https://doi.org/10.31891/2307-5740-2026-352-5
УДК 35.072: 004.056
JEL classification: H11, K24, K42, L86

КИРИЧЕНКО Ганна
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0000-0003-1067-8758
e-mail: kabasis87@gmail.com

ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ СУЧАСНИХ ВИКЛИКІВ

У сучасних умовах глобальної цифровізації та зростання гібридних загроз питання інформаційної безпеки набувають критичного значення для функціонування держави та суспільства. Посилення інформаційного протиборства, кіберзагроз і маніпулятивного впливу на громадську свідомість актуалізує потребу у вдосконаленні механізмів публічного управління в цій сфері. У статті здійснено теоретико-правовий аналіз публічного управління у сфері інформаційної безпеки в контексті сучасних викликів. Розкрито сутність та зміст поняття «інформаційна безпека» як об'єкта публічного управління, а також визначено ключові підходи до розуміння категорії «публічне управління» у вітчизняній та зарубіжній науковій думці. Проаналізовано нормативно-правове забезпечення інформаційної безпеки, окреслено його структурні елементи та виявлено основні проблеми правового регулювання у цій сфері. Особливу увагу приділено характеристиці сучасних викликів інформаційній безпеці, серед яких виокремлено кіберзлочинність, інформаційні війни, поширення дезінформації, а також вразливість критичної інформаційної інфраструктури. Визначено роль органів публічної влади у формуванні та реалізації державної політики у сфері інформаційної безпеки, зокрема в частині забезпечення координації між інституціями, впровадження інноваційних управлінських підходів та підвищення рівня цифрової грамотності населення. У результаті дослідження обґрунтовано необхідність удосконалення механізмів публічного управління у сфері інформаційної безпеки шляхом гармонізації національного законодавства з міжнародними стандартами, розвитку інституційної спроможності органів влади та впровадження комплексного підходу до протидії сучасним загрозам. Зроблено висновок, що ефективне публічне управління у сфері інформаційної безпеки є ключовим чинником забезпечення національної безпеки, стійкості держави та захисту інформаційного суверенітету.

Ключові слова: публічне управління, інформаційна безпека, національна безпека, державне регулювання, цифровізація, дезінформація.

KYRYCHENKO Hanna
Open International University of Human Development "Ukraine"

PUBLIC ADMINISTRATION IN THE FIELD OF INFORMATION SECURITY: THEORETICAL AND LEGAL ANALYSIS OF CURRENT CHALLENGES

In the current conditions of global digitalization and the growth of hybrid threats, information security issues are becoming critical for the functioning of the state and society. The intensification of information confrontation, cyber threats, and manipulative influence on public consciousness actualizes the need to improve public governance mechanisms in this area. The article provides a theoretical and legal analysis of public governance in the area of information security in the context of modern challenges. The essence and content of the concept of "information security" as an object of public governance are revealed, and key approaches to understanding the category of "public governance" in domestic and foreign scientific thought are identified. The regulatory and legal support for information security is analyzed, its structural elements are outlined, and the main problems of legal regulation in this area are identified. Particular attention is paid to the characteristics of modern challenges to information security, among which cybercrime, information wars, the spread of disinformation, and the vulnerability of critical information infrastructure are highlighted. The role of public authorities in the formation and implementation of state policy in the field of information security is determined, in particular in terms of ensuring coordination between institutions, implementing innovative management approaches and increasing the level of digital literacy of the population. The study substantiates the need to improve public governance mechanisms in the field of information security by harmonizing national legislation with international standards, developing the institutional capacity of authorities and implementing an integrated approach to countering modern threats. It is concluded that effective public governance in the field of information security is a key factor in ensuring national security, state stability and protecting information sovereignty.

Key words: public administration, information security, national security, state regulation, digitalization, disinformation.

