і статистика – формування недостовірної або методологічно неправильної статистики, порушення принципу статистичної конфіденційності, відступ від єдиного порядку звітності; 4) КЕП та електронні довірчі послуги – неналежне зберігання особистих ключів, передання засобів підпису іншим особам, використання підпису поза межами повноважень, компрометація ключів; 5) Режимно-секретна діяльність і персональні дані – неправомірний доступ, розголошення, неналежне зберігання носіїв, порушення класифікації й несанкціонований обмін відомостями. У сукупності це свідчить, що доказова база для притягнення суб'єктів інформаційно-правового забезпечення до юридичної відповідальності формується переважно зсередини, через журналювання операцій у ЄРДР, СЕД, аналітичних системах, офіційне оприлюднення наказів, документовані регламенти доступів і процедурні карти

процесів, які фіксують як належні, так і протиправні моделі поведінки.

З огляду на викладене, можна впевнено стверджувати, що загальні суб'єкти прокурори та державні службовці, несуть відповідальність за повноту, достовірність, своєчасність та правомірність інформаційних операцій: від внесення даних у Єдиний реєстр досудових розслідувань (ЄРДР) до реєстрації документів у системі електронного документообігу (СЕД) і ведення статистики в інформаційно-аналітичній системі «ОСОП». Незалежно від адміністративної посади, вони діють у межах єдиного правового статусу прокурора й підпорядковуються внутрішнім нормативно-правовим актам.

Натомість спеціальні суб'єкти додатково відповідають за організаційно-методичне керівництво, включаючи: впровадження інформаційних систем, адміністрування доступу, захист інформації (включаючи криптографічні методи), інтеграцію з державними реєстрами, відповідність звітності європейським стандартам, забезпечення роботи центрів обробки даних та каналів зв'язку, а також відкритість даних. Обсяг їхньої відповідальності включає організаційний компонент - за архітектуру, стабільність і контроль інформаційних процесів.

Ключовими процесуальними гарантіями інформаційної відповідальності є: регламентований доступ до ЄРДР, системи логування дій, правила опрацювання звітності в ІАС «ОСОП», вимоги до зберігання носіїв, політики щодо кваліфікованого електронного підпису (КЕП), порядок набрання чинності наказами. Усі ці елементи слугують інструментами превенції та доказовою базою у справах про юридичну відповідальність, забезпечують перевірюваність і відтворюваність дій, що є ознаками належного публічного управління.

Виходячи із цього ми з упевненістю можемо визначити, що юридична відповідальність суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури - це закріплений у законодавстві та внутрішньому регламенті інститут державного примусу, що передбачає застосування до відповідальних осіб (прокурорів, держслужбовців, технічного персоналу) санкцій адміністративного, дисциплінарного, матеріального або кримінального

характеру у разі порушення норм щодо обігу інформації, доступу до інформації, експлуатації інформаційних систем чи захисту службової й персональної інформації. Її мета, це забезпечити законність, ефективне функціонування цифрової інфраструктури прокуратури та підтримання інформаційної безпеки у межах виконання повноважень.

Розгляд особливостей юридичної відповідальності в інформаційно-правовій сфері органів прокуратури був би неповним без аналізу судової та дисциплінарної практики. Такі кейси розгортаються в межах трьох правових режимів: доступу до публічної інформації, захисту таємниці досудового розслідування, а також персоніфікованої відповідальності працівників прокуратури. Для їх правової оцінки доцільним є застосування критеріального підходу: визначення правового статусу інформації; наявність «трискладового тесту» (законність, легітимна мета, пропорційність); технічна фіксація дій; індивідуалізація відповідальності.

Так, у справі № 101393078/2021 (Одеський окружний адміністративний суд, 26.11.2021) суд визнав протиправною відмову прокуратури надати копію розпорядчого акту, посилаючись на те, що документ уже існував, не підпадав під таємницю слідства і мав розглядатися як публічна інформація. Встановлено порушення норм Закону України «Про доступ до публічної інформації» та недотримання обов'язку вмотивованої відповіді [166].

У рішенні № 640/7688/21 від 21.03.2024 суд розглядав відмову у наданні інформації з ЄРДР. Хоча відповідач обґрунтовував відмову таємницею досудового розслідування (ст. 222 КПК України), суд наголосив, що обмеження мають бути конкретизованими й пропорційними, а не автоматичними [167].

Значущим є і дисциплінарний кейс КДКП щодо прокурора Бадіона М.О., який, за даними службового розслідування, допустив витік інформації під час НСРД. За результатами технічної ідентифікації було встановлено його причетність, що стало підставою для звільнення. Хоча дисциплінарна відповідальність застосована, судово підтвердження рішення станом на дату огляду не знайдено [168].

Ще один приклад - це справа про відмову Запорізької обласної прокуратури в наданні інформації на адвокатський запит. Суд визнав таку відмову неправомірною, оскільки вона не відповідала критеріям законності, мети та необхідності, а частковий доступ не був наданий, попри наявність відповідних процесуальних інструментів [169].

Стабільну позицію щодо умов обмеження доступу до інформації займає Конституційний Суд України, який наголошує: це право не є абсолютним, але обмеження мають відповідати вимогам закону, легітимної мети та необхідності [170].

Таким чином, судова практика, виконує не лише індикативну функцію для правозастосування, а й виявляє структурні проблеми: прогалини у правовому регулюванні, конкуренцію норм процесуального й інформаційного права, проблеми в належному інформуванні та фіксації службових дій. У межах діяльності органів прокуратури це особливо актуально, адже від прозорості рішень, дотримання регламентів і правового режиму обігу інформації залежить як ефективність правозастосування, так і дисциплінарна та адміністративна відповідальність службових осіб.

Узагальнюючи викладене, слід підкреслити, що особливості юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України зумовлені поєднанням їхнього єдиного публічно-правового статусу, високого рівня довіри до інституції прокуратури та цифрово-технологічного характеру сучасних інформаційних процесів. Загальні суб'єкти (прокурори, державні службовці) несуть персональну відповідальність за коректність, повноту, своєчасність і правомірність операцій з даними в ЄРДР, СЕД, ІАС «ОСОП» та інших системах, тоді як спеціальні суб'єкти додатково відповідають за організацію, адміністрування й контроль інформаційної інфраструктури, що посилює їхній організаційно-правовий вимір відповідальності. Комплекс зовнішніх (закони про прокуратуру, інформацію, доступ, персональні дані, державну таємницю, електронні документи, КК, КУпАП) та внутрішніх (накази, положення, інструкції) регуляторів формує

нормативну основу для застосування дисциплінарних, адміністративних, матеріальних і кримінально-правових санкцій, а вбудовані у відомчі системи механізми журналювання, регламентованого доступу, використання КЕП і процедурного контролю забезпечують доказовість та індивідуалізацію відповідальності. У підсумку юридична відповідальність у цій сфері постає не лише як каральний інститут, а як системний інструмент підтримання законності, належного функціонування інформаційної інфраструктури органів прокуратури та стійкості інформаційної безпеки в умовах зростання обсягів і чутливості оброблюваних даних.

Висновки до розділу 3

1. Порівняльний аналіз досвіду Франції та Польщі засвідчує наявність двох працездатних, але концептуально різних моделей інформаційно-правового забезпечення прокуратури – процесно-орієнтованої (з акцентом на єдині цифрові платформи кримінальної юстиції) та реєстрово-сервісної (з акцентом на уніфіковані реєстри, відкриті дані й формалізовані канали комунікації «запит – відповідь»). Для України перспективною є синтетична модель, що поєднує «наскрізну» цифрову платформу правосуддя з розгалуженою системою публічних та відомчих реєстрів, адаптованих до особливостей конституційно-правового статусу органів прокуратури, структури публічної адміністрації та фактичного рівня цифрової інфраструктури.

2. Перспективи формування інформаційно-правових технологій у діяльності органів прокуратури України мають комплексний характер і охоплюють право, організацію, техніку, кадри та міжнародну взаємодію. Нормативний пріоритет - це систематизація та гармонізація з європейськими стандартами, включно з режимами обміну даними, кібербезпекою та е-правосуддям. Організаційно ключовими є посилення аналітики (Big Data, AI), розгортання е-документообігу й сервісів на кшталт «розподіленого офісу». Технічно потрібні модернізація IT-інфраструктури й зрілі практики інформаційної безпеки. Кадровий вимір передбачає безперервне навчання та

міждисциплінарну підготовку. Необхідно чітко визначити функції, права й відповідальність суб'єктів та розвивати партнерства з державними, міжнародними й громадськими структурами. В умовах воєнного стану та відновлення пріоритетами є стійкість, безперервність, захищені віддалені доступи й електронні репозиторії доказів, що разом веде до інтегрованої цифрової екосистеми прокуратури.

3. Запропоновані напрями вдосконалення та внесення змін до законодавчої бази (Дисциплінарний статут прокуратури України, КУпАП тощо), що виводять на формування сучасної системи інформаційної безпеки органів прокуратури, у межах якої вибудовується чітка ієрархія режимів доступу та рівнів захисту даних. Йдеться про узгодження конституційних, законодавчих і підзаконних актів із міжнародними стандартами захисту персональних даних, кібербезпеки, електронного правосуддя, деталізацію вимог до внутрішніх регламентів, типових положень, інструкцій та цифрових політик, що регулюють роботу з інформаційними ресурсами прокуратури.

4. Обґрунтовано розуміння юридичної відповідальності не лише як карального механізму, а як ключового елементу превентивної та комплаєнс-орієнтованої політики в органах прокуратури. Регулярне підвищення кваліфікації, цільова атестація щодо знань інформаційної безпеки й цифрових регламентів, пов'язання доступу до інформаційних систем із результатами такого оцінювання, а також можливість тимчасового обмеження доступу у разі порушення вимог формують дієвий механізм внутрішнього самоконтролю.

5. Інститут юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України постає як комплексний механізм, що поєднує дисциплінарні, адміністративні та інші заходи впливу за порушення правових режимів інформації (службової, персональної, процесуальної, оперативної, таємниці досудового розслідування). Удосконалення цього інституту передбачає деталізацію складів правопорушень у КУпАП і спеціальному законодавстві, корекцію відомчих актів.

ВИСНОВКИ

У дисертації здійснено комплексне теоретико-прикладне адміністративно-правове дослідження інформаційно-правового забезпечення діяльності органів прокуратури України в умовах становлення інформаційного суспільства та цифрової трансформації публічного управління, з'ясовано сутність, зміст та генезис інформаційно-правового забезпечення прокурорської діяльності, визначено його мету, принципи та завдання, розкрити структуру й особливості нормативно-правових засад, а також виробити цілісну систему практико-орієнтованих пропозицій щодо вдосконалення законодавчої бази та юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України. За результатами дослідження сформульовано такі основні висновки:

1. На підставі комплексного теоретико-правового аналізу визначено сутність та особливості інформаційно-правового забезпечення діяльності органів прокуратури України як нормативно врегульованої, інституційно організованої та процесуально визначеної системи засобів, способів і механізмів адміністративно-правового впливу, спрямованих на формування, отримання, оброблення, зберігання, використання, обмін та захист інформації, необхідної для реалізації функцій прокуратури. Визначено еволюційний характер становлення інформаційно-правового забезпечення у системі публічного управління України, виділивши чотири етапи: радянський, пострадянський, нормативно-інституційний та цифровий. Радянський етап характеризувався жорстким централізованим контролем, репресивним підходом до інформації, фрагментарним підзаконним регулюванням та відсутністю конституційно закріпленого права на інформацію, що зумовлювало закритість інформаційних потоків. Пострадянський етап пов'язаний із формуванням інформаційного суверенітету: прийняття Конституції України та Закону «Про інформацію» заклало правові засади права на доступ до інформації й базового понятійного апарату, однак механізми практичного адміністрування інформаційних процесів залишалися переважно декларативними. На нормативно-інституційному етапі, у

зв'язку з прийняттям спеціальних законів про захист персональних даних, доступ до публічної інформації та оновленої редакції Закону «Про інформацію», інформаційно-правове забезпечення набуло системного характеру, було інтегровано в управлінський процес через інструменти прозорості, відкритих даних та електронного документообігу. Цифровий етап ознаменував перехід до цілісної моделі цифрового адміністрування, у межах якої інформаційно-правове забезпечення пов'язується з розвитком електронних сервісів, формуванням механізмів «цифрової довіри», гармонізацією з європейськими стандартами, зокрема: (GDPR - General Data Protection Regulation, Загальний регламент про захист даних), (NIS2 – директива Європейського Союзу, яка встановлює більш суворі вимоги до кібербезпеки) та інституціоналізацією кібербезпеки, що свідчить про трансформацію інформації з об'єкта контролю на ключовий ресурс сучасного публічного управління.

2. Установлено, що категорії «мета», «принцип» і «завдання» утворюють внутрішньо узгоджену систему, яка визначає зміст та спрямованість адміністративно-правового режиму інформаційної діяльності органів прокуратури. Мета інформаційно-правового забезпечення у цьому контексті полягає у створенні таких правових, організаційних, технічних та інституційних умов, за яких стає можливим належне виконання конституційно визначених функцій прокуратури (підтримання державного обвинувачення, представництво інтересів держави, нагляд за досудовим розслідуванням). Принципи виступають обов'язковими орієнтирами досягнення цієї мети (законність, відкритість у межах закону, достовірність, пропорційність обмежень, належна обробка персональних даних відповідно до національних норм і стандартів GDPR), тоді як завдання конкретизуються у вигляді процедур та регламентів (реєстрація, оприлюднення, обмеження доступу, облік запитів, функціонування реєстрів, електронні форми взаємодії), зміст яких додатково деталізовано Законом України «Про адміністративну процедуру». Доведено, що саме їх узгоджена взаємодія забезпечує цілісність адміністративно-правового режиму функціонування прокуратури в інформаційній сфері, тоді як порушення будь-

якого з елементів призводить до деформації цього режиму – від неправомірного обмеження доступу до інформації до неналежної обробки персональних даних.

3. З'ясовано, що система нормативно-правових актів, яка визначає засади інформаційно-правового забезпечення діяльності органів прокуратури України, має багаторівневий і міжгалузевий характер та виступає важливим чинником інституційної спроможності прокуратури в сучасному демократичному правопорядку. Вона формується на конституційному рівні (норми Конституції України щодо права на інформацію, організації публічної влади й верховенства права), законодавчому рівні (загальне інформаційне законодавство, спеціальні акти про прокуратуру, кримінальний процес, національну безпеку й державну таємницю), підзаконному рівні (накази Офісу Генерального прокурора та інші відомчі документи щодо електронного документообігу, діловодства, зберігання, архівування й обміну даними) та міжнародно-правовому рівні (акти й стандарти Ради Європи та ЄС у сфері доступу до інформації, захисту персональних даних, прозорості й підзвітності прокуратури). Доведено, що ця система не є набором ізольованих актів, а функціонує як цілісна правова архітектура, що регулює інформаційне адміністрування, захист даних і публічну відкритість діяльності прокуратури, водночас потребує подальшої систематизації, цифрової модернізації та адаптації до європейських стандартів із урахуванням балансу між відкритістю, правами громадян і необхідною конфіденційністю.

4. Установлено, що класифікація видів інформаційно-правового забезпечення діяльності органів прокуратури України має багатовимірний характер і є ключовим методологічним інструментом побудови цілісної моделі прокурорської діяльності в умовах інформатизації. Обґрунтовано доцільність її побудови за системою взаємопов'язаних критеріїв: за функціональним призначенням (процесуальне, організаційно-управлінське, комунікаційне, безпекове забезпечення та їх підвиди), за джерелом і походженням інформації (внутрішньоорганізаційне, міжвідомче, зовнішнє), за правовим режимом і рівнем доступу (публічна інформація, інформація з обмеженим доступом, таємна інформація), а також за формою реалізації та ступенем стандартизації (паперове

й електронне, стандартизоване й нестандартизоване забезпечення. Доведено, що кожен із виділених видів має бути підкріплений відповідним нормативним регулюванням, організаційними процедурами, технічними рішеннями й механізмами відповідальності, а запропонована класифікація не лише усуває фрагментарність правового регулювання інформаційної діяльності прокуратури, але й виконує нормативно-проектну функцію, слугуючи концептуальним каркасом подальшого вдосконалення законодавства та відомчих актів у сфері інформаційно-правового забезпечення.

5. Виявлено, що інформаційно-правове забезпечення діяльності органів прокуратури України має чітко виражену багаторівневу структуру, яка охоплює нормативно-правовий, інституційний, організаційно-процесуальний, інфраструктурно-технологічний та індивідуально-посадовий рівні. Нормативно-правовий рівень формує базові правила функціонування інформаційної сфери прокуратури, інституційний – задає організаційний каркас реалізації інформаційної політики, організаційно-процесуальний – забезпечує формалізацію та відтворюваність інформаційних процедур, інфраструктурно-технологічний – надає технічні інструменти обробки й аналізу даних, тоді як індивідуально-посадовий рівень персоніфікує відповідальність за дотримання інформаційних режимів через статус, компетентність та етичні стандарти прокурорів. Їх взаємозв'язок утворює цілісний контур адміністративно-правового впливу, без якого неможливе ефективне функціонування органів прокуратури в умовах цифрової трансформації. Доведено, що основні напрями інформаційно-правового забезпечення діяльності прокуратури доцільно розглядати як системно впорядковані вектори використання інформації: процесуально-інформаційний, організаційно-управлінський, комунікаційно-прозорий, аналітико-прогнозний, інформаційно-безпековий, міжвідомчий та міжнародний (інтеграційний). Кожен із них відображає окремий аспект реалізації публічно-владних повноважень прокуратури – від забезпечення кримінального провадження та внутрішнього управління до відкритості, аналітичного супроводу публічної політики, захисту інформації та інтеграції в

європейський правовий простір. Сукупність визначених рівнів і напрямів формує концептуальну рамку подальшого вдосконалення законодавства й відомчих актів у сфері інформаційно-правового забезпечення діяльності органів прокуратури України.

6. Здійснено комплексне теоретико-правове узагальнення та нове вирішення наукового завдання щодо визначення сутності, структури та функціонального призначення адміністративно-правових форм і методів інформаційно-правового забезпечення діяльності органів прокуратури України в умовах цифрової трансформації публічного управління та європейської інтеграції. Доведено, що адміністративно-правові форми виступають зовнішньо-юридичними способами об'єктивації інформаційної діяльності органів прокуратури, тоді як методи відображають внутрішню динаміку владно-організуючого впливу на інформаційні відносини, а їх єдність формує цілісний інструментарій публічного адміністрування в інформаційній сфері.

У роботі сформовано розгорнуту класифікацію адміністративно-правових форм інформаційно-правового забезпечення діяльності органів прокуратури, що дозволило розкрити багатовимірність зовнішніх проявів інформаційної діяльності прокуратури та їх зв'язок із реалізацією процесуальних, управлінських, аналітичних і комунікаційних функцій. Водночас систематизовано основні адміністративно-правові методи в досліджуваній сфері (регулятивно-нормувальні, координаційно-організаційні, інформаційно-аналітичні, переконання і формування інформаційної культури, контрольні та наглядові, стимулюючі, примусові, інноваційно-цифрові), завдяки чому розкрито внутрішні механізми управління інформаційними потоками, режимами доступу та інформаційною безпекою.

Доведено, що саме через взаємодію форм і методів забезпечуються юридична визначеність інформаційних процедур, можливість контролю та оскарження рішень, дотримання прав людини на доступ до інформації й захист персональних даних, а також інтеграція діяльності прокуратури в єдиний цифровий простір публічного управління. Показано, що адміністративно-правові

форми й методи виконують гарантійну, організаційну, безпекову, аналітико-прогнозну та інтеграційну функції, забезпечуючи баланс між відкритістю прокуратури та охороною інформації з обмеженим доступом.

7. Проведений аналіз дає підстави стверджувати, що система органів прокуратури України становить ієрархічно організовану сукупність суб'єктів інформаційно-правового забезпечення, у межах якої кожна ланка має власний адміністративно-правовий статус і чітко окреслену роль у формуванні та реалізації єдиної інформаційної політики. Офіс Генерального прокурора виступає системним «ядром» механізму інформаційно-правового забезпечення, де зосереджено нормотворче та організаційно-управлінське керівництво, адміністрування ключових інформаційних систем і стандартизація електронного документообігу та захисту даних. Спеціалізована антикорупційна прокуратура, будучи юридичною особою публічного права, поєднує включеність до єдиної системи з високим рівнем інституційної автономії, самостійно організовуючи документообіг, режимно-секретну роботу й внутрішній контроль в антикорупційній сфері. Обласні прокуратури виконують роль регіональних центрів імплементації загальної політики та координаторів інформаційних процесів окружної ланки, тоді як окружні прокуратури формують «операційний контур» механізму, перетворюючи норми та відомчі регламенти на щоденні інформаційні процедури реєстрації, обігу, аналізу й захисту даних. У своїй сукупності ці елементи забезпечують цілісність, керованість і функціональну ефективність інформаційно-правового режиму в органах прокуратури України.

8. Узагальнення проведеного порівняльного аналізу дає підстави стверджувати, що французька та польська моделі інформаційно-правового забезпечення діяльності органів прокуратури формують цінний орієнтир для вітчизняної правової доктрини та практики. У Франції прокурор інституційно інтегрований у режим обробки персональних даних і функціонування єдиних цифрових платформ (зокрема CASSIOPEE) за умов поєднання автоматизації з відкритістю (open data судових рішень) та високими стандартами захисту приватності. Польська модель демонструє ефективність ієрархічно організованої

прокуратури в поєднанні з уніфікованими реєстрами (KPK/e-KPK) і загальними правилами доступу до публічної інформації (UDiP/BiP), посилені участю в екосистемі правосуддя ЄС. На цьому підґрунті обґрунтовано доцільність для України поетапного формування «дорожньої карти» цифрової модернізації прокуратури, що має включати створення спеціалізованого цифрового агентства, законодавче закріплення принципів електронної публічності й відкритих даних, розроблення інтегрованої платформи «прокуратура – поліція – суд», посилення кібербезпеки та розвиток публічної звітності й аналітики. Водночас наголошено на необхідності адаптації зазначених підходів до національних правових, організаційних та ресурсних умов, що має забезпечити збалансований розвиток інформаційно-правового забезпечення органів прокуратури України.

9. Перспективи формування інформаційно-правових технологій у діяльності органів прокуратури України мають комплексний характер і охоплюють, насамперед: подальше вдосконалення та систематизацію нормативної бази інформатизації з урахуванням європейських стандартів захисту персональних даних, відкритості державних інформаційних ресурсів і міжнародно-правових підходів до кібербезпеки та електронного правосуддя; організаційно-управлінську перебудову прокуратури через формування спеціалізованих підрозділів (ІТ, аналітики, безпеки, електронного документообігу), розвиток інформаційно-аналітичної діяльності, запровадження повноцінного електронного документообігу й єдиної корпоративної інформаційної системи, інтегрованої з державними реєстрами та системами е-правосуддя; технічну модернізацію ІТ-інфраструктури з упровадженням аналітичних платформ, інструментів роботи з великими даними та механізмів комплексного кіберзахисту; кадрово-освітній розвиток через підготовку фахівців із поєднанням юридичної та цифрової компетентності, підвищення кваліфікації працівників і формування високої інформаційної культури та етичних стандартів роботи з даними; уточнення правового статусу інформаційно-правових технологій та зміцнення міжвідомчої й міжнародної взаємодії в інформаційній сфері. Окремо наголошено на необхідності адаптації

таких технологій до умов воєнного стану та подальшої післявоєнної трансформації через забезпечення мобільності, стійкості й безперервності інформаційних процесів, створення резервних та автономних систем і майбутнє цифрове відновлення, включно з електронними архівами та єдиними репозиторіями доказів воєнних злочинів, що в цілому визначає стратегічний вектор модернізації інформаційно-правового забезпечення органів прокуратури України.

10. Доведено, що подолання прогалин інформаційно-правового забезпечення діяльності органів прокуратури можливе лише через цілеспрямоване оновлення профільних актів. Автором розроблено проєкт Закону України Про внесення змін до «Дисциплінарного статуту прокуратури України», який передбачає запровадження нового розділу IV про інформаційні дисциплінарні проступки (з визначенням їх поняття, типології та категорій тяжкості, процедур фіксації й доказування інцидентів), а також доповнення ст. 9 Статуту новим видом дисциплінарного стягнення – тимчасовою заборонаю доступу до службової інформації з ескалаційною шкалою стягнень залежно від повторності й наслідків порушення. Конкретизовано зміни до Кодексу України про адміністративні правопорушення: запровадження додаткового стягнення у вигляді позбавлення спеціального права доступу до інформаційних (автоматизованих) систем (доповнення ст. 24, введення ст. 32-2 з легальними дефініціями та визначенням кола суб'єктів і строків), доповнення ст. 212-5 частинами 3–5 щодо порушень ведення ЄРДР, ст. 212-6 – частиною 7 щодо компрометації особистих ключів, а також уведення приміток із визначеннями «реєстратора», «користувача» та «інформаційних (автоматизованих) систем» і розширення повноважень Державної служби спеціального зв'язку та захисту інформації України (ст. 255 КУпАП). У поєднанні з новелами до Закону України «Про інформацію» (розділ про службову та конфіденційну інформацію), формуванням підінституту інформаційної дисциплінарної відповідальності й веденням реєстру повторності проступків ці пропозиції утворюють цілісну авторську модель посилення режиму обігу службових даних, невідворотності

відповідальності та стійкого функціонування цифрової інфраструктури органів прокуратури України.

11. Узагальнення нормативних і відомчих приписів дає змогу стверджувати, що юридична відповідальність суб'єктів інформаційно-правового забезпечення органів прокуратури України має комплексний характер і реалізується через сукупність дисциплінарних, адміністративних, матеріальних і кримінальних санкцій, доповнених доктринально окресленою інформаційно-правовою відповідальністю. Дисциплінарні механізми забезпечують реагування на порушення внутрішніх регламентів роботи з ЄРДР, СЕД, ІАС «ОСОП», КЕП та режимно-секретною інформацією, тоді як адміністративні й кримінально-правові норми охоплюють більш небезпечні делікти, пов'язані з порушенням загальних правил інформаційної діяльності й функціонуванням автоматизованих систем. Фокус ризиків у сегментах реєстрів, електронного документообігу, статистики, електронного підпису та захисту персональних і секретних даних зумовлює те, що доказова база відповідальності формується переважно внутрішніми засобами – через журналювання операцій, регламентацію доступів і формалізовані процедури контролю, які перетворюють інформаційно-правовий режим на дієвий інструмент персоніфікації відповідальності в системі прокуратури.

СПИСОК ЛІТЕРАТУРИ

1. Гайдай С. Інформатизація прокурорської діяльності: теоретико-правові засади. *Актуальні проблеми правознавства*. 2019. № 1 (17). С. 120–125. URL: <https://appj.wunu.edu.ua/index.php/appj/article/view/626>

2. Мазурик С. Поняття інформаційного забезпечення та класифікація інформації в прокурорській діяльності. *Актуальні проблеми правознавства*. 2016. № 3 (7). С. 30-34. URL: <https://appj.wunu.edu.ua/index.php/appj/article/view/74/74>

3. Lesko N. Modern information technologies in the activities of prosecutor's offices. *Visnik Nacional'nogo universitetu «Lvivska politehnika»*. Seria: Uridicni nauki. 2022. Vol. 9. no. 35. P. 155–160. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2022/dec/29222/23.pdf>

4. Білозьорова Л. В. Деякі питання щодо особливостей інформаційно-правового забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2023. № 5. С. 513-522. URL: http://pravoisuspilstvo.org.ua/archive/2023/5_2023/74.pdf

5. 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>

6. Про інформацію : Закон України від 02.10.1992 № 2657-ХІІ : перша редакція. URL: <https://zakon.rada.gov.ua/laws/show/2657-12/ed19921002#Text>

7. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : перша редакція. URL: <https://zakon.rada.gov.ua/laws/show/2297-17/ed20100601#Text>

8. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : перша редакція. URL: <https://zakon.rada.gov.ua/laws/show/2939-17/ed20110113#Text>

9. Про інформацію : Закон України від 02.10.1992 № 2657-ХІІ : станом на 09 вер. 2011 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12/ed20110509#Text>

10. Міністерство цифрової трансформації України. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Міністерство_цифрової_трансформації_України

11. Українці найбільше довіряють програмі «Держава у смартфоні» та цифровізації – опитування «Рейтинг». Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/news/technologies/ukraintsi-naybilshe-doviryayut-programi-derzhava-u-smartfoni-ta-tsifrovizatsii-opituvannya-reyting>
12. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР : станом на 31 груд. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/393/96-вр#Text>
13. 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>
14. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 1 серп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
15. Терещук Г. А., Мазурик С. В. Інформаційна безпека органів прокуратури: питання організаційно-правового забезпечення. *Соціологія права*. 2017. № 3-4. С. 107-115. URL: <http://soclaw.idpnan.kyiv.ua/archive/2017/3-4/21.pdf>
16. Про затвердження Порядків обробки персональних даних в органах прокуратури України : Наказ Генерального прокуратура України від 26 липня 2014 року № 77. URL: https://old.gp.gov.ua/ua/personal_data_protection
17. Про затвердження Переліку відомостей, що становлять службову інформацію та можуть міститися в документах органів прокуратури України : Наказ Офісу Ген. прокурора від 09.12.2020 № 578 : станом на 26 листоп. 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/v0578905-20#Text>
18. Малетова О., Глущенко А. Правове регулювання інформаційного обміну між державними інституціями в умовах воєнного стану: виклики та перспективи. Науковий вісник Ужгородського Національного Університету. 2025. Т. 3, № 90. С. 309–316. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/47-2.pdf>
19. Звіт оцінки. Зовнішня незалежна оцінка ефективності діяльності національного агентства з питань запобігання корупції. URL:

<https://www.kmu.gov.ua/storage/app/sites/1/perevirka%20NAZK/zvit-komisiyi-z-provedennia-nezaleznoi-otsinky-efektyvnosti-diialnosti-nazk.pdf>

20. Загальна теорія держави і права : підручник / за ред. М. В. Цвіка, О. В. Петришина. Харків : Право, 2009. 584 с. URL: https://shron1.chtyvo.org.ua/Tsvik_Marko/Zahalna_teoriiia_derzhavy_i_prava.pdf

21. Regulation - 2016/679 - EN - gdpr - EUR-Lex. EUR-Lex. Access to European Union law – choose your language. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

22. Про адміністративну процедуру : Закон України від 17.02.2022 № 2073-IX : станом на 15 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2073-20#Text>

23. 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>

24. Принципи адміністративного права. Академія адміністративно-правових наук. Науково-дослідний інститут публічного права. URL: <https://www.ssaals.com.ua/pravo/pryntsy-py-administratyvnoho-prava/1517/>

25. Принципи адміністративного права: лекція для студентів 2 курсу доктора юридичних наук, професора, голови Академії адміністративно-правових наук Валентина Галуцько. Академія адміністративно-правових наук. Науково-дослідний інститут публічного права. URL: <https://www.ssaals.com.ua/pravo/pryntsy-py-administratyvnoho-prava-le/6628/>

26. Лушер В.В. Поняття інформаційного забезпечення органів прокуратури України. Форум права. 2014. № 1. С. 338–341. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=FP_index.htm_2014_1_59

27. Банах С. В. Міжнародні стандарти організації та управління в органах прокуратури. Наукові записки. Серія: Право. 2020. № 8. С. 140–148. URL: https://cusu.edu.ua/images/nauk_zapiski/pravo/8_2020/випуск_8_2020-140-148.pdf
28. Гаврюшенко Г. В. Організаційно-правові засади забезпечення транспарентності прокурорської діяльності: автореф. дис. ... канд. юрид. наук: 12.00.10. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2015. 20 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/10538/1/Gavryushenko_G_V_2015.pdf
29. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII : станом на 31 груд. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231>
30. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV : станом на 31 груд. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>
31. 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>
32. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 8 серп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
33. 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>
34. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 31 берез. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19/ed20230331#Text>
35. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII : станом на 16 груд. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/3855-12/ed20231216>

36. Наказ Генеральної прокуратури України №266 від 28.12.2018 «Про впровадження в промислову експлуатацію та забезпечення функціонування інформаційної системи «Система електронного документообігу органів прокуратури України». URL: <https://data.gov.ua/dataset/c7d2ea18-33dc-41a6-b62d-aa5796f43e05/resource/5f33f33c-70b8-4e85-b239-2cb27ce0578e>

37. Про затвердження Тимчасової інструкції з діловодства в органах прокуратури України : Наказ Ген. прокуратури України від 12.02.2019 № 27. URL: <https://zakon.rada.gov.ua/laws/show/v0027900-19#Text>

38. Про затвердження Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України : Наказ Офісу Ген. прокурора від 22.11.2021 № 371/846. URL: <https://zakon.rada.gov.ua/laws/show/v0371905-21#Text>

39. Конвенція про захист прав людини і основоположних свобод : Конвенція Ради Європи від 04.11.1950 : станом на 1 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

40. Конвенція Ради Європи про доступ до офіційних документів : Конвенція Ради Європи від 18.06.2009 : станом на 20 трав. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/994_001-09#Text

41. Directive - 2016/680 - EN - Law Enforcement Directive. EUR-Lex – Access to European Union law – choose your language. URL: <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>

42. The role of public prosecutors outside the criminal justice system. URL: <https://rm.coe.int/16807096c5>

43. Білозьорова Л. В. Основні засади нормативно-правового регулювання інформаційного забезпечення діяльності органів прокуратури України. Право і суспільство. 2024. № 2. С. 743-755. URL: http://pravoisuspilstvo.org.ua/archive/2024/2_2024/109.pdf

44. Амелін О. Ю. Адміністративно-правове регулювання інформаційного забезпечення діяльності органів прокуратури України : дис. ...

канд. юрид. наук : 12.00.07. Київ, 2020. 229 с. URL:

<https://drive.google.com/file/d/1cwe85yU3rZzxmpBrcxvHrNMp-uQFnWXg/view>

45. Цимбалюк В. Правова інформатика в діяльності прокуратури України. Правова інформатика. 2007. № 2(14). С. 18-27. URL: <https://ippi.org.ua/sites/default/files/07tvdpu.pdf>

46. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / Р. А. Калюжний, М. Я. Швець, В. С. Цимбалюк, В. Д. Гавловський та ін.; за ред. Р. А. Калюжного, В. О. Шамрая – Академія державної податкової служби України. – К.: Видавництво “КВІЦ”, 2002. 296 с. URL: <https://ippi.org.ua/51-monografii-stor-17>

47. Банах С., Колесніков А. Інформаційне забезпечення діяльності прокуратури. Науковий вісник Ужгородського національного університету. 2020. Т. 2, № 61. С. 129–132. URL: https://www.researchgate.net/publication/342250425_INFORMACIJE_ZABEZPE_CENNA_DIALNOSTI_PROKURATURI_INFORMATION_PROVISION_OF_THE_PROSECUTOR'S_ACTIVITIES

48. Eucrim. URL: https://eucrim.eu/media/issue/pdf/eucrim_issue_2023-02.pdf

49. Блажівський Є. М. Значення інформації у діяльності органів прокуратури України. Науково-інформаційний вісник. 2013. № 7. С. 115–119. URL: <https://visnyk.iful.edu.ua/wp-content/uploads/2019/02/7-17-13.pdf>

50. Хомич А. С. Адміністративно правові засади інформаційного забезпечення діяльності органів прокуратури. Форум права. 2012. № 1. С. 1046–1049. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/e6f1214e-efbc-4e5b-87e9-d768de04b714/content>

51. Піляй І. Питання удосконалення інформаційно-аналітичного забезпечення реалізації електронної прозорості в органах прокуратури. Актуальні проблеми правознавства. 2018. № 3 (15). С. 64–69. URL: <https://appj.wunu.edu.ua/index.php/appj/article/view/306/302>

52. Directive - 2022/2555 - EN - EUR-Lex. EUR-Lex – Access to European Union law – choose your language. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
53. Жилияєв І. Б. Інформаційне право України: теорія і практика: монографія. — К.: Парламентське видавництво. 2009. 104 с.
54. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 416 с. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/4844/1/InformPravoUKR.pdf>
55. European judicial systems Efficiency and quality of justice. CEPEJ STUDIES. 2016. No. 24. URL: <https://www.giurisprudenzapenale.com/wp-content/uploads/2016/11/Scarica-lo-studio-tematico-%E2%80%9CUse-of-information-technology-in-European-Courts%E2%80%9D-ENG.pdf>
56. Adaptation of the Ukrainian Administrative Justice System to EU Requirements: Transparency, Efficiency and Accessibility in Public Law Disputes. CERIDAP. URL: <https://ceridap.eu/adaptation-of-the-ukrainian-administrative-justice-system-to-eu-requirements-transparency-efficiency-and-accessibility-in-public-law-disputes/?lng=en>
57. Григорчук М.В. Місце і роль інформаційного права в системі права України. Legal Bulletin. 2023. № 4(10). 161–165. URL: <https://lbku.krok.edu.ua/index.php/legal-bulletin/article/view/427/368>
58. Use of Information and Communication Technologies/ICT in judicial activity. URL: <https://rm.coe.int/sep-2017-use-of-information-and-communication-technologies-ict-in-judic/16809ebf0a>
59. Drozd Oleksii, Politanskyi Viacheslav, Zaikina Hanna, Pyliuha Liliia, Shkoda Vlada, Integration Challenges of Ukrainian Anti-Corruption Reform on the Way to EU. Science of Law, 2025, No. 1, pp. 183-189. URL: <https://www.legal-science.com/index.php/SoL/article/view/326>

60. Адміністративне право України : підручник / кол. авт.: Ю. П. Битяк, В. М. Гаращук, О. В. Дьяченко та ін. ; за ред. Ю. П. Битяка; М-во освіти і науки України. – Київ: Юрінком Інтер, 2007. 543 с.
61. Адміністративне право : підручник / Ю.П. Битяк (кер.авт.кол.), І.М. Балакарева, І.В. Бойко та ін. : за аг. ред. Ю. П. Битяка. Харків: Право, 2020. 392 с.
62. Anatolii P. Getman, Oleg M. Yaroshenko, Roman V. Shapoval, Roman Ye. Prokopiev, Maryna I. Demura he impact of artificial intelligence on legal decision-making. *International Comparative Jurisprudence*. Vol. 9 No. 2 (2023). p. 155-169. URL: <https://doi.org/10.13165/j.icj.2023.12.001>
63. Білозьорова Л. В. Сучасний адміністративно-правовий механізм інформаційно-правового забезпечення діяльності органів прокуратури України. *Правові новели*. 2024. № 23. С. 563-576. URL: http://legalnovels.in.ua/journal/23_2024/78.pdf
64. Богданов Р. І. Компетенція територіальних управлінь державного бюро розслідувань. *Вісник ЛННІ ім. Е. О. Дідоренка*. 2024. № 2 (106) Ч. 1. С. 63–71. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/6eb5c8a2-2f5b-4725-b6d3-cb9e0e81c6f6/content>
65. Покатаєв П. С. Основи публічного управління та адміністрування : навч. посіб. для здобувачів спеціальності 281 «Публічне управління та адміністрування» / П. С. Покатаєв, М. А. Латинін, С. В. Степаненко, Г. П. Пасемко, О. М. Таран. – Харків : ТОВ «Оберіг», 2024. 240 с. URL: https://duikt.edu.ua/uploads/1_1359_76599186.pdf
66. Фролова Є. І. Методи публічного адміністрування: понятійно-змістовна характеристика. *Juris Europensis Scientia*. 2023. № 1. С. 114–117. URL: http://jes.nuoua.od.ua/archive/1_2023/22.pdf
67. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: <https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20->

[%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf](#)

68. Пилип В. Правові засади взаємодії генеральної прокуратури України з інститутами громадянського суспільства. Адміністративне право та процес. 2023. 3(42). 16-27. URL: <https://applaw.net/index.php/journal/article/view/789/691>

69. Marchenko V. Systematization of components of competence of subjects of free legal aid provision in Ukraine: administrative and legal aspect. Public Administration and Law Review. 2021. (3). 33–39. URL:<https://public.scnchub.com/palr/index.php/palr/article/download/106/86/190>

70. Білозьорова Л. В. Суб'єкти інформаційно-правового забезпечення діяльності органів прокуратури України. Право і суспільство. 2025. № 2. С. 731-743. URL: http://pravoisuspilstvo.org.ua/archive/2025/2_2025/101.pdf

71. Yevdokimenko S. V., Naumova A. O., Yakymchuk S. O., & Povydysh V. V. Foreign experience of administrative and legal support of citizens' rights by prosecutor's offices and possibilities of its use in Ukraine. Amazonia Investiga. 2020. 9(27). 544-551. URL: <https://www.amazoniainvestiga.info/index.php/amazonia/article/download/1267/1141/3606>

72. Подкопаєв С. В. Організація та діяльність прокуратури в Україні : монографія / С. В. Подкопаєв. Харків : Право, 2020. 364 с.

73. Про окремі питання забезпечення початку роботи окружних прокуратур : Наказ Офісу Ген. прокурора від 17.02.2021 № 39 : станом на 22 груд. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/v0039905-21#Text>

74. Положення про самостійні структурні підрозділи. Головна - Офіс Генерального прокурора. URL: <https://gp.gov.ua/ua/posts/polozhennya-pro-samostijni-strukturni-pidrozdili>

75. European Public Prosecutor's Office. URL: <https://www.eppo.europa.eu/en>

76. Regulation 2017/1939 EN EPPO. EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2017/1939/oj>

77. Recommendation Rec(2000)19 of the Committee of Ministers to Member States on the Role of Public Prosecution in the Criminal Justice System. Refworld. Refworld. URL:

<https://www.refworld.org/legal/resolution/coeministers/2000/en/31721>

78. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 : станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

79. Case of M.M. v. The United Kingdom. Hudoc. European Court of Human Rights. URL: [https://hudoc.echr.coe.int/eng#%7B"itemid":\["001-114517"\]%7D](https://hudoc.echr.coe.int/eng#%7B)

80. Présentation du parquet général de la Cour de cassation. URL: <https://www.courdecassation.fr/presentation-du-parquet-general-de-la-cour-de-cassation>

81. Les magistrats du parquet. Ministère de la justice. URL: <https://www.justice.gouv.fr/justice-france/acteurs-justice/magistrats/magistrats-du-parquet>

82. Code de l'organisation judiciaire. URL: https://www.legifrance.gouv.fr/codes/article_1c/LEGIARTI000038314091

83. L'organisation du parquet de Paris. Tribunal de Paris. URL: <https://www.tribunal-de-paris.justice.fr/75/lorganisation-du-parquet-de-paris>

84. Vie-publique. URL: <https://www.vie-publique.fr/fiches/38127-quest-ce-que-le-parquet-ou-ministere-public>

85. Vérification de sécurité. Precisement.org - Vérification. Blog. URL: <https://www.precisement.org/blog/+L-e-Administration-avance,568+.html>

86. French Business Law - French Legislation. French Business Law. URL: <https://french-business-law.com/french-legislation/legiscta000006151873-legiscta000006167418-section-3-powers-of-the-public-prosecutor/>

87. Article 230-8 of the French Code of Criminal Procedure. French Business Law. URL: <https://french-business-law.com/french-legislation-art/article-230-8-of-the-french-code-of-criminal-procedure/>

88. Cassiopee. Wikipédia. URL: <https://fr.wikipedia.org/wiki/CASSIOPEE>

89. Données personnelles – CASSIOPEE. Justice.fr. Justice.fr. Vos droits et démarches. URL: [https://www.justice.fr/donnees-personnelles/cassiopee#:~:text=Le%20bureau%20d'ordre%20national,le%20contrôle%20d'un%20magistrat](https://www.justice.fr/donnees-personnelles/cassiopee#:~:text=Le%20bureau%20d'ordre%20national,le%20contr%C3%B4le%20d'un%20magistrat)
90. Statistical file form the processing of Cassiopée, completed cases – Le CASD – Centre d'accès Sécurisé aux Données. CASD - Centre d'accès sécurisé aux données. URL: <https://www.casd.eu/en/source/statistical-file-form-the-processing-of-cassiopee-completed-cases/>
91. Projet de loi d'orientation et de programmation du ministère de la justice 2023-2027. URL: <https://docs.reclaimthenet.org/pjl22-569.pdf>
92. Open data of court decisions. Ministère de la justice. URL: <https://www.justice.gouv.fr/documentation/open-data-court-decisions>
93. Ad Hoc Information Report. Data protection: Redress mechanisms and their use. Institut Français des Droits et Libertés (IFDL). 2012. URL: https://fra.europa.eu/sites/default/files/access_to_data_protection_remedies_country_fr.pdf
94. CNIL. Particulier. URL: <https://www.cnil.fr/en>
95. Key Figures of Justice. 2023. Edition. URL: https://www.justice.gouv.fr/sites/default/files/2024-01/Chiffres_cle%CC%81s_2023_ENG_En_ligne.pdf
96. Prawo o prokuraturze. 2016. URL: <https://dziennikustaw.gov.pl/D2016000017701.pdf>
97. Prokuratury Regionalne. Prokuratura Krajowa. Portal Gov.pl. URL: <https://www.gov.pl/web/prokuratura-krajowa/lista-prokuratury-regionalne>
98. LexLege. Art. 28. - Prawo o prokuraturze. Rozdział 1. Organy i struktura organizacyjna prokuratury. URL: https://lexlege.pl/prawo-o-prokuraturze/art-28/#google_vignette
99. Organizacja jednostki - Prokuratura Krajowa - Portal Gov.pl. Prokuratura Krajowa. URL: <https://www.gov.pl/web/prokuratura-krajowa/organizacja-jednostki10>

100. Podstawowe informacje - Prokuratura Okręgowa w Nowym Sączu - Portal Gov.pl. Prokuratura Okręgowa w Nowym Sączu. URL: <https://www.gov.pl/web/po-nowy-sacz/podstawowe-informacje>

101. Opinion on the Act on the Public Prosecutor's office, as amended, adopted by the Venice Commission at its 113th Plenary Session. Poland URL: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2017\)028-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2017)028-e)

102. The draft amendments to the Law on the Public Prosecutor's Office adopted by the Venice Commission at its 140th Plenary Session. URL: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2024\)034-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)034-e)

103. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej. URL: <https://dziennikustaw.gov.pl/D2001112119801.pdf>

104. Strona główna. Biuletyn Informacji Publicznej - Portal Gov.pl. URL: <https://www.gov.pl/web/bip>

105. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Internetowy System Aktów Prawnych. URL: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000>

106. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Internetowy System Aktów Prawnych. URL: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000125>

107. Євтушенко О. Законодавче врегулювання судового провадження щодо кримінальних проступків: досвід країн континентальної системи права. Knowledge, Education, Law, Management. 2022. № 4 (48). С. 331–337. URL: <https://kelmczasopisma.com/viewpdf/9071>

108. System e-KRK. URL: <https://ekrk.ms.gov.pl/ep-web/login>

109. Portal Rejestrów Sądowych. URL: <https://prs.ms.gov.pl/krs>

110. Krajowy Rejestr Zadłużonych. Ministerstwo Sprawiedliwości. URL: <https://krz.ms.gov.pl/#!/application/KRZPortalPUB/1.9/KrzPortalPubGui.StronaGlowna?params=JTdCJTdE&itemId=item-0&seq=0>

111. Ceidg.gov.pl - Centralna Ewidencja i Informacja o Działalności Gospodarczej. URL: <https://aplikacja.ceidg.gov.pl/CEIDG/Index.aspx>

112. Sprawdź dane swoje lub swojego dziecka w rejestrze PESEL i pobierz zaświadczenie. Gov.pl. Portal. URL: <https://www.gov.pl/web/gov/spawdz-swoje-dane-w-rejestrze-pesel>

113. Rejestr Sprawców Przepływów na Tle Seksualnym. Ministerstwo Sprawiedliwości. Portal Gov.pl. URL: <https://www.gov.pl/web/sprawiedliwosc/rejestr-sprawcow-przeplywow-na-tle-seksualnym>

114. Portal Informacyjny Sądów Powszechnych. Biuletyn Informacji Publicznej Sąd Okręgowy Warszawa. Praga w Warszawie. URL: <https://warszawapraga.so.gov.pl/artukul/171/114/portal-informacyjny-sadow-powszechnych>

115. Підтвердження довіреного профілю на платформі ePUAP - Польща в Україні - Portal Gov.pl. Польща в Україні. URL: <https://www.gov.pl/web/ukraina-uk/Pidtverdzhennia-ePUAP>

116. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym. Internetowy System Aktów Prawnych. URL: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20000500580>

117. Krajowy Rejestr Karny - Portal Gov.pl. Krajowy Rejestr Karny. URL: <https://www.gov.pl/web/krajowy-rejestr-karny>

118. Poland's Membership in the European Public Prosecutor's Office Becomes a Fact. Ministry of Justice. Gov.pl website. URL: <https://www.gov.pl/web/justice/polands-membership-in-the-european-public-prosecutors-office-becomes-a-fact#:~:text=Poland's%20Membership%20in%20the%20European%20Public%20Prosecutor's%20Office%20Becomes%20a%20Fact,->

[13.12.2024&text="We%20have%20joined%20the%20European,Sweden,%20we%20can%20announce%20it](#)

119. Agence nationale des techniques d'enquêtes numériques judiciaires. Ministère de la justice. URL: <https://www.justice.gouv.fr/ministere-justice/organismes-rattaches/agence-nationale-techniques-denquetes-numeriques-judiciaires>

120. Agence nationale des techniques d'enquêtes numériques judiciaires. Wikipedia. URL: https://en.wikipedia.org/wiki/Agence_nationale_des_techniques_d'enquêtes_numériques_judiciaires

121. LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746>

122. Loi pour une République numérique. Wikipedia. URL: https://en.wikipedia.org/wiki/Loi_pour_une_République_numérique

123. Remote Courts Worldwide. France. URL: <https://remotecourts.org/country/france.htm>

124. LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368>

125. CMS Expert Guide to Digital Litigation in France. URL: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-digital-litigation/france>

126. Білозьорова Л. В. Досвід Франції та Польщі щодо інформаційно-правового забезпечення діяльності органів прокуратури. Knowledge, Education, Law, Management. 2024. № 7 (67). С. 400-412. URL: <https://kelmczasopisma.com/ua/jornal/94>

127. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : Наказ Офісу Ген. прокурора від 30.06.2020 № 298 : станом на 16 верес. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/v0298905-20#Text>

128. Документи з питань організації та ведення Єдиного реєстру досудових розслідувань. Головна - Офіс Генерального прокурора. URL:

<https://gp.gov.ua/ua/posts/dokumenti-z-pitan-organizaciyi-ta-vedennya-yedinogo-reyestru-dosudovih-rozsliduvan>

129. Статистика. Головна - Офіс Генерального прокурора. URL: <https://gp.gov.ua/ua/posts/statistika>

130. Вхід до системи. Єдиний реєстр досудових розслідувань. URL: <https://erdr.gp.gov.ua/erdr/erdr.web.system.LoginPage.cls>

131. Електронний суд. URL: <https://id.court.gov.ua/>

132. Система електронної взаємодії державних електронних інформаційних ресурсів. Державне підприємство «ДІЯ». URL: <https://se.diia.gov.ua/trembita>

133. Tabolina K., Tabolin V. Digital Transformation of the Prosecutor's Office and Its Impact on Criminal Proceedings. 1st International Scientific Conference "Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development" (LARDER 2020), Prague, Czech Republic, 22–23 October 2020. Paris, France, 2021. URL: <https://doi.org/10.2991/aebmr.k.210318.023>

134. Sereda O., Mamnitskyi V., Kornieva P. Cherevatenko I. New Steps of Digitalisation of Civil Justice in Ukraine. Access to Justice in Eastern Europe. 2024. Vol. 7, no. 1. P. 416–426. URL: <https://doi.org/10.33327/ajee-18-7.1-n000118>

135. Антонюк О. Електронне кримінальне провадження: міжнародний досвід використання інформаційних систем алгоритмізації кримінальної юстиції. Науковий вісник Дніпровського державного університету внутрішніх справ, 2024. (1). с. 253–263. URL: <https://visnik.dduvs.edu.ua/index.php/visnyk/article/view/952>

136. Maglona V. V., Hbur Z. V., Koshova S. P., Yeremenko S. A. Formation of electronic government in Ukraine problems and prospects of development. Monograph. Warsaw: RSGlobalSp. zO.O., 2021. 60p. URL: <https://doi.org/10.31435/rsglobal/040>

137. Левочко Р. Б., Гандзюк Л. С., Потинський А. М. Цифровізація наглядової діяльності прокурора у досудовому розслідуванні. Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.

2023. № 37. с. 119-126. URL: <https://doi.org/10.5281/zenodo.7985980>.

<https://nzlubp.org.ua/index.php/journal/article/download/788/716/>

138. Popovych M. V. Features of maintaining the Unified Register of Pre-trial Investigations (URPI) and the information and telecommunication system at the stage of pre-trial investigation. Uzhhorod National University Herald. Series: Law. 2024. Vol. 4, no. 85. P. 393–398. URL: <https://doi.org/10.24144/2307-3322.2024.85.4.58>

139. Щодо дистанційного навчання користувачів КП "Д-3". URL: <https://ks.if.court.gov.ua/sud0910/news/42175/>

140. Про застосування сучасних новітніх інформаційних технологій в прокуратурі Одеської області. Регіональні новини. Генеральна прокуратура України. URL: https://old.gp.gov.ua/ua/reegions_news_detail.html? m=publications& c=view & t=rec& id=83027& s=print

141. Кормич Б. А. Інформаційне право : підручник. Харків : Бурун і К, 2011. 334 с. URL: https://www.researchgate.net/publication/369358287_Informacijne_pravo

142. Ludmila Stasiuk, Oleksandr Stasiuk, Serhii Zytskyk, 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

143. Про затвердження Інструкції про порядок розгляду звернень і запитів в органах прокуратури України, Порядку організації та проведення особистого прийому громадян в органах прокуратури України : Наказ Офісу Ген. прокурора від 25.06.2024 № 153 : станом на 18 лип. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/v0153905-24#Text>

144. Про внесення змін до Інструкції про порядок забезпечення доступу до публічної інформації в органах прокуратури України, затвердженої наказом Генерального прокурора від 06.08.2020 № 363, та Інструкції про порядок розгляду звернень і запитів в органах прокуратури України, затвердженої наказом Генерального прокурора від 25.06.2024 № 153 : Наказ Офісу Ген.

прокурора від 17.07.2024 № 171. URL:
<https://zakon.rada.gov.ua/laws/show/v0171905-24#Text>

145. Деякі питання документування управлінської діяльності : Постанова Каб. Міністрів України від 17.01.2018 № 55 : станом на 3 жовт. 2025 р. URL:
<https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text>

146. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 № 518 : станом на 7 верес. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>

147. 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>

148. 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>

149. 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

150. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

151. 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>

152. 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_campaignid=22638344346&gbraid=0AAAAAo4yQR0tSg1Uy1JC59J1192CR4TJi&gclid=CjwKCAjw04HIBhB8EiwA8jGNbQUHf2q4SYImC4nlmx93YI91SJuxBkqNhr3XCoT7DUKDRI5MPsmMMhoCJQkQAvD_BwE

153. Білозьорова Л. В. Вдосконалення нормативно-правової бази діяльності органів прокуратури з інформаційно-правового забезпечення. Правові новели. 2025. № 26. С. 377-390. URL: http://legalnovels.in.ua/journal/26_2025/45.pdf

154. 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. Белякова. Київ: КВІЦ, 2019. 344 с. URL: <https://dspace.nlu.edu.ua/handle/123456789/16729>

155. 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>.

156. 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>

157. Федоренко Т. В., Садковський С. П. Юридична відповідальність в інформаційній сфері: поняття та особливості. Часопис Київського університету права. 2022. (2-4) С. 82-85. URL: <https://chasprava.com.ua/index.php/journal/article/view/918>

158. Про затвердження Дисциплінарного статуту прокуратури України : Постанова Верхов. Ради України від 06.11.1991 № 1796-ХІІ : станом на 15 лип. 2015 р. URL: <https://zakon.rada.gov.ua/laws/show/1796-12#Text>

159. 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>

160. Dubynskyy O., Dubynskyy 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>

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

162. 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>

163. Дисциплінарна відповідальність прокурорів в Україні / О. Банчук, М. Каменєв, Є. Крапівін, 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

164. 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>

165. Білозьорова Л. В. Деякі питання удосконалення юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури. *Юридичний науковий електронний журнал*. 2025. № 8. С. 338-346. URL: http://lsej.org.ua/8_2025/72.pdf

166. Рішення № 101393078. 26.11.2021. Одеський окружний адміністративний суд. URL: <https://youcontrol.com.ua/catalog/court-document/101393078/>

167. 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=100003cda1e1c2a50c3abd457cd5c19edc73dc&d=5>

168. Кваліфікаційно-дисциплінарна комісія прокурорів. Офіційний сайт.
URL: <https://kdkp.gov.ua/decision/2024/08/6/4833>

169. Рішення № 99680763. 16.09.2021. Запорізький окружний адміністративний суд. URL: <https://youcontrol.com.ua/catalog/court-document/99680763/>

170. 4.3.1. Право на інформацію. Конституційний Суд України. Офіційний вебсайт. URL: <https://ccu.gov.ua/storinka-knygy/431-pravo-na-informaciyu>

ДОДАТКИ

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИЙ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких висвітлено основні наукові результати дисертації:

1. Білозьорова Л. В. Деякі питання щодо особливостей інформаційно-правового забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2023. № 5. С. 513-522. URL: http://pravoisuspilstvo.org.ua/archive/2023/5_2023/74.pdf

2. Білозьорова Л. В. Основні засади нормативно-правового регулювання інформаційного забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2024. № 2. С. 743-755. URL: http://pravoisuspilstvo.org.ua/archive/2024/2_2024/109.pdf

3. Білозьорова Л. В. Досвід Франції та Польщі щодо інформаційно-правового забезпечення діяльності органів прокуратури. *Knowledge, Education, Law, Management*. 2024. № 7 (67). С. 400-412. URL: <https://kelmczasopisma.com/ua/jornal/94>

4. Білозьорова Л. В. Сучасний адміністративно-правовий механізм інформаційно-правового забезпечення діяльності органів прокуратури України. *Правові новели*. 2024. № 23. С. 563-576. URL: http://legalnovels.in.ua/journal/23_2024/78.pdf

5. Білозьорова Л. В. Суб'єкти інформаційно-правового забезпечення діяльності органів прокуратури України. *Право і суспільство*. 2025. № 2. С. 731-743. URL: http://pravoisuspilstvo.org.ua/archive/2025/2_2025/101.pdf

6. Білозьорова Л. В. Деякі питання удосконалення юридичної відповідальності суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури. *Юридичний науковий електронний журнал*. 2025. № 8. С. 338-346. URL: http://lsej.org.ua/8_2025/72.pdf

7. Білозьорова Л. В. Вдосконалення нормативно-правової бази діяльності органів прокуратури з інформаційно-правового забезпечення. *Правові новели*. 2025. № 26. С. 377-390. URL: http://legalnovels.in.ua/journal/26_2025/45.pdf

які засвідчують апробацію матеріалів дисертації:

8. Білозьорова Л. В. Сучасний погляд на використання інформації з єдиних і державних реєстрів України представниками слідчих та правоохоронних органів. Сектор безпеки України: актуальні питання науки та практики: збірник наукових статей, тез доповідей та повідомлень за матеріалами XIII Міжнародної науково-практичної конференції (27 березня 2025 року, Національний юридичний університет імені Ярослава Мудрого, м. Харків). У 2-х частинах. Частина 1. Серія «Сектор безпеки України». Вип. 54. Упорядник Мех Ю.В. Харків: Друкарня Мадрид, 2025. С. 15-18.

9. Білозьорова Л. В. Щодо інформаційно-правового забезпечення діяльності органів прокуратури України в умовах цифрової трансформації. Актуальні питання адміністративного права та адміністративного судочинства: збірник наукових статей, тез доповідей та повідомлень за матеріалами II Міжнародної науково-практичної конференції (15 травня 2025 року, Національний юридичний університет імені Ярослава Мудрого, м. Харків). Серія «Сектор безпеки України». Вип.55. Упорядник Мех Ю.В. Харків: Друкарня Мадрид, 2025. С. 12-18.

10. Білозьорова Л.В. Інформаційно-правове забезпечення функціонування прокуратури України: суб'єктний аспект: збірник наукових статей, тез доповідей та повідомлень за матеріалами Мультидисциплінарної науково-практичної конференції «Сучасні тенденції соціально-гуманітарного розвитку суспільства», (3-5 листопада 2025 року, Україна, м. Харків, Німеччина, м. Циттау). Соціально-гуманітарний вісник: зб. наук. пр. Вип. 61. Харків: СГ НТМ «Новий курс», 2025. С. 69.

11. Білозьорова Л. В. Юридична відповідальність суб'єктів інформаційно-правового забезпечення діяльності органів прокуратури України: Modern Perspectives on Science and Economic Progress: Collection of Scientific Papers with Proceedings of the 2nd International Scientific and Practical Conference. International Scientific Unity (November 5-7, 2025. Vilnius, Lithuania). P. 230-233.

Закон України
Про внесення змін до
«Дисциплінарного статуту прокуратури України»

Верховна Рада України п о с т а н о в л я є:

I. Внести до Дисциплінарного статуту прокуратури України, затвердженого Постановою Верховної Ради України від 06.11.1991 № 1796-ХІІ (Відомості Верховної Ради України (ВВР), 1992, N 4), наступні зміни:

1. Доповнити статтю 9 пунктом 7, який викласти у наступній редакції:
«заборона доступу до окремих категорій службової інформації на певний строк».

2. Доповнити статтю 11 абзацем третім, який викласти у наступній редакції:

«Ескалаційна шкала стягнень:

- до легких проступків застосовується такі види стягнень: зауваження, заборона доступу до окремих категорій службової інформації на певний строк.

- до значних проступків – догана, пониження в посаді.

- до грубих проступків – догана, звільнення.

3. Доповнити статтю 13 абзацем другим, який викласти у наступній редакції:

«Підрозділи по роботі з кадрами органів прокуратури ведуть електронний облік накладених на працівників дисциплінарних стягнень. Вказана інформація враховується при прийнятті рішення щодо обрання виду відповідальності (у разі

повторності вчинення правопорушення – застосовується більш суворе покарання)».

4. Доповнити Дисциплінарний статут прокуратури України розділом IV «Дисциплінарна відповідальність за проступки у сфері обігу інформації, а також під час роботи в інформаційних системах».

5. Розділ IV Дисциплінарного статуту прокуратури України доповнити:

1) статтею 1, яку викласти у наступній редакції:

«Інформаційний дисциплінарний проступок – це умисне порушення встановленого порядку доступу, зберігання, класифікації, обліку, розкриття чи передачі службової або конфіденційної інформації (у т.ч інформації, що міститься в інформаційних системах прокуратури, ЄРДР), невиконання обов’язкових техніко-організаційних заходів під час роботи з інформаційними системами, перешкоджання інцидент-менеджменту».

2) статтею 2, яку викласти у наступній редакції:

«види проступків, пов’язаних із порушенням режиму поводження з інформацією:

- неналежне зберігання документів (відсутність шифрування, зберігання на неавторизованих носіях), що містять службову або конфіденційну інформацію, без негативних наслідків;

- невиконання внутрішніх політик інформаційної безпеки;

- недотримання правил зберігання цифрових носіїв та резервного копіювання;

- незабезпечення повного, всебічного та достовірного обліку обов’язкових до внесення відомостей про кримінальне правопорушення до ЄРДР, вчинене і усунуте протягом звітного періоду, яке не призвело до викривлення статистичної звітності;

- недотримання процедури доступу до електронних інформаційних систем (доступ без правової підстави);

- внесення реєстраторами відомостей до ЄРДР у строки понад 24 години з моменту прийняття процесуального рішення або набрання чинності рішенням слідчого судді (суду) щодо відомостей, передбачених в електронних формах ЄРДР;

- неналежне зберігання документів (відсутність шифрування, зберігання на неавторизованих носіях), що містять службову або конфіденційну інформацію, що призвело до їх витоку, втрати, пошкодження, знищення;

- розголошення службової інформації в будь-якій формі (усній, письмовій, цифровій);

- незабезпечення повного, всебічного та достовірного обліку обов'язкових до внесення відомостей про кримінальне правопорушення до ЄРДР, що призвело до викривлення статистичної звітності, порушень КПК України».

3) статтею 3, яку викласти у наступній редакції:

«Категорії інформаційних дисциплінарних проступків:

а) легкі (без наслідків, або порушення усунуті одразу);

б) значні (є ризик шкоди правам людини/інтересам правосуддя);

в) грубі (реальний витік інформації, порушення таємниці, викривлення статистичної звітності, порушення КПК України, істотна шкода інтересам громадян)».

4) статтею 4, яку викласти у наступній редакції:

«Процедура фіксації інциденту, пов'язаного з інформаційним дисциплінарним проступком:

Працівник структурного підрозділу Офісу Генерального прокурора, САП, обласної, окружної прокуратури, який виявив інформаційний дисциплінарний проступок, протягом 24 годин з моменту виявлення, складає мотивований та обґрунтований рапорт, яким доповідає безпосередньому керівнику.

Керівник ініціює проведення службової перевірки за викладеними у рапорті фактами, забезпечує складання внутрішнього аналітичного звіту, збереження електронних логінів та первинне блокування доступу до особистого ключа та відповідного йому кваліфікованого сертифіката відкритого ключа».

До проведення службової перевірки залучаються працівники структурних підрозділів, спеціально утворених для забезпечення впровадження в органах прокуратури новітніх технічних комплексів, забезпечення адміністрування ІС «ЄРДР», ІАС «ОСОП», ІС «СЕД», автоматизованої інформаційно-аналітичної системи «Кадри-WEB», надання доступу до них, здійснення контролю за їх роботою, забезпечення дотримання єдиних вимог щодо підготовки документів та організації роботи з ними, які документально підтверджують або спростовують викладену у рапорті інформацію.

За результатами проведеної службової перевірки Генеральним прокурором, керівником САП, керівниками обласних прокуратур приймається рішення щодо наявності підстав для притягнення особи до відповідальності.

При обранні виду дисциплінарного стягнення враховується категорія інформаційного дисциплінарного проступку, а також повторність його вчинення.

5) статтею 5, яку викласти у наступній редакції:

«Доказами вчинення інформаційного дисциплінарного проступку є: витяги з електронних журналів, витяги з інформаційних систем, відомості щодо технічних логінів, форензик-знімки криптографічних алгоритмів, призначених для захисту службової інформації, результати аналітичних досліджень, якими підтверджено факт використання відповідних засобів та алгоритмів не за призначенням».

II. Прикінцеві положення

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування.

2. Генеральному прокурору України протягом трьох місяців з дня набрання чинності цим Законом привести відомчі накази та положення у відповідність із цим Законом.

Голова Верховної Ради України

АКТ

ЗАТВЕРДЖУЮ

Проректор
Харківського національного
університету внутрішніх справ,
доктор юридичних наук, професор,
заслужений юрист України

 **Олександр МУЗИЧУК**
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
2025 р.



АКТ

впровадження результатів дисертаційного дослідження Білозьорової Людмили Володимирівни «Інформаційно-правове забезпечення діяльності органів прокуратури України», поданого на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право у наукову діяльність Харківського національного університету внутрішніх справ

Комісія в складі:

Голова: начальник відділу організації наукової діяльності Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент Абламський С.Є.

Члени комісії:

1. учений секретар секретаріату Вченої ради Харківського національного університету внутрішніх справ, доктор юридичних наук, доцент Невядовський В.О.;

2. завідувач кафедри адміністративної діяльності навчально-наукового інституту № 3 Харківського національного університету внутрішніх справ; доктор юридичних наук, професор Джафарова О.В.;

3. завідувач науково-дослідної лабораторії з проблем досудового розслідування навчально-наукового інституту № 1 Харківського національного університету внутрішніх справ; доктор юридичних наук, професор Шатрава С.О.

Розглянувши матеріали дисертаційної роботи Людмили Володимирівни Білозьорової «Інформаційно-правове забезпечення діяльності органів прокуратури України», поданого на здобуття наукового ступеня кандидата юридичних наук за спеціальністю (12.00.07 - адміністративне право і процес; фінансове право; інформаційне право), комісія дійшла висновку про їх наукову цінність, внутрішню узгодженість та придатність до впровадження у науково-дослідну діяльність Харківського національного університету внутрішніх справ. Встановлено, що у дослідженні послідовно обґрунтовано категоріальний апарат

і концептуальну модель інформаційно-правового забезпечення прокурорської діяльності, визначено його мету, завдання, структуру та функції, розкрито адміністративно-правовий механізм такого забезпечення крізь призму суб'єктного складу, повноважень, процедур, інструментів і технологій, а також надано пропозиції щодо оптимізації правових, організаційних і технічних засад функціонування відповідних інформаційних процесів.

Зміст дисертації демонструє, що інформаційно-правове забезпечення органів прокуратури України є цілісним інститутом адміністративного права, який акумулює норми матеріального та процесуального характеру, визначає статус і взаємодію суб'єктів (органи прокуратури та інші державні органи, установи, організації), формалізує процедури збирання, обміну, обробки, зберігання та захисту даних, а також інтегрує ризик-орієнтовані підходи до інформаційної безпеки та захисту персональних даних. Комісія відзначає, що зроблені у роботі висновки та розроблені пропозиції можуть бути безпосередньо використані: під час розроблення теоретичних положень щодо сутності, структури та завдань інформаційно-правового забезпечення прокурорської діяльності; при доктринальному та прикладному обґрунтуванні правової природи і побудови адміністративно-правового механізму такого забезпечення; у деталізації ролі суб'єктів механізму, у тому числі шляхом визначення їх компетенцій, повноважень та меж відповідальності; при оцінюванні сучасних викликів цифровізації, розвитку відкритих даних, кіберзагроз і вимог інтероперабельності державних інформаційних систем; а також під час формування пропозицій з удосконалення нормативно-правового, організаційного та технологічного підґрунтя інформаційних процесів у системі органів прокуратури.

З огляду на наведене комісія вважає доцільним інтегрувати результати дисертаційного дослідження в науково-дослідну діяльність університету шляхом використання напрацьованих теоретичних і методичних положень у формуванні та реалізації перспективних тем фундаментальних і прикладних досліджень, спрямованих на розвиток адміністративно-правової доктрини інформаційно-правового забезпечення. Матеріали дисертації є релевантними для підготовки проектів законів і підзаконних нормативно-правових актів, що регулюють інформаційні процеси у діяльності органів прокуратури (зокрема щодо врегулювання інформаційної взаємодії з іншими органами публічної влади, стандартизації процедур доступу до даних, побудови регламентів обробки і зберігання інформації, впровадження механізмів аудитування та моніторингу інформаційної безпеки), а також для підготовки науково-правових висновків на запити органів державної влади. Запропоновані у роботі методичні підходи можуть слугувати основою для розроблення моделей і алгоритмів інформаційних процедур, типових регламентів взаємодії суб'єктів, методик оцінювання ефективності функціонування інформаційних систем і процесів, а також індикаторів зрілості управління інформацією у прокурорських органах.

Передбачається, що впровадження результатів роботи забезпечить комплексний науковий ефект: по-перше, сприятиме поглибленню доктрини

адміністративного права у частині інституціоналізації інформаційно-правового забезпечення органів прокуратури, уточненню його понятійно-категоріального апарату, структури та функцій; по-друге, дозволить удосконалити науково-методичний інструментарій дослідження інформаційних процесів і цифрових технологій у прокурорській діяльності (з урахуванням балансу між публічними інтересами кримінальної юстиції та правами людини, вимогами захисту персональних даних, режимів службової інформації і державної таємниці); по-третє, забезпечить формування сучасних підходів до організації інформаційного обміну, обробки та захисту даних на основі процедурної формалізації, ризик-менеджменту, інтероперабельності та безперервного удосконалення; по-четверте, підвищить ефективність адміністративно-правового регулювання функціонування органів прокуратури в умовах цифровізації публічного управління, забезпечивши узгодженість правових і технологічних рішень. Окремо підкреслюється потенціал використання матеріалів дисертації в освітній та просвітницькій діяльності (включення у навчальні плани, програми підвищення кваліфікації, підготовку навчально-методичних матеріалів для працівників органів прокуратури та суміжних інституцій).

З метою практичної реалізації результатів дослідження доцільно, по-перше, інкорпорувати ключові положення в тематику та методологічне забезпечення наукових проєктів і наукових програм університету, що стосуються модернізації правових основ функціонування інформаційних систем у секторі правосуддя; по-друге, використати напрацьовані у дисертації моделі адміністративно-правових процедур для розроблення типових регламентів інформаційної взаємодії органів прокуратури з іншими суб'єктами публічної адміністрації; по-третє, застосувати запропоновані критерії та індикатори оцінювання для аудитів ефективності та безпеки інформаційних процесів; по-четверте, організувати наукові комунікаційні майданчики (конференції, круглі столи, науково-практичні форуми) з обговоренням прикладних аспектів інтеграції правових і технологічних рішень у прокурорській діяльності. У межах експертної підтримки нормотворчості пропонується використати висновки та пропозиції дисертації під час підготовки проєктів законів та змін до підзаконних актів, у тому числі щодо деталізації компетенції суб'єктів інформаційно-правового забезпечення, уніфікації процедур доступу до інформації та обміну даними, запровадження незалежних механізмів контролю і моніторингу дотримання режимів захисту інформації.

Узагальнюючи викладене, комісія підтверджує наявність усіх необхідних підстав для впровадження результатів дисертаційного дослідження Людмили Володимирівни Білозьорової у науково-дослідну діяльність Харківського національного університету внутрішніх справ. Матеріали дисертації рекомендовано до використання у процесі виконання перспективних фундаментальних і прикладних досліджень університету, підготовки проєктів нормативно-правових актів і науково-правових висновків, а також при формуванні тематики національних та міжнародних наукових заходів, спрямованих на подальший розвиток адміністративно-правових засад

інформаційно-правового забезпечення діяльності органів прокуратури України. Комісія вважає, що системне застосування положень роботи сприятиме підвищенню інституційної спроможності органів прокуратури, утвердженню належного правового режиму даних і процесів, зміцненню інформаційної безпеки, а також зростанню якості взаємодії органів прокуратури з іншими суб'єктами публічної влади в умовах цифрової трансформації державного управління.

Голова комісії



Сергій АБЛАМСЬКИЙ

Члени комісії



Владислав НЕВЯДОВСЬКИЙ



Олена ДЖАФАРОВА



Сергій ШАТРАВА

АКТ

«Затверджую»

В.о. проректора з навчально-методичної
роботи Національного юридичного
університету імені Ярослава Мудрого

2025 р.

Д.С. Бойчук



АКТ

**впровадження матеріалів дисертаційного дослідження
«Інформаційно-правове забезпечення діяльності органів прокуратури
України»
здобувачки Науково-дослідного інституту публічного права
Білозьорової Людмили Володимирівни**

Цей акт складений в тому, що матеріали дисертаційної роботи Білозьорової Людмили Володимирівни «Інформаційно-правове забезпечення діяльності органів прокуратури України», поданої на здобуття наукового ступеня кандидата юридичних наук, використовуються в навчальному процесі Національного юридичного університету імені Ярослава Мудрого при викладанні навчальних дисциплін «Адміністративне право», «Адміністративний процес», «Адміністративне деліктне право», «Адміністративно-процесуальна діяльність правоохоронних органів».

Начальник навчального відділу
Національного юридичного
університету імені Ярослава Мудрого

Т.О. Чухлебова