УДК 342.9:004.738.5:35.077.3
DOI https://doi.org/10.32782/pdu.2024.4.64

В. С. Крушеніцький
аспірант кафедри права та правоохоронної діяльності
Центральноукраїнського державного
університету імені Володимира Винниченка
ORCID ID: 0000-0001-9194-7897

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ РЕАГУВАННЯ НА ІНФОРМАЦІЙНІ ЗАГРОЗИ: ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ

У статті досліджено адміністративно-правові механізми реагування на інформаційні загрози в умовах сучасної цифрової трансформації та зростаючих гібридних викликів. Акцент зроблено на важливості інформаційної безпеки як складової національної безпеки України, що вимагає скоординованого та ефективного державного реагування.

Автором систематизовано нормативно-правову базу у сфері інформаційної безпеки, зокрема проаналізовано положення Конституції України, законів «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України» та інших ключових актів. Розкрито функціонування інституційного механізму через діяльність уповноважених державних органів, таких як РНБО України, Держспецзв'язок, Національний координаційний центр кібербезпеки, Міністерство цифрової трансформації України.

Особливу увагу приділено контрольним та наглядовим механізмам, методам колегіального контролю, інструментам адміністративної відповідальності, сертифікації, ліцензування, дозвільної діяльності та процедурі реєстрації засобів масової інформації. Вказано, що адміністративна відповідальність є ефективним засобом реагування на правопорушення у сфері інформаційної безпеки. Автор наголошує, що ефективність цих механізмів безпосередньо залежить від рівня нормативної чіткості, міжвідомчої координації та цифрової спроможності органів влади.

У статті запропоновано шляхи удосконалення адміністративно-правових засобів, серед яких: гармонізація законодавства з міжнародними стандартами, розвиток цифрових платформ для обміну інформацією, підвищення кваліфікації кадрів, а також впровадження інноваційних технологій у процеси виявлення та нейтралізації інформаційних загроз.

Ключові слова: *інформаційна безпека, інформаційні загрози, адміністративне право, адміністративно-правові механізми, кібербезпека, нормативно-правове регулювання, державне управління, національна безпека, дезінформація, гібридна війна, цифровізація, контроль і нагляд, правова відповідальність, інституційний механізм, інформаційне законодавство.*

Постановка проблеми. У сучасних умовах активного розвитку цифрових технологій, глобалізації інформаційного простору та зростання гібридних загроз, питання інформаційної безпеки держави набуває особливої актуальності. Інформаційні загрози можуть набирати різноманітних форм – від поширення дезінформації та фейкових новин до кіберзлочинності та інформаційно-психологічного впливу на суспільну свідомість.

У зв'язку з цим виникає потреба у формуванні ефективних адміністративно-правових механізмів реагування на такі загрози. Проте, на сьогоднішній день нормативно-правова база України у сфері інформаційної безпеки ще не є достатньо цілісною та систематизованою. Адміністративно-правові засоби протидії інформаційним загрозам мають фрагментарний характер, а відповідні повноваження державних органів іноді перетинаються або є неузгодженими.

Теоретико-правовий аспект проблеми полягає у необхідності комплексного осмислення природи інформаційних

загроз як об'єкта адміністративно-правового регулювання, визначення чіткого правового статусу суб'єктів протидії, а також формування ефективного механізму координації дій на рівні державного управління.

Таким чином, дослідження адміністративно-правових механізмів реагування на інформаційні загрози є важливою складовою забезпечення національної безпеки України і потребує як науково-теоретичного осмислення, так і практичної реалізації через вдосконалення законодавства.

Аналіз останніх досліджень та публікацій. Вивченню різних аспектів у сфері інформаційної безпеки присвячені роботи українських вчених: В. Антонюка, І. Арістової, І. Березовської, М. Биченка, Н. Бортник, В. Грищенка, М. Гуцалюка, Б. Демидова, О. Довгань, Я. Жаркова, В. Зайцева. І. Замаруєва, С. Єсімова, Р. Калюжного, Б. Кормича, О. Кохановської, В. Ліпкан, Г. Линник, О. Литвиненка, П. Мельника, В. Негодченка, О. Олійника, Д. Русака, Т. Перуна, Т. Слінько, Д. Федченка, В. Цимбалюка, В. Шамрая, М. Швеця, Ю. Яцишина та багатьох інших.

Метою статті є всебічне дослідження адміністративно-правових механізмів реагування на інформаційні загрози в умовах цифровізації суспільства та зростання гібридних загроз.

Виклад основного матеріалу. У нормативно-правовому полі України питання інформаційної безпеки набуло особливої ваги в умовах гібридної війни, глобалізації та цифровізації суспільства. Визначальним документом у цій сфері є Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року, в якій інформаційні загрози визначаються як потенційно або реально негативні явища, тенденції та чинники, що діють в інформаційному середовищі з метою ускладнення чи унеможливлення реалізації національних інтересів і збереження національних цінностей. Ці загрози можуть завдати як прямої, так і опосередкованої шкоди інтересам держави, її національній безпеці й обороноздатності [1; 2, с. 264].

У науковій доктрині також спостерігається спроба систематизації поняття «інформаційна загроза». Так, В. В. Антонюк визначає її як умови та фактори, що можуть призвести до порушення основних параметрів інформації – конфіденційності, цілісності, доступності, – у тому числі й тієї, яка циркулює в інформаційних системах і забезпечує потреби громадян, державних інституцій та комерційних структур [3; 2, с. 264]. Таке трактування дозволяє розглядати інформаційні загрози не лише в контексті зовнішнього втручання, а й внутрішньої нестабільності інформаційного середовища.

У свою чергу, О. В. Скочиляс-Павлів підкреслює, що інформаційні загрози охоплюють потенційно небезпечні події або явища, які здатні поставити під ризик не лише інформаційні ресурси, а й саму структуру національної безпеки, через вплив на соціальну стабільність, громадську думку та стратегічне управління державою [2, с. 264].

Системно аналізуючи нормативні і наукові підходи можемо дійти висновку, що інформаційні загрози – це багатовимірне явище, яке поєднує технічні, соціальні, політичні та правові аспекти. Їхній вплив виходить за межі інформаційної сфери, безпосередньо зачіпаючи національну безпеку та сталий розвиток держави.

Безумовно інформаційна безпека є складним, системним та багаторівневим явищем, яке перебуває під впливом постійного впливу чинників внутрішнього та зовнішнього середовища, з врахуванням політичної світової обстановки, мікроклімату в середині самої держави, стану та рівня інформацій-комунікаційної обстановки держав світу. Наявність загроз, які стосуються інформаційної безпеки більшою мірою супроводжуються існуванням загроз в економічній, політичній, державно-управлінській та інших сферах. Загрози, які виникають в інформаційній сфері зумовлені загрозам, які інших сфер, які мають дотичний характер до інформації, і за рахунок інформаційних ресурсів несуть руйнівні наслідки [4, с. 156].

Адміністративно-правові механізми реагування на інформаційні загрози відіграють вагоме значення у формуванні ефективної державної політики забезпечення інформаційної безпеки, оскільки

саме через них здійснюється реалізація нормативно-правових приписів, контроль за дотриманням інформаційного законодавства, превентивна діяльність та оперативне втручання у випадках виникнення загроз.

Адміністративно-правові механізми реагування на інформаційні загрози регулюються низкою нормативно-правових актів. Основу правового регулювання становить Конституція України, яка гарантує право на інформацію та захист від незаконного втручання в особисте життя (статті 32, 34) [5]. Закон України «Про інформацію» визначає основи інформаційних відносин, права і обов'язки суб'єктів інформаційної діяльності [6]. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регламентує захист інформації, оброблюваної в IT-середовищах [7], а Закон України «Про основні засади забезпечення кібербезпеки України» встановлює принципи, організаційну структуру та повноваження органів у сфері кібербезпеки [8] . Кодекс України про адміністративні правопорушення передбачає адміністративну відповідальність за правопорушення у сфері інформаційної безпеки (зокрема, ст. 212-3, 212-6, 212-7).

До ключових адміністративно-правових механізмів забезпечення інформаційної безпеки слід віднести насамперед систему нормативно-правового регулювання, яка включає в себе розроблення та прийняття законодавчих актів, підзаконних нормативно-правових документів, інструкцій, положень і стандартів. Ці документи встановлюють загальні принципи, правила і процедури, що регламентують порядок захисту інформації, а також механізми реагування на інциденти у сфері інформаційної безпеки. Нормативне регулювання відіграє роль основоположного інструменту, який забезпечує легітимність усіх інших форм державного впливу в цій сфері.

Інституційний механізм реалізується через діяльність уповноважених державних органів, зокрема Ради національної безпеки і оборони України, Державної служби спеціального зв'язку та захисту інформації, Національного координаційного центру кібербезпеки, Міністерства цифрової трансформації України. Зазначені органи здійснюють стратегічне планування, оперативне управління та координацію заходів у сфері інформаційної безпеки, що дозволяє забезпечити цілісність, системність та безперервність державної політики в цій сфері.

Окрему групу адміністративно-правових засобів становлять контрольні та наглядові функції, що включають моніторинг інформаційного простору, проведення аудитів у сфері кібербезпеки, інспекцій, перевірок об'єктів критичної інфраструктури. Серед них особливе значення має метод колегіальності контролю за додержанням режиму секретності, який полягає у проведенні систематичних колегіальних перевірок (внутрішньооб'єктових, галузевих, відомчих, загальнодержавних) із залученням представників уповноважених органів. Як зазначає О. Олійник, такий підхід дозволяє досягти об'єктивності та повноти перевірки дотримання вимог конфіденційності на всіх рівнях управління [9].

Адміністративна відповідальність є ефективним засобом реагування на правопорушення у сфері інформаційної безпеки. Вона реалізується через механізми притягнення порушників до відповідальності шляхом накладення штрафів, застосування адміністративного арешту, попереджень тощо, що виконує як каральну, так і превентивну функцію.

До важливих адміністративно-правових інструментів належать також механізми ліцензування та дозвільної діяльності. Вони забезпечують допуск до окремих видів діяльності лише тих суб'єктів, які відповідають визначеним критеріям безпеки, зокрема під час обробки конфіденційної чи захищеної інформації. Водночас системна робота з інформування та навчання кадрів є передумовою ефективного функціонування всієї системи інформаційної безпеки. Проведення освітніх заходів, професійної перепідготовки та підвищення кваліфікації персоналу сприяє зменшенню кількості кіберінцидентів та загроз людського фактора.

Окреме місце посідає сертифікація технічних і програмних засобів захисту інформації, а також діяльності, пов'язаної

із забезпеченням охорони державної таємниці. Цей процес має бути максимально жорстко регламентованим та контрольованим з боку держави, оскільки йдеться про національну безпеку.

Реєстраційний метод, у свою чергу, виступає складовою контрольно-наглядової діяльності виконавчої влади. Наприклад, згідно зі ст. 4 Закону України «Про друковані засоби масової інформації (пресу) в Україні», державна реєстрація ЗМІ є обов'язковою передумовою для початку їхньої діяльності. Процедура включає подання заяви, її розгляд протягом встановленого терміну, ухвалення рішення про реєстрацію або відмову, а також повідомлення про виявлені недоліки в документах [10]

Висновок. Для підвищення ефективності адміністративно-правових механізмів доцільним є впровадження міжвідомчих платформ обміну інформацією, зміцнення координації між виконавчими органами, а також поступова гармонізація вітчизняного законодавства із нормами права Європейського Союзу та стандартами НАТО.

Також, необхідно впроватити низку захолів. По-перше, необхідно запровадити ризик-орієнтований підхід у системі державного управління, який дозволить ефективно і раціонально розподіляти ресурси відповідно до рівня загроз. По-друге, слід цифровізувати адміністративні процедури у сфері контролю, включно з онлайн-реєстрацією, автоматизацією звітності та перевірок, що зменшить вплив людського фактора й підвищить прозорість. Також важливо створити єдиний реєстр кіберінцидентів та правопорушень, який стане інструментом для аналітики, виявлення повторюваних загроз та вироблення запобіжних заходів. Крім того, слід розвивати міжсекторне партнерство між державою, бізнесом і наукою, що сприятиме модернізації технічних рішень і вдосконаленню правозастосовної практики. Посилення юридичної відповідальності, включно з введенням персоніфікованих санкцій та прогресивної шкали штрафів за порушення у сфері інформаційної безпеки, має підвищити превентивний ефект адміністративних заходів. Доцільним також є створення Центру компетенцій з адміністративного права у сфері кібербезпеки, який забезпечуватиме методичну, аналітичну та консультативну підтримку органам влади. Нарешті, варто запровадити системний моніторинг виконання Україною міжнародних зобов'язань у сфері кібербезпеки, що дозволить підвищити рівень правової сумісності, прозорості та стратегічного партнерства на міжнародному рівні. Реалізація зазначених заходів сприятиме підвищенню ефективності адміністративно-правового забезпечення інформаційної безпеки та адаптації правової системи до сучасних викликів цифрової епохи.

Список використаної літератури:

1. Стратегія інформаційної безпеки від 28 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7
2. Скочиляс-Павлів О.В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. *Юридичний науковий електронний журнал*. 2023. №9. С. 263-266.
3. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. *Державне управління: удосконалення та розвиток*. 2014. № 8. С. 22–27.
4. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір. 2021. № 176. С. 155-158.
5. Конституція України від 28.06.1996 № 254к/96-ВР. URL : https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80
6. Про інформацію: Закон України від 2 жовтня 1992 року №2657-XII. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 р. №80/94-ВР. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed19940705#Text
8. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Олійник О. В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних

ресурсів. *Право і безпека.* 2014. № 1(52). С. 103–109.
10. Чистоклетов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки України. *ІТ-право: проблеми та перспективи розвитку в Україні:* Зб. матеріалів ІІ-ї Міжнар. наук.-практ. конф. (Львів, 17 листоп. 2017 р.). Львів, 2017. С. 212–217.

Krushenitskyi V. S. Administrative and legal mechanisms of responding to information threats: theoretical and legal aspect

The article examines the administrative and legal mechanisms for responding to information threats in the context of modern digital transformation and growing hybrid challenges. Emphasis is placed on the importance of information security as a component of Ukraine's national security, which requires a coordinated and effective state response.

The author systematizes the regulatory framework in the field of information security, in particular, analyzes the provisions of the Constitution of Ukraine, the laws «On Information», «On Information Protection in Information and Telecommunications Systems», «On the Basic Principles of Ensuring Cybersecurity of Ukraine» and other key acts. The functioning of the institutional mechanism is revealed through the activities of authorized state bodies, such as the National Security and Defense Council of Ukraine, the State Service for Special Communications, the National Coordination Center for Cybersecurity, and the Ministry of Digital Transformation of Ukraine.

Particular attention is paid to control and supervisory mechanisms, methods of collegial control, instruments of administrative responsibility, certification, licensing, permitting activities and the procedure for registering mass media. The author emphasizes that the effectiveness of these mechanisms directly depends on the level of regulatory clarity, interdepartmental coordination and digital capacity of government bodies. It is indicated that administrative liability is an effective means of responding to offenses in the field of information security.

The article proposes ways to improve administrative and legal means, including: harmonization of legislation with international standards, development of digital platforms for information exchange, improvement of personnel skills, as well as the introduction of innovative technologies into the processes of identifying and neutralizing information threats.

Key words: *information security, information threats, administrative law, administrative and legal mechanisms, cybersecurity, regulatory and legal regulation, public administration, national security, disinformation, hybrid warfare, digitalization, control and supervision, legal responsibility, institutional mechanism, information legislation.*