УДК 351.86:004.056:342.9

А. П. Лелеченко,
д. держ. упр., професор, професор кафедри публічного управління та адміністрування,
Національний університет "Київський авіаційний інститут"
ORCID ID: https://orcid.org/0000-0002-0850-3724
М. В. Кочеров,
д. ю. н., професор кафедри публічного управління та адміністрування,
Національний університет "Київський авіаційний інститут"
ORCID ID: https://orcid.org/0000-0001-8687-8604

DOI: 10.32702/2306-6814.2026.5.302

МЕХАНІЗМИ ДЕРЖАВНОГО РЕАГУВАННЯ НА ІНФОРМАЦІЙНІ ВИКЛИКИ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

A. Lelechenko,
Doctor of Science in Public Administration, Professor, Professor of the Department of Public Management and Administration, The National University "Kyiv Aviation Institute"
M. Kocherov,
Doctor of Science of Law,
Professor of the Department of Public Management and Administration, The National University "Kyiv Aviation Institute"

MECHANISMS OF STATE RESPONSE TO INFORMATION CHALLENGES IN THE CONTEXT OF NATIONAL SECURITY

У статті проаналізовано механізми державного реагування на інформаційні виклики у контексті національної безпеки та окреслено їхню структурну конфігурацію як цілісної системи, здатної забезпечувати ефективну протидію сучасним гібридним загрозам. Обгрунтовано, що інформаційні виклики, включаючи дезінформацію, маніпулятивні інформаційні впливи та інформаційно-психологічні операції, чинять значний вплив на стабільність державних інститутів, процеси ухвалення рішень і формування суспільних настроїв, що обумовлює необхідність системного підходу до організації державного реагування. Встановлено, що механізми державного реагування мають дві взаємопов'язані складові: інституційно-нормативний та ресурсно-технологічний виміри. Інституційно-нормативний блок включає нормативно-правовий механізм, організаційно-функціональний розподіл повноважень і відповідальності, а також механізм міжвідомчої координації. Показано, що саме інституційно-нормативний вимір визначає правила, межі та процедури діяльності суб'єктів реагування, формує правові передумови для взаємодії та координації між державними органами і спеціалізованими підрозділами, а також забезпечує юридичну визначеність і системність реагування на інформаційні виклики. Визначено, що ресурсно-технологічний вимір включає кадровий потенціал, фінансове забезпечення та технологічні інструменти, що дозволяють реалізувати інституційні правила на практиці. Обгрунтовано, що кадровий механізм формує професійні компетентності, спеціалізацію та аналітичні спроможності суб'єктів реагування, фінансовий механізм забезпечує стабільність ресурсного наповнення, розвиток аналітичної та технологічної інфраструктури, техніко-технологічний механізм інтегрує цифрові платформи, аналітичні системи та інструменти моніторингу інформаційного простору, що скорочує час від виявлення загрози до ухвалення контрзаходів.

Узагальнено структурну конфігурацію механізмів державного реагування, що демонструє взаємозв'язок інституційно-нормативного та ресурсно-технологічного вимірів, їхню взаємодію та принципову роль для забезпечення ефективності державного реагування на інформаційні виклики у контексті національної безпеки.

The article analyses the mechanisms of state response to information challenges within the context of national security and outlines their structural configuration as an integrated system capable of ensuring effective counteraction to contemporary hybrid threats. It substantiates that information challenges, including disinformation, manipulative information influence, and information-psychological operations, exert a significant impact on the stability of state institutions, decision-making processes, and the formation of public attitudes, thereby necessitating a systemic approach to the organisation of state response. The study establishes that the mechanisms of state response comprise two interrelated dimensions: the institutional-regulatory and the resource-technological. The institutional-regulatory block includes the legal-regulatory mechanism, the organisational-functional distribution of powers and responsibilities, and the mechanism of interagency coordination. It is demonstrated that the institutional-regulatory dimension defines the rules, boundaries, and procedures governing the activities of response actors, forms the legal preconditions for interaction and coordination among public authorities and specialised units, and ensures legal certainty and systemic coherence in responding to information challenges. The resource-technological dimension is defined as encompassing human resource capacity, financial support, and technological instruments that enable the practical implementation of institutional rules. It is substantiated that the human resource mechanism develops professional competencies, specialisation, and analytical capacities of response actors; the financial mechanism ensures the stability of resource provision and the development of analytical and technological infrastructure; while the technical-technological mechanism integrates digital platforms, analytical systems, and information-space monitoring tools, thereby reducing the time between threat detection and the adoption of countermeasures. A generalised classification of state response mechanisms is presented, demonstrating the interconnection between the institutional-regulatory and resource-technological dimensions, their interaction, and their fundamental role in ensuring the effectiveness of state responses to information challenges within the national security framework.

Ключові слова: державне реагування, інформаційні виклики, національна безпека, інституційно-нормативний вимір, ресурсно-технологічний вимір, кадровий потенціал, фінансове забезпечення, технологічні платформи, міжвідомча координація.

Key words: state response, information challenges, national security, institutional and regulatory dimension, resource and technological dimension, human resource capacity, financial support, technological platforms, interagency coordination.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах загострення загроз національній безпеці інформаційні виклики посідають одне з провідних місць у системі факторів, що впливають на стабільність держави та ефективність функціонування її інститутів. Дезінформація, маніпулятивні інформаційні впливи, інформаційно-психологічні операції та цілеспрямоване викривлення суспільно значущої інформації використовуються як інструменти тиску на процеси ухвалення державних рішень, формування суспільних настроїв і підрив довіри до органів державної влади. За таких умов держава змушена розглядати реагування на інформаційні виклики як складову забезпечення національної безпеки, що потребує системного підходу та чітко вибудуваних механізмів. Актуальність дослідження зумовлена необхідністю підвищення спроможності держави до своєчасного та ефективного реагування на інформаційні виклики в умовах гібридного протиборства та тривалих кризових процесів. Практика свідчить, що наявність окремих нормативних актів або організаційних рішень не гарантує результативності державного реагування за відсутності узгодженої системи механізмів його реалізації. Недостатня чіткість нормативно-правового регулювання, розпорошення функцій між суб'єктами реагування, обмеженість кадрових і фінансових ресурсів, а також технологічна аси-

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

метрія у можливостях моніторингу та аналізу інформаційного простору знижують ефективність протидії інформаційним загрозам.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика державного реагування на інформаційні виклики у контексті національної безпеки активно досліджується в сучасній науковій літературі, однак переважна більшість робіт зосереджується на аналізі окремих компонентів інформаційної безпеки, без формування цілісного уявлення про структуру та взаємодію механізмів державного реагування. Значний масив досліджень присвячений нормативно-правовим засадам забезпечення інформаційної безпеки. У працях А. Ряполова (2025) [1], О. Скочиляс-Павлів (2024) [2], А. Гріщенка (2020) [3] розкрито еволюцію правового регулювання інформаційної безпеки в Україні, окреслено проблеми адаптації правових норм до умов гібридних загроз. Окремий вимір правового регулювання інформаційної безпеки представлено в роботі І. Брацука та С. Кавина (2023) [4], де акцент зроблено на міжнародно-правових механізмах, сформованих у межах системи ООН. У низці досліджень увага приділяється інституційному та організаційному аспектам інформаційної безпеки. Зокрема, В. Крушеніцький (2024) [5] аналізує роль органів публічної влади як суб'єктів формування і реалізації політики національної безпеки в інформаційному просторі; колективна праця С. Балана, Л. Балан та ін. (2025) [6] розкриває політико-правові засади державної інформаційної політики в умовах гібридних загроз. Ресурсно-фінансові та економічні компоненти забезпечення кібербезпеки досліджуються у працях А. Маццокколі та М. Нальді (2021) [9]. Аналітичні документи міжнародних інституцій акцентують увагу на практичних інструментах державного реагування, зокрема розвитку кадрового потенціалу, інституційної спроможності та технологічних стандартів. Відповідні підходи окреслено у звітах Європейської Комісії щодо розбудови кіберспроможностей держав, аналітичних матеріалах з фінансової стійкості кіберпростору, ресурсного забезпечення та публічно-приватної взаємодії [8; 10]. Методологічні засади технологічного реагування систематизовано у "Рамці кібербезпеки 2.0" (2024) [11] Національного інституту стандартів і технологій США.

ПОСТАНОВКА ЗАВДАННЯ

Формулювання цілей статті (постановка завдання) — комплексний аналіз механізмів державного реагування на інформаційні виклики у контексті національної безпеки та систематизація інституційно-нормативних і ресурсно-технологічних вимірів їх функціонування, що формують належний рівень забезпечення національної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Інституційно-нормативний вимір державного реагування на інформаційні виклики формує базові умови функціонування всієї системи забезпечення інформаційної безпеки у контексті національної безпеки. Саме в межах цього виміру визначаються правила, межі та процедури діяльності державних органів, закріплюються їхні повноваження й відповідальність, а також створюються правові передумови для координації реагування на інформаційні загрози. Основним елементом зазначеного виміру є нормативно-правовий механізм, який забезпечує формалізацію державного реагування та надає йому інституційно закріпленого характеру.

Нормативно-правовий механізм державного реагування на інформаційні виклики охоплює сукупність правових норм, що визначають засади захисту інформаційного простору, порядок дій у разі виникнення загроз, а також юридичні наслідки порушення встановлених правил у сфері інформаційної безпеки. У наукових дослідженнях цей механізм розглядається як системно організований комплекс, покликаний забезпечити стабільність, передбачуваність і результативність державного реагування.

Зокрема, А. П. Ряполов, аналізуючи нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії [1], підкреслює, що чинне законодавство формує необхідну правову базу для протидії дезінформації та іншим інформаційним впливам, що загрожують національній безпеці. Водночас автор звертає увагу на те, що ефективність нормативно-правового механізму визначається не лише кількістю та формальною наявністю правових норм, а їхньою здатністю адаптуватися до динаміки сучасних інформаційних загроз і забезпечувати баланс між інтересами безпеки та дотриманням фундаментальних прав і свобод людини.

Системний характер нормативно-правового механізму акцентується також у дослідженні О. Скочиляс-Павлів [2], де правові норми розглядаються як центральний елемент механізму забезпечення інформаційної безпеки держави. Автор доводить, що саме якісне нормативне регулювання визначає правила діяльності суб'єктів у сфері інформаційної безпеки, встановлює порядок моніторингу та реагування на інформаційні загрози, а також формує правові підстави для притягнення до відповідальності за порушення у цій сфері. Важливим є й підкреслений у роботі взаємозв'язок правових механізмів із політичними та техніко-технологічними компонентами реагування, що дозволяє розглядати нормативно-правовий механізм як інтегровану частину системи державного реагування у цій сфері.

Нормативно-правовий механізм встановлює рамку інформаційних відносин. Як зазначає А. Гріщенко [3], правові підходи до розуміння інформаційної безпеки формують юридичні стандарти захисту інформації, визначають коло суб'єктів відповідних правовідносин та обсяг їхніх прав і обов'язків. Це дозволяє розглядати інформаційну безпеку не лише як технічну або політичну категорію, а як правовий інститут, що має чітко визначені межі та механізми реалізації.

Окрім цього, нормативно-правовий механізм забезпечує регламентацію процедур державного реагування на інформаційні виклики. Через правові норми визначаються алгоритми дій органів державної влади у разі виявлення інформаційних загроз,

встановлюються підстави для застосування спеціальних режимів реагування та врегульовується порядок взаємодії суб'єктів у кризових ситуаціях. Саме в такому контексті законодавство у сфері національної безпеки створює правові умови для функціонування спеціалізованих інституцій реагування, зокрема органів, відповідальних за протидію дезінформації.

Важливою складовою нормативно-правового механізму є також забезпечення юридичної відповідальності за порушення норм інформаційної безпеки. Застосування адміністративних, цивільно-правових або кримінально-правових санкцій за поширення дезінформації, несанкціонований доступ до інформаційних систем або інші дії, що завдають шкоди національній безпеці, виступає стримувальним і регулятивним інструментом державного реагування. У цьому контексті показовими є дослідження І. Брацук та С. Кавина [4], які, аналізуючи міжнародно-правове регулювання інформаційної безпеки в рамках ООН, підкреслюють значення узгоджених правових норм і механізмів відповідальності для протидії транснаціональним інформаційним загрозам та гармонізації національних правових систем.

Таким чином, нормативно-правовий механізм державного реагування на інформаційні виклики формує інституційну основу для функціонування всієї системи реагування, забезпечуючи правову визначеність, процедурну впорядкованість та можливість реалізації державної політики у сфері національної безпеки в умовах сучасних інформаційних загроз.

Однак самі правові норми не забезпечують належної реалізації державного реагування за відсутності чіткої організаційної структури, визначеного розподілу функцій та відповідальності між суб'єктами, залученими до забезпечення інформаційної безпеки. У цьому контексті організаційно-функціональний механізм виступає ключовою ланкою, що трансформує нормативні положення у практичну діяльність органів державної влади та спеціалізованих структур. Організаційно-функціональний механізм розподілу повноважень і відповідальності визначає, які саме державні органи, за якими напрямами відповідальності і в якій послідовності діють під час виявлення, аналізу й реагування на інформаційні виклики. В українській науковій літературі ця проблема розглядається здебільшого в контексті необхідності узгодженого функціонування широкого кола суб'єктів інформаційної безпеки. Так, у дослідженні В. Крушеніцького [5] наголошується на важливості чіткого розподілу функцій між відповідними структурами державної влади, що формують державну політику у сфері та реалізують конкретні заходи щодо захисту інформаційного простору.

За категоріальною сутністю організаційно-функціональний механізм виступає як система визначення ролей і відповідальності суб'єктів, що входять до національної системи інформаційної безпеки. Це не лише формальний перелік відповідальних органів, а й структуровані процеси взаємодії між ними, які забезпечують оперативне реагування на загрози: від ідентифікації інформаційного впливу до його нейтралізації. Таким чином, організаційно-функціональний механізм трансформує встановлені в нормативних актах правила в структуровану діяльність суб'єктів державного реагування, визначаючи порядок і послідовність їхніх дій у відповідь на інформаційні виклики, що виступає ключовою умовою результативності державної політики інформаційної безпеки.

Проте ефективність такої системи неможлива без чітко налагоджених механізмів міжвідомчої координації, які забезпечують обмін інформацією, синхронізацію дій та узгоджене оперативне прийняття управлінських рішень. Саме міжвідомча координація виступає тим ключовим "зв'язком", що перетворює окремі повноваження та функції в цілісну, скоординовану систему реагування на загрози, слугує засобом узгодження політик, процесів і дій між різними державними структурами, які мають спільні або взаємопов'язані завдання щодо виявлення, аналізу та нейтралізації інформаційних викликів. У науковому дискурсі наголошується, що координація — це не просто обмін даними, а складний механізм взаємодії, що включає спільне планування, розподіл відповідальності та узгодження оперативних заходів між суб'єктами безпекового сектору. Такий підхід передбачає створення спеціальних міжвідомчих структур або робочих груп, які наділені повноваженнями забезпечувати системне реагування на складні інформаційні виклики.

В Україні практичний вимір міжвідомчої координації у сфері державного реагування на інформаційні виклики, зокрема в умовах гібридних загроз, все більше привертає увагу науковців і практиків [6]. Сучасні дослідження вказують на необхідність вдосконалення механізмів міжвідомчої координації як одного з ключових факторів підвищення спроможності держави реагувати на інформаційні виклики. Методологічно механізм міжвідомчої координації розглядається як сукупність процедур, інструментів комунікації та організаційних форматів, що дозволяють різним суб'єктам безпекового сектору узгоджувати свої дії у режимах повсякденної діяльності та в кризових ситуаціях [7]. Таким чином, механізм міжвідомчої координації забезпечує інтеграцію діяльності суб'єктів державного реагування у досліджуваній сфері, що є важливим фактором посилення ефективності державної політики умовах сучасних гібридних загроз.

Інституційно-нормативний вимір державного реагування на інформаційні виклики потребує ресурсного та технологічного забезпечення, що включає кадрові компетентності, фінансові можливості і сучасні технічні інструменти. Ці елементи становлять ресурсно-технологічний вимір, який функціонує як механізм реалізації та операціоналізації державної політики у відповідь на інформаційні загрози.

Ресурсно-кадровий механізм становить базову складову ресурсно-технологічного виміру державного реагування на інформаційні виклики, оскільки саме людський капітал визначає здатність держави трансформувати нормативні та організаційні рішення у ре-

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

альні управлінські дії. У наукових дослідженнях кадровий ресурс розглядається не лише як сукупність посад і функцій, а як система професійних компетентностей, спеціалізації та аналітичних спроможностей, необхідних для виявлення, оцінювання та нейтралізації інформаційних загроз у динамічному середовищі.

У цьому контексті концепція "capacity building" (розвиток потенціалу) набула статусу основної аналітичної рамки для оцінювання спроможності держав реагувати на інформаційні та кіберзагрози. У звіті "Розвиток міжнародного кіберпотенціалу: глобальні тенденції та сценарії" (International cyber capacity building: global trends and scenarios) Європейської Комісії (2021) [8] кадровий потенціал визначається як один із критичних вимірів національної кібер- та інформаційної безпеки поряд із правовими й технологічними інструментами. Експерти наголошують, що ефективне реагування держави на інформаційні виклики потребує системної підготовки державних службовців, формування спеціалізованих навчальних програм, розвитку міждисциплінарних компетентностей, а також інституціоналізації міжнародного обміну досвідом у сфері інформаційної безпеки. Саме кадровий потенціал розглядається як умова реалізації державної політики реагування в умовах гібридних загроз.

Водночас кадровий потенціал не може функціонувати автономно без належного фінансового забезпечення, що зумовлює перехід до аналізу фінансового механізму державного реагування. Фінансовий механізм у цьому вимірі виконує системоутворювальну функцію, оскільки забезпечує можливість підтримки професійної підготовки кадрів, розвитку аналітичної та технологічної інфраструктури, а також реалізації превентивних і реактивних заходів у сфері інформаційної безпеки.

Попри обмежену кількість спеціалізованих українських досліджень, економічні моделі інвестування у кібербезпеку, розроблені в зарубіжній науковій літературі, створюють теоретичне підгрунтя для аналізу державних фінансових рішень у цій сфері. Зокрема, у дослідженні А.Маццокколі та М.Налді (2021) [9] обгрунтовується підхід до оптимального інвестування у кібербезпеку з урахуванням співвідношення між витратами на захист і потенційними втратами від інформаційних інцидентів. Хоча автори аналізують поведінку багатопрофільних компаній, запропонована модель дозволяє екстраполювати ці висновки на державний рівень, де фінансові ресурси також мають розподілятися з урахуванням ризиків, імовірності загроз та стратегічних пріоритетів.

Міжнародні аналітичні звіти підкреслюють значення фінансового механізму як інструменту підтримки стійкості державних систем безпеки. У "Звіті про кібербезпеку та стійкість фінансової системи" (Cybersecurity and Financial System Resilience Report, 2024) [10] Федеральної резервної системи США фінансове забезпечення розглядається як критичний чинник забезпечення довгострокової стійкості до цифрових загроз. У документі наголошується на необхідності поєднання державних інвестицій із розвитком публічно-приватних партнерств, що дозволяє розширювати технологічні можливості реагування без надмірного навантаження на державний бюджет.

У структурі державного реагування фінансовий механізм виконує низку взаємопов'язаних функцій: забезпечує фінансування підготовки та сертифікації фахівців, підтримує розвиток аналітичних центрів і спеціалізованих підрозділів, створює умови для впровадження інноваційних технологій і стимулює кооперацію з приватним сектором у сфері інформаційної безпеки.

У сучасних умовах технології відіграють вирішальну роль у реалізації державних політик безпеки. Зокрема, техніко-технологічний механізм, який безпосередньо забезпечує операціоналізацію державного реагування. У сучасних умовах саме технології визначають швидкість, точність і масштабність реакції на інформаційні виклики. Техніко-технологічний механізм охоплює цифрові платформи моніторингу інформаційного простору, аналітичні системи обробки великих масивів даних, інструменти автоматизованого виявлення загроз і підтримки управлінських рішень.

Методологічною основою для аналізу цього механізму виступає "Рамка кібербезпеки 2.0" (Cybersecurity Framework 2.0), розроблена Національним інститутом стандартів і технологій США (NIST) [11]. У цьому документі технологічні інструменти розглядаються як складова цілісної системи управління ризиками, що інтегрує технічні, організаційні та людські компоненти реагування. Особливий акцент зроблено на безперервному моніторингу, аналітиці в реальному часі та координації інформаційних потоків між різними суб'єктами безпеки, що є критично важливим для протидії інформаційним атакам.

Таким чином, техніко-технологічний механізм виступає каталізатором швидких управлінських рішень, оскільки скорочує часовий розрив між фіксацією інформаційного впливу та ухваленням контрзаходів. У поєднанні з кадровими та фінансовими механізмами він формує цілісну основу для державного реагування на інформаційні виклики.

Проведений аналіз інституційно-нормативного та ресурсно-технологічного вимірів державного реагування на інформаційні виклики дозволяє стверджувати, що ефективність реагування формується цілісною конфігурацією взаємопов'язаних механізмів. Інституційно-нормативний блок механізмів забезпечує формування правил, розподіл повноважень та координацію суб'єктів реагування. Ресурсно-технологічний блок створює умови для практичної реалізації цих правил через кадрові, фінансові та технічні спроможності. Узгодженість зазначених механізмів є принципово важливою, оскільки нормативна визначеність без ресурсного наповнення не трансформується у дієве реагування, так само як наявність ресурсів без чітких інституційних рамок породжує фрагментарність і неузгодженість дій. Структура механізмів державного реагування на інформаційні вик-

Таблиця 1. Структура механізмів державного реагування на інформаційні виклики у контексті національної безпеки

Вимір державного реагування	Механізм	Функціональне призначення
Інституційно-нормативний вимір	Нормативно-правовий механізм	Формування правових засад реагування; визначення процедур, повноважень і відповідальності у сфері інформаційної безпеки
	Організаційно-функціональний механізм	Розподіл компетенцій між суб'єктами реагування; закріплення структури, функцій та меж відповідальності у системі забезпечення національної безпеки
	Механізм міжвідомчої координації	Забезпечення узгодженості дій органів державної влади у сфері забезпечення національної безпеки; інтеграція інформаційних потоків і спільне реагування на загрози
Ресурсно-технологічний вимір	Ресурсно-кадровий механізм	Формування професійної спроможності суб'єктів реагування; розвиток компетентностей і спеціалізації
	Фінансовий механізм	Забезпечення сталого фінансування заходів інформаційної безпеки; підтримка кадрового і технологічного розвитку
	Техніко-технологічний механізм	Операціоналізація реагування через цифрові платформи, аналітичні системи та моніторинг інформаційного простору

Джерело: складено автором.

лики у контексті національної безпеки наведена у таблиці 1.

Таким чином, державне реагування на інформаційні виклики у контексті національної безпеки доцільно розглядати як багатокомпонентну систему, що поєднує інституційно-нормативні та ресурсно-технологічні механізми. Інституційно-нормативний вимір формує регулятивне та організаційне середовище реагування, визначаючи правила, суб'єктів і координаційні зв'язки. Ресурсно-технологічний вимір забезпечує практичну здатність держави реалізовувати ці правила шляхом залучення професійних кадрів, фінансових ресурсів і сучасних технологічних інструментів.

Визначена структура демонструє системність державного реагування як цілісної архітектури, спроможної адаптуватися до динамічних інформаційних загроз. Запропонована класифікація механізмів може слугувати аналітичною основою для подальших досліджень ефективності державного реагування, а також для вдосконалення практичного їх застосування.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Підсумовуючи зазначимо, що ефективність державного реагування на інформаційні виклики у контексті національної безпеки забезпечується скоординованою взаємодією інституційно-нормативного та ресурсно-технологічного компонентів. Узгоджена робота нормативно-правових, організаційно-функціональних і координаційних механізмів у поєднанні з кадровим, фінансовим та технологічним ресурсним забезпеченням формує цілісну архітектуру реагування, здатну адаптуватися до динаміки сучасних інформаційних загроз. Перспективними напрямами подальших розвідок може бути оцінка ефективності взаємодії механізмів у реальних умовах кризових ситуацій та гібридних загроз, зокрема через моделювання сценаріїв реагування та аналіз практичних кейсів реалізації.

Література:

1. Ряполов А. П.. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Том 3 № 89. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/336476

2. Скочиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. Вісник Національного університету "Львівська політехніка". Серія "Юридичні науки". 2024. Том 11, № 2 (42), с. 151—158. URL: https://science.lpnu.ua/uk/law/vsi-vypusky/vypusk-11-nomer-2-42-2024/pravovi-mehanizmy-zabezpechennya-informaciynoyi-bezpeky-v

3. Гріщенко А. О.. Підходи до розуміння категорії "інформаційна безпека" та правові засади її забезпечення. Інформація і право. 2020. № 4 (35). URL: http://il.ippi.org.ua/article/view/221239

4. Брацук І.,.Кавин С. Міжнародне правове регулювання забезпечення інформаційної безпеки в рамках ООН. Вісник Київського національного університету імені Тараса Шевченка. Юридичні дослідження. 2023. № 125 (1), С. 21—26. URL: https://legal.bulletin.knu.ua/uk/article/view/590/745

5. Крушеніцький В.С.. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі. Наукові записки. Серія: Право. 2024. № 17. URL: https://pravo.-cusu.edu.ua/index.php/pravo/article/view/544

6. Балан С., Балан Л. та ін. Державна інформаційна політика в умовах гібридних загроз: правові та політичні аспекти. Соціально-правові студії. 2025. Т. 8, № 1. URL: https://sls-journal.com.ua/uk/journals/tom-8-1-2025/

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

derzhavna-informatsiyna-politika-v-umovakh-gibridnikh-zagroz-pravovi-ta-politichni-aspekti

7. Актуальні проблеми теорії та практики службово-бойової діяльності складових сектору безпеки та оборони в сучасних умовах: матеріали II Всеукр. наук. практ. конф. (м. Київ, 24 травня 2024 року). Київ: Київський інститут Національної гвардії України, 2024. 364 с. URL: https://surl.li/lnwxat

8. International cyber capacity building: global trends and scenarios. European Commission. 2021. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf

9. Mazzoccoli, Alessandro; Naldi, Maurizio. Optimal investment in cybersecurity under cyber insurance for a multibranch firm, Multidisciplinary Digital Publishing Institute. 2021. Vol. 9, Iss. 1. URL: https://www.econstor.eu/bitstream/10419/258114/1/risks-09-00024.pdf

10. Report to Congress. Cybersecurity and Financial System. Resilience Report. 2024. URL: https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf

11. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

References:

1. Ryapolov, A.P. (2025), "Regulatory and Legal Foundations of Information Security of Ukraine under Conditions of Hybrid Aggression", Scientific Bulletin of Uzhhorod National University. Series: Law, Vol. 3, No. 89, Available at: http://visnyk-pravo.uzhnu.edu.ua/article/view/336476 (Accessed: January 2026).

2. Skochylias-Pavliv, O. (2024), "Legal Mechanisms for Ensuring Information Security in Ukraine", Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, Vol. 11, No. 2 (42), pp. 151—158, Available at: https://science.lpnu.ua/uk/law/vsi-vypusky/vypusk-11-nomer-2-42-2024/pravovi-mehanizmy-zabezpechennya-informaciynoyi-bezpeky-v (Accessed: December 2025).

3. Hrishchenko, A.O. (2020), "Approaches to Understanding the Category of 'Information Security' and Legal Principles of Its Provision", Information and Law, vol. 4 (35), Available at: http://il.ippi.org.ua/article/view/221239 (Accessed: January 2026).

4. Bratsuk, I. and Kavyn, S. (2023), "International Legal Regulation of Information Security within the United Nations", Bulletin of Taras Shevchenko National University of Kyiv. Legal Studies, vol. 125 (1), pp. 21—26, Available at: https://legal.bulletin.knu.ua/uk/article/view/590/745 (Accessed: December 2025).

5. Krushenitskyi, V.S. (2024), "Public Authorities as Subjects of Formation and Implementation of National Security Policy in the Information Space", Scientific Notes. Series: Law, vol. 17, Available at: https://pravo.cusu.-edu.ua/index.php/pravo/article/view/544 (Accessed: January 2026).

6. Balan, S. and Balan, L (2025), "State Information Policy under Hybrid Threats: Legal and Political Aspects", Socio-Legal Studies, Vol. 8, No. 1, Available at: https://sls-journal.com.ua/uk/journals/tom-8-1-2025/derzhavna-informatsiyna-politika-v-umovakh-gibridnikh-zagroz-pravovi-ta-politichni-aspekti (Accessed: December 2025).

7. Kyiv Institute of the National Guard of Ukraine (2024), Actual Problems of Theory and Practice of Service and Combat Activities of the Security and Defence Sector Components in Modern Conditions: Proceedings of the II All-Ukrainian Scientific and Practical Conference (Kyiv, May 24, 2024), Kyiv, 364 p, Available at: https://surl.li/lnwxat (Accessed: January 2026).

8. European Commission (2021), International Cyber Capacity Building: Global Trends and Scenarios, Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf (Accessed: November 2025).

9. Mazzoccoli, A. and Naldi, M. (2021), "Optimal Investment in Cybersecurity under Cyber Insurance for a Multibranch Firm", Risks, Vol. 9, no. 1, Multidisciplinary Digital Publishing Institute, Available at: https://www.econstor.eu/bitstream/10419/258114/1/risks-09-00024.pdf (Accessed: January 2026).

10. Federal Reserve System (2024), "Cybersecurity and Financial System Resilience Report: Report to Congress", Available at: https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf (Accessed: November 2025).

11. National Institute of Standards and Technology (2024), "The NIST Cybersecurity Framework (CSF) 2.0", Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (Accessed: January 2026).

Отримано редакцією журналу / Received: 10.02.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 10.03.26

https://**nayka.com.ua**

Електронне фахове видання

ДЕРЖАВНЕ УПРАВЛІННЯ

удосконалення та розвиток

Виходить 12 разів на рік

включено до переліку наукових фахових видань України з питань ДЕРЖАВНОГО УПРАВЛІННЯ (Категорія «Б»)

Наказ Міністерства освіти і науки України від 28.12.2019 №1643

Спеціальність 281

e-mail: economy_2008@ukr.net

viber: +38 050 3820663