Стаття надійшла до редакції / Received 20.02.2026
Прийнята до друку / Accepted 26.03.2026
Опубліковано / Published 31.03.2026

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

У сучасних умовах стрімкої цифрової трансформації суспільства та держави суттєво зростає значення інформаційної безпеки як ключового елементу національної безпеки. Водночас розвиток інформаційно-комунікаційних технологій супроводжується появою новітніх загроз, зокрема кіберзлочинності, інформаційних атак, дезінформації та маніпулятивного впливу на суспільну свідомість, що створює додаткові виклики для системи публічного управління.

Проблема полягає у невідповідності існуючих теоретико-правових засад та управлінських механізмів публічного управління у сфері інформаційної безпеки сучасним умовам та динаміці загроз. Зокрема, спостерігається фрагментарність нормативно-правового забезпечення, недостатній рівень координації між суб'єктами публічної влади, обмеженість інституційної спроможності щодо ефективного реагування на інформаційні виклики, а також відсутність цілісного підходу до формування та реалізації державної політики у цій сфері.

Крім того, актуалізується потреба у науковому осмисленні категоріального апарату публічного управління в умовах цифровізації, уточненні змісту поняття інформаційної безпеки та визначенні ролі держави у забезпеченні стійкості інформаційного простору. Недостатня розробленість теоретико-правових аспектів ускладнює формування ефективних управлінських рішень та знижує рівень захищеності держави від сучасних інформаційних загроз.

Отже, існує об'єктивна необхідність комплексного теоретико-правового аналізу публічного управління у сфері інформаційної безпеки з метою виявлення ключових проблем та обґрунтування напрямів їх вирішення в умовах сучасних викликів.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз наукових досліджень і публікацій у сфері публічного управління інформаційною безпекою свідчить про значне зростання інтересу до проблематики забезпечення кіберстійкості держави та захисту інформаційного простору. У працях [1–3] основний акцент зроблено на теоретичних засадах публічного управління у сфері інформаційної безпеки, де автори досліджують категоріальний апарат, понятійно-термінологічні підходи та методологічні засади формування державної політики. Дослідження [4–6] присвячені аналізу сучасних викликів інформаційній безпеці, зокрема кіберзлочинності, інформаційних атак, дезінформації та вразливості критичної інформаційної інфраструктури, підкреслюючи необхідність адаптації управлінських механізмів до динамічного розвитку загроз.

У працях [7–8] значну увагу приділено нормативно-правовому забезпеченню та інституційним аспектам публічного управління інформаційною безпекою. Автори акцентують на важливості гармонізації національного законодавства з міжнародними стандартами, розвитку міжвідомчої координації та підвищення інституційної спроможності органів державної влади для ефективного протидій кіберзагрозам. Дослідження [9–10] підкреслюють роль міжнародного співробітництва та інтеграції національної політики у глобальні механізми кібербезпеки, наголошуючи на важливості міждержавної координації та обміну інформацією.

Разом із тим, у наукових працях інформаційна безпека здебільшого розглядається в окремих аспектах — технологічному, правовому або управлінському, що виявляє прогалини у комплексному підході до формування державної політики. Водночас відсутнє достатнє наукове обґрунтування інтеграції управлінських, правових та технологічних механізмів, а також адаптації їх до сучасних викликів інформаційного середовища. Це зумовлює потребу подальших досліджень, спрямованих на розроблення системних та комплексних стратегій публічного управління інформаційною безпекою.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на значну кількість досліджень у сфері публічного управління та інформаційної безпеки, залишаються невирішеними ряд важливих питань, що зумовлюють актуальність даної статті. Передусім, недостатня теоретична розробленість категоріального апарату — попередні дослідження здебільшого фрагментарно аналізують поняття «публічне управління» та «інформаційна безпека», не формуючи цілісної концептуальної основи для застосування у практиці державного управління. Також, фрагментарність нормативно-правового регулювання — існуюче законодавство часто не відповідає сучасним викликам, пов'язаним із кіберзагрозами, інформаційними атаками та дезінформацією, а механізми координації між державними органами залишаються недостатньо ефективними. Також, обмежена інституційна спроможність органів публічної влади — відсутність комплексного підходу до управління інформаційною безпекою ускладнює своєчасне виявлення та нейтралізацію загроз, а також упровадження превентивних заходів. Тому, недостатнє узгодження національної політики з міжнародними стандартами — проблемним залишається адаптація управлінських і правових механізмів до глобальних норм кібербезпеки та інтеграція найкращих практик зарубіжних держав.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є здійснення комплексного теоретико-правового аналізу публічного управління у сфері інформаційної безпеки в умовах сучасних викликів, а також обґрунтування напрямів удосконалення відповідних управлінських механізмів і нормативно-правового забезпечення з метою підвищення ефективності державної політики у цій сфері.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Сучасний етап розвитку суспільства характеризується стрімким зростанням ролі інформації та цифрових технологій у всіх сферах життєдіяльності, що зумовлює трансформацію підходів до забезпечення національної безпеки. У цих умовах публічне управління у сфері інформаційної безпеки набуває особливого значення як інструмент протидії новітнім загрозам та забезпечення стійкості держави й суспільства.

У сучасних умовах цифровізації та глобалізації інформаційна безпека набуває статусу одного з ключових елементів національної безпеки та водночас виступає важливим об'єктом публічного управління. У науковому дискурсі інформаційна безпека розглядається як стан захищеності інформаційного середовища, за якого забезпечується цілісність, конфіденційність, доступність інформації, а також стійкість до деструктивних інформаційних впливів. На відміну від вузького технічного трактування, сучасне розуміння інформаційної безпеки охоплює не лише кіберзахист, але й ширші аспекти, зокрема захист інформаційного суверенітету держави, протидію дезінформації та інформаційно-психологічним операціям, а також забезпечення стабільності суспільної свідомості [1].

Інформаційна безпека як об'єкт публічного управління характеризується комплексністю та багаторівневістю, тому її зміст доцільно розглядати через сукупність взаємопов'язаних компонентів (рис. 1).

Рис. 1. Основні компоненти інформаційної безпеки, як об'єкт публічного управління

Джерело: сформовано автором на основі даних [2]

Таким чином, інформаційна безпека у публічно-управлінському вимірі постає як інтегрована система, що поєднує політичні, правові, технологічні та соціальні інструменти впливу, спрямовані на захист національних інтересів в інформаційній сфері. Перехід до аналізу категорії публічного управління є логічно зумовленим, оскільки ефективність забезпечення інформаційної безпеки безпосередньо залежить від обраної моделі управління, характеру взаємодії між суб'єктами владних відносин та ступеня залучення недержавних акторів. Саме теоретичні підходи до розуміння публічного управління визначають інституційні рамки, механізми та інструменти реалізації політики у сфері інформаційної безпеки, що зумовлює необхідність їх ґрунтовного розгляду.

Категорія «публічне управління» є багатовимірною та характеризується різноманіттям теоретичних підходів як у вітчизняній, так і в зарубіжній науковій думці. Загалом публічне управління визначається як цілеспрямована діяльність органів державної влади, органів місцевого самоврядування та інших суб'єктів,

спрямована на реалізацію публічних інтересів, вироблення і впровадження політики, а також надання публічних послуг [3].

У вітчизняній науці можна виокремити кілька ключових підходів до розуміння цього феномена (рис. 2).

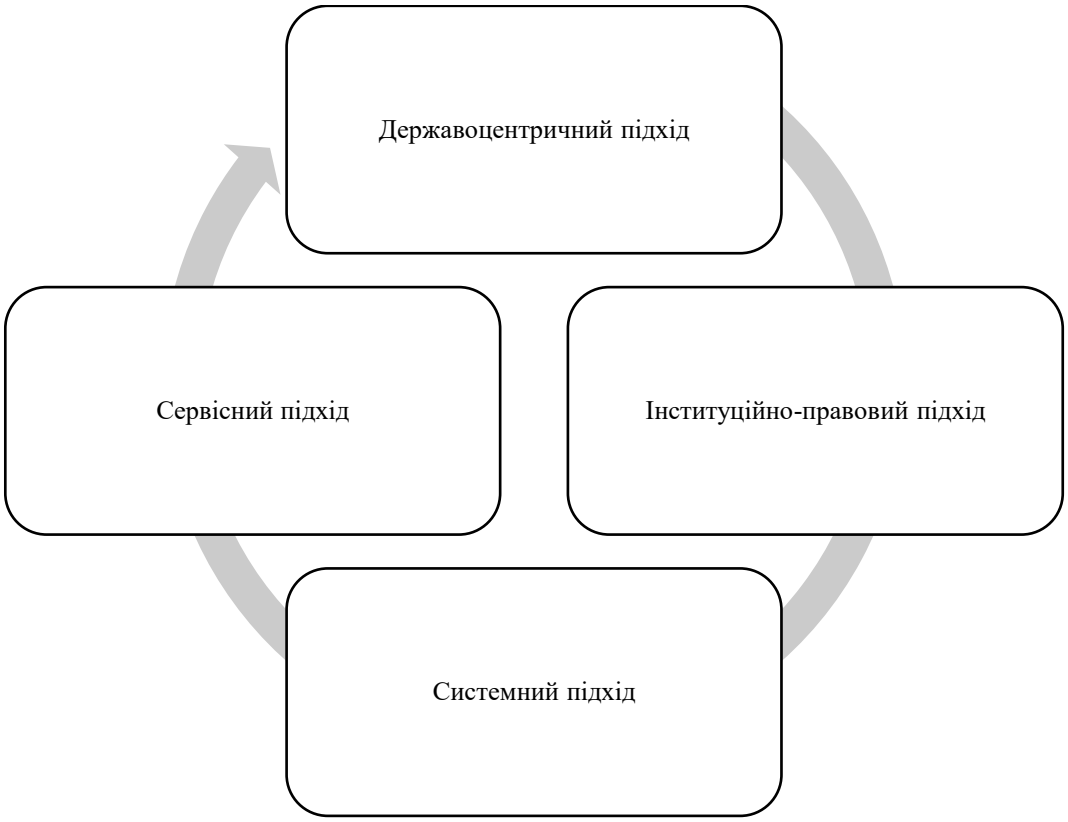

Рис. 2. Теоретичні підходи до розуміння сутності публічного управління у сфері інформаційної безпеки
Джерело: сформовано автором на основі даних [4]

Розглянемо кожний із даних підходів більш детальніше:

1. Державоцентричний підхід трактує публічне управління як діяльність передусім органів державної влади, акцентуючи увагу на владно-розпорядчих функціях та ієрархічній організації управління. У межах цього підходу держава виступає домінуючим суб'єктом формування та реалізації політики, зокрема у сфері інформаційної безпеки.

2. Інституційно-правовий підхід зосереджується на формальних правилах, процедурах та інститутах, які визначають механізми управлінської діяльності. У цьому контексті публічне управління розглядається як система нормативно закріплених взаємодій між суб'єктами.

3. Системний підхід інтерпретує публічне управління як складну відкриту систему, що функціонує через взаємодію держави, бізнесу та громадянського суспільства. Такий підхід є особливо релевантним для сфери інформаційної безпеки, де ефективність залежить від міжсекторальної координації.

4. Сервісний підхід (або публічно-сервісна модель) акцентує увагу на орієнтації держави на потреби громадян, розглядаючи її як надавача якісних і доступних послуг [5].

У такий спосіб, інформаційна безпека як об'єкт публічного управління є складним багатовимірним явищем, що потребує інтегрованого підходу до свого забезпечення. Її ефективне функціонування можливе лише за умови поєднання інституційних, правових, технологічних і соціальних механізмів.

Водночас сучасні підходи до публічного управління демонструють поступовий відхід від державоцентричних моделей до більш гнучких, мережевих і цифрово орієнтованих форм взаємодії. У цьому контексті забезпечення інформаційної безпеки вимагає застосування гібридних управлінських моделей, які поєднують державний контроль, міжсекторальне партнерство та інноваційні технологічні рішення.

Логічним продовженням розгляду інформаційної безпеки як об'єкта публічного управління є аналіз її нормативно-правового забезпечення, оскільки саме правові механізми визначають інституційні засади, інструменти та межі реалізації державної політики у цій сфері. Нормативно-правова база виступає системоутворюючим елементом, який забезпечує узгодженість дій суб'єктів публічного управління та ефективність протидії сучасним інформаційним загрозам (табл. 1).

Таблиця 1

Нормативно-правове забезпечення інформаційної безпеки: структура та проблеми

№	Структурний елемент	Зміст	Конкретні приклади для України	Основні проблеми правового регулювання
1	Конституційний рівень	Визначає базові принципи інформаційних відносин, права і свободи людини	Конституція України (свобода слова, доступ до інформації)	Декларативність норм, відсутність чітких механізмів реалізації в умовах інформаційної війни
2	Базове законодавство	Регулює інформаційні відносини, доступ до інформації, захист даних	Закони «Про інформацію», «Про доступ до публічної інформації»	Фрагментарність, дублювання норм, слабка адаптація до цифрових викликів
3	Спеціальне законодавство у сфері безпеки	Визначає засади кібербезпеки, інформаційної безпеки, захисту інфраструктури	Закон «Про основні засади забезпечення кібербезпеки України»	Вузька спеціалізація, недостатня інтеграція з іншими сферами безпеки
4	Стратегічні документи	Формують державну політику та пріоритети у сфері інформаційної безпеки	Стратегія інформаційної безпеки (2021), Доктрина інформаційної безпеки	Нечіткість механізмів реалізації, декларативний характер, слабкий моніторинг виконання
5	Підзаконні нормативні акти	Конкретизують процедури, стандарти, повноваження органів влади	Постанови КМУ, акти РНБО, відомчі інструкції	Надмірна кількість, неузгодженість між собою, складність практичного застосування
6	Міжнародно-правові акти	Визначають стандарти та зобов'язання у сфері інформаційної та кібербезпеки	Угоди з ЄС, стандарти NATO	Часткова імплементація, розрив між міжнародними стандартами та національною практикою
7	Правозастосовна практика	Реалізація норм у діяльності органів влади та судовій практиці	Діяльність СБУ, кіберполіції, судова практика	Низька ефективність правозастосування, брак спеціалізованої експертизи, складність доказування кіберзлочинів

Джерело: сформовано автором на основі даних [6]

Розширений аналіз нормативно-правових проблем у сфері інформаційної безпеки дозволяє більш глибоко виявити їх системний характер та взаємозв'язок, що суттєво впливає на ефективність державної політики у цій сфері. Передусім, фрагментарність правового регулювання проявляється у відсутності єдиного кодифікованого нормативного акту, який би комплексно охоплював усі аспекти інформаційної безпеки. Натомість правове поле складається з великої кількості розрізнених законів і підзаконних актів, що регулюють окремі сегменти — інформаційні відносини, кібербезпеку, захист персональних даних, державну таємницю тощо. Така розпорошеність призводить до колізій норм, дублювання положень і ускладнює їх практичне застосування, особливо в умовах гібридних загроз, які потребують комплексного реагування.

Технологічне відставання законодавства є ще однією критичною проблемою. Темпи розвитку інформаційно-комунікаційних технологій, зокрема штучного інтелекту, великих даних, хмарних сервісів і кіберзброї, значно випереджають швидкість оновлення нормативної бази. Як наслідок, законодавство часто не охоплює новітні види кіберзагроз, не визначає належним чином правовий статус нових технологій і не забезпечує ефективних інструментів реагування. Це створює правові прогалини, якими можуть користуватися як внутрішні, так і зовнішні суