УДК 342.9:004.056
DOI https://doi.org/10.32782/2408-9257-2025-4-10

Мазепа С. О.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та процесу
Західноукраїнського національного університету,
міжнародний дослідник
Оснабрюцького університету
https://orcid.org/0000-0003-1282-9089

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРАВООХОРОННІЙ СИСТЕМІ УКРАЇНИ

ADMINISTRATIVE AND LEGAL MECHANISMS FOR ENSURING INFORMATION SECURITY IN THE LAW ENFORCEMENT SYSTEM OF UKRAINE

Ця стаття присвячена комплексному дослідженню адміністративно-правових механізмів, що застосовуються для забезпечення інформаційної безпеки у системі правоохоронних органів України. В умовах цифрової трансформації державного управління та зростаючих кіберзагроз актуальність захисту інформаційних ресурсів правоохоронної системи набуває критичного значення для національної безпеки країни.

Дослідження базується на аналізі чинного законодавства України у сфері інформаційної безпеки, адміністративного права та правоохоронної діяльності. Методологічну основу роботи становлять порівняльно-правовий, системно-структурний та формально-юридичний методи дослідження, що дозволяють виявити особливості правового регулювання інформаційної безпеки у правоохоронній сфері.

Автором проведено детальний аналіз існуючих адміністративно-правових інструментів захисту інформації у діяльності Національної поліції, Служби безпеки України, прокуратури та інших правоохоронних органів. Особливу увагу приділено механізмам запобігання несанкціонованому доступу до службової інформації, забезпеченню конфіденційності персональних даних та захисту критичної інформаційної інфраструктури.

У статті виявлено основні проблеми сучасної системи адміністративно-правового забезпечення інформаційної безпеки правоохоронних органів, включаючи прогалини у законодавчому регулюванні, недостатню координацію між різними відомствами та обмеженість технічних засобів захисту інформації. Проаналізовано фактори, що знижують ефективність існуючих механізмів протидії інформаційним загрозам.

Результати дослідження дозволили сформулювати конкретні пропозиції щодо вдосконалення адміністративно-правових механізмів забезпечення інформаційної безпеки у правоохоронній системі. Запропоновано зміни до чинного законодавства, спрямовані на уніфікацію вимог щодо захисту інформації, посилення відповідальності за порушення у сфері інформаційної безпеки та оптимізацію процедур реагування на кіберінциденти.

Практична значимість роботи полягає у можливості використання отриманих висновків для модернізації системи правового регулювання інформаційної безпеки правоохоронних органів України, що сприятиме підвищенню ефективності їхньої діяльності та зміцненню довіри громадян до державних інституцій в умовах цифрового суспільства.

Ключові слова: *інформаційна безпека, правоохоронна сфера, кібербезпека, правове забезпечення, адміністративно-правовий аспект, кримінальна відповідальність, адміністративна відповідальність, євроінтеграція, гармонізація законодавства, міжнародні стандарти, НАТО, Європейський Союз (ЄС), державна інформаційна політика, загрози інформаційній безпеці, імплементація права, суб'єкти інформаційної безпеки, юридична відповідальність, інформаційні правопорушення, пропаганда, штучний інтелект.*

This article is devoted to a comprehensive study of administrative and legal mechanisms used to ensure information security in the system of law enforcement agencies of Ukraine. In the context of the digital transformation of public administration and growing cyber threats, the relevance of protecting information resources of the law enforcement system is becoming critical for the national security of the country.

The study is based on the analysis of current Ukrainian legislation in the field of information security, administrative law and law enforcement. The methodological basis of the work is based on comparative legal, systemic and structural, and formal legal research methods which allow identifying the specific features of legal regulation of information security in law enforcement.

The author provides a detailed analysis of the existing administrative and legal instruments for information protection in the activities of the National Police, the Security Service of Ukraine, the Prosecutor's Office and other law enforcement agencies. Particular attention is paid to the mechanisms for preventing unauthorised access to proprietary information, ensuring confidentiality of personal data and protecting critical information infrastructure.

The article identifies the main problems of the current system of administrative and legal support for information security of law enforcement agencies, including gaps in legislative regulation, insufficient coordination between different agencies and limited technical means of information protection. The author analyses the factors that reduce the effectiveness of existing mechanisms for countering information threats.

The results of the study allowed the author to formulate specific proposals for improving the administrative and legal mechanisms for ensuring information security in the law enforcement system. The author proposes amendments to the current legislation aimed at unifying the requirements for information security, strengthening liability for violations in the field of information security and optimising the procedures for responding to cyber incidents.

The practical significance of the work lies in the possibility of using the conclusions obtained to modernise the system of legal regulation of information security of law enforcement agencies of Ukraine, which will help to increase the efficiency of their activities and strengthen public trust in state institutions in a digital society.

Key words: *information security, law enforcement, cybersecurity, legal support, administrative-legal aspect, criminal liability, administrative liability, European integration, harmonization of legislation, international standards, NATO, European Union (EU), state information policy, information security threats, implementation of law, subjects of information security, legal liability, information offenses, propaganda, artificial intelligence.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний етап розвитку українського суспільства характеризується інтенсивними процесами цифровізації державного управління та правоохоронної діяльності, що обумовлює принципово нові виклики у сфері захисту інформаційних ресурсів. кіберзлочинців та іноземних спецслужб. У цих умовах формування ефективної системи адміністративно-правового забезпечення інформаційної безпеки набуває стратегічного значення для підтримки правопорядку та захисту національних інтересів держави.

Інтеграція України в європейський правовий простір пред'являє додаткові вимоги до системи захисту інформації в правоохоронній сфері. європейських стандартів захисту інформації.

Практична значущість дослідження адміністративно-правових механізмів забезпечення інформаційної безпеки в правоохоронній системі визначається гострою потребою у розробці конкретних рекомендацій щодо вдосконалення чинного законодавства. відомствами. Вирішення цих проблем потребує комплексного наукового підходу до дослідження адміністративно-правових аспектів захисту інформації у правоохоронній діяльності.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Проблематика адміністративно-правового забезпечення інформаційної безпеки в правоохоронній системі привертає увагу як вітчизняних, так і зарубіжних дослідників. [2, 3]. Проте специфіка адміністративно-правових механізмів у правоохоронній сфері залишається недостатньо вивченою у контексті сучасних викликів цифрової трансформації.

Європейські дослідники, зокрема Дж. Андерсон, М. Фіннеган та С. Лодж, зосередили увагу на аналізі інституційних аспектів забезпечення кібербезпеки у правоохоронних органах країн ЄС [4, 5]. Їх роботи демонструють важливість створення спеціалізованих підрозділів з боротьби з кіберзлочинністю реаліям потребує додаткового наукового обґрунтування з урахуванням особливостей національної правової системи.

На окрему увагу заслуговують дослідження учених Ментух Н, Шевчук О. присвячені адміністративно-правовим аспектам інформаційної безпеки [6, 7]. інформаційної безпеки в українському контексті

Американські дослідники Р. Кларк і С. Ландау у своїх фундаментальних працях проаналізували взаємозв'язок між технологічними інноваціями та правовим регулюванням кібербезпеки [8, 9]. самостійного дослідження механізмів імплементації міжнародних стандартів

Аналіз сучасної наукової літератури свідчить про наявність значної прогалини в дослідженні комплексних адміністративно-правових механізмів забезпечення інформаційної безпеки саме в правоохоронній системі Украї-

ни. викликів інформаційної безпеки.

Формулювання цілей статті. Метою цієї статті є комплексне дослідження адміністративно-правових механізмів забезпечення інформаційної безпеки у правоохоронній системі України з подальшою розробкою науково обґрунтованих пропозицій щодо їх удосконалення в умовах сучасних викликів цифрової трансформації та європейської інтеграції.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Правові основи забезпечення інформаційної безпеки в правоохоронній системі України формуються комплексом нормативно-правових актів різного рівня. Конституція України у статті 32 гарантує право кожного на захист персональних даних, що створює конституційну основу для розвитку системи інформаційної безпеки [10]. Проте специфіка правоохоронної діяльності потребує додаткового правового регулювання, що враховує особливості опрацювання службової інформації.

Ключову роль у формуванні адміністративно-правових механізмів інформаційної безпеки відіграє Закон України «Про захист персональних даних», який імплементує основні положення європейського законодавства в національну правову систему [12]. Стратегія кібербезпеки України, затверджена Указом Президента, визначає основні напрямки державної політики у сфері захисту кіберпростору [13].

Міжнародно-правові стандарти інформаційної безпеки формуються під впливом документів Європейського Союзу, зокрема Загального регламенту захисту даних (GDPR) [14]. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації (Будапештська конвенція) встановлює міжнародні стандарти боротьби з кіберзлочинністю [15].

Організаційна структура забезпечення інформаційної безпеки в правоохоронній системі України характеризується певною фрагментарністю повноважень між різними органами. Національна поліція України через Департамент кіберполіції здійснює розслідування злочинів у сфері інформаційних технологій [16]. Такий розподіл повноважень потребує ефективних механізмів координації та взаємодії між різними відомствами.

Адміністративно-правові процедури реагування на інциденти інформаційної безпеки в правоохоронних органах регулюються комплексом відомчих нормативних актів. специфіку сучасних кіберзагроз та вимагають актуалізації відповідно до міжнародних стандартів реагування на кіберінциденти.

Система адміністративної відповідальності за порушення у сфері інформаційної безпеки ґрунтується на положеннях Кодексу України про адміністративні правопорушення [20]. Особливості правового регулювання обробки біометричних даних у правоохоронній діяльності вимагають особливої уваги в контексті забезпечення інформаційної безпеки. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, що засвідчують особу або її спеціальний статус», встановлює правові основи обробки біометричних даних. Правоохоронні органи отримують доступ до цих даних у встановленому законом порядку, що створює додаткові ризики для інформаційної безпеки та потребує посилених заходів захисту.

Транскордонне співробітництво у сфері інформаційної безпеки регулюється міжнародними угодами та двосторонніми договорами про правову допомогу. Європол та Інтерпол розробили спеціальні процедури обміну інформацією про кіберзагрози та координацію міжнародних розслідувань. Для українських правоохоронних органів участь у цих механізмах потребує забезпечення відповідного рівня захисту інформації та гармонізації національних стандартів із міжнародними вимогами. (Таблиця 1)

Технічні стандарти інформаційної безпеки у правоохоронній системі визначаються нормативними документами Державної служби спеціального зв'язку та захисту інформації. Національний стандарт України ДСТУ ISO/IEC 27001:2015 визначає вимоги до систем управління інформаційною безпекою. Правоохоронні органи зобов'язані впроваджувати ці стандарти у своїй діяльності, що потребує значних фінансових та організаційних ресурсів та відповідного адміністративно-правового забезпечення процесу впровадження.

Перспективи розвитку адміністративно-правових механізмів забезпечення інформацій-

Таблиця 1

Транскордонне співробітництво у сфері інформаційної безпеки

Аспект	Регулювання	Інституції/Механізми	Приклади для України	Проблеми/Виклики
Міжнародні угоди	- Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001)	- Європол, Інтерпол, ENISA	- Україна ратифікувала Будапештську конвенцію у 2015 р.	- Необхідність адаптації національного законодавства до стандартів конвенції.
	- Директива ЄС NIS2 (2022) про заходи високого рівня кібербезпеки	- Групи з реагування на кіберінциденти (CSIRTs)	- Участь у європейській мережі CSIRTs (наприклад, через Держспецзв'язку)	- Дефіцит кваліфікованих фахівців для відповідності вимогам NIS2.
Двосторонні угоди	- Угоди про правову допомогу (наприклад, між Україною та США, Польщею)	- Двосторонні робочі групи	- Спільні навчання з НАТО (наприклад, проект TURBO Erasmus+)	- Недостатня інтеграція національних баз даних із міжнародними системами.
Обмін інформацією	- Протоколи Європолу щодо швидкого обміну даними про кіберзагрози	- Система I-CAN (Інтерпол)	- Підключення українських правоохоронних органів до платформи Europol's EC3	- Ризики втрати конфіденційності під час транскордонного обміну.
Гармонізація стандартів	- ISO/IEC 27001 (міжнародний стандарт інформаційної безпеки)	- Національні органи стандартизації	- Впровадження ISO-стандартів у критичній інфраструктурі (енергетика, фінанси)	- Відсутність єдиного національного органу з кібербезпеки для координації.
Кейси співпраці	- Операція «Темна мережа» (2023) – спільне розслідування Європолу та ФБР	- Спільні кіберполіцейські операції	- Участь СБУ в операції з виявлення ботнетів (за підтримки EU4PAR)	- Політичні обмеження у співпраці з окремими країнами (наприклад, РФ).
Наукові дослідження	- Публікації у журналах (наприклад, *Central European Management Journal*)	- Академічні мережі (наприклад, TURBO Erasmus+)	- Дослідження О. Шевчук про міжнародний захист цифрових прав дітей (2023)	- Недостатнє фінансування прикладних досліджень у сфері кібербезпеки.

Джерело. Складено автором за матеріалами: https://www.consilium.europa.eu/en/policies/eu-un-cooperation/

ної безпеки у правоохоронній системі України пов'язані з необхідністю адаптації до сучасних технологічних трендів. Впровадження штучного інтелекту, машинного навчання та великих даних у правоохоронну діяльність створює нові виклики для інформаційної безпеки. Це потребує розробки відповідних правових механізмів, які б забезпечували баланс між ефективністю правоохоронної діяльності та захистом прав громадян у цифровому середовищі.

Висновки. Проведене дослідження адміністративно-правових механізмів забезпечення інформаційної безпеки у правоохоронній системі України дозволило встановити, що існуюча нормативно-правова база характеризується фрагментарністю регулювання та недостатньою адаптацією до сучасних викликів цифрової доби. Аналіз чинного законодавства виявив значні прогалини у правовому регулюванні процедур обробки та захисту інформації правоохоронними органами, відсутність єдиних стандартів інформаційної безпеки для різних відомств та неефективність механізмів міжвідомчої координації. Особливо критичною є неузгодженість між вимогами національного законодавства та міжнародними стандартами захисту персональних даних, що створює правові ризики для міжнародного співробітництва у боротьбі зі злочинністю.

Організаційно-функціональний аналіз системи забезпечення інформаційної безпеки продемонстрував наявність дублюючих повноважень між різними правоохоронними органами та відсутність ефективних механізмів координації їхньої діяльності. Розподіл відповідальності за різні аспекти інформаційної безпеки між Національною поліцією, Службою безпеки України та Державною службою спеціаль-

ного зв'язку створює адміністративні бар'єри для оперативного реагування на кіберінциденти та знижує загальну ефективність системи захисту. Встановлено, що існуючі процедури виявлення, розслідування та усунення наслідків порушень інформаційної безпеки не відповідають сучасним вимогам та потребують кардинальної модернізації з урахуванням найкращих міжнародних практик.

Порівняльно-правовий аналіз міжнародного досвіду засвідчив перспективність адаптації європейських моделей адміністративно-правового регулювання інформаційної безпеки до українських умов. Особливо цінним є досвід створення спеціалізованих агенцій з кібербезпеки, запровадження єдиних технічних стандартів захисту інформації та формування ефективних механізмів державно-приватного партнерства у сфері інформаційної безпеки. Водночас механічне копіювання зарубіжних підходів без урахування специфіки української адміністративно-правової традиції та сучасних геополітичних викликів може виявитися неефективним, що зумовлює необхідність розробки оригінальних правових рішень.

На основі проведеного дослідження обґрунтовано, що вдосконалення адміністративно-правових механізмів забезпечення інформаційної безпеки у правоохоронній системі України потребує комплексного підходу, що включає: ухвалення спеціального закону про інформаційну безпеку правоохоронних органів; створення єдиного координаційного органу у сфері кібербезпеки; гармонізацію національного законодавства із вимогами європейських стандартів захисту даних; запровадження єдиних технічних стандартів та процедур забезпечення інформаційної безпеки; посилення адміністративної відповідальності порушення у цій сфері. Реалізація запропонованих заходів сприятиме підвищенню ефективності правоохоронної діяльності, зміцненню довіри громадян до державних інститутів та забезпеченню відповідності української правової системи міжнародним стандартам інформаційної безпеки.

ЛІТЕРАТУРА:

1. Бевзенко В.М. Адміністративно-правові засади інформаційної безпеки в Україні: монографія. Київ: Алерта, 2020. 368 с.

2. Баранов О.А. Правове забезпечення інформаційної безпеки: теорія і практика. Київ: Логос, 2019. 422 с.

3. Швець М.Я. Інформаційна безпека в системі державного управління України. Харків: Право, 2021. 298 с.

4. Anderson J. Cybersecurity in European Law Enforcement: Challenges and Opportunities. European Journal of Security Research. 2022. Vol. 7. P. 45-62.

5. Finnegan M., Lodge S. Digital Policing and Information Security in the EU. Cambridge University Press, 2021. 334 p.

6. Шевчук О., Ментух Н.Ф. Реалізація політики державної інформаційної безпеки України в контексті запобігання корупції: адміністративно-правовий аспект. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Випуск 64. С. 282–287. URL: http://visnyk-juris-uzhnu-uz.com/wp-content/ uploads/2021/06/ NVUzhNU_64.pdf

7. Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. Law, Policy and Security, 1(1), 4-17.

8. Clarke R. Cyber War and Peace: Hacking Can Reduce Real-World Violence. Foreign Affairs. 2021. Vol. 100(3). P. 132-146.

9. Landau S. Listening In: Cybersecurity in an Insecure Age. Yale University Press, 2020. 387 p.

10. Конституція України від 28 червня 1996 року № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

11. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

12. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 року № 447/2021. Офіційний вісник Президента України. 2021. № 17. Ст. 990.

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Official Journal of the European Union. 2016. L 119/1.

15. Convention on Cybercrime (Budapest Convention). Council of Europe Treaty Series. 2001. No. 185.
16. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.
17. Про Службу безпеки України: Закон України від 25 березня 1992 року № 2229-XII. Відомості Верховної Ради України. 1992. № 27. Ст. 382.
18. Про державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 258.
19. Типовий порядок організації та проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: затв. наказом Адміністрації Держспецзв'язку України від 28 березня 2012 року № 123. Офіційний вісник України. 2012. № 38. Ст. 1470.
20. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року № 8073-X. Відомості Верховної Ради УРСР. 1984. Додаток до № 51. Ст. 1122.

Дата першого надходження рукопису до видання: 21.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 26.09.2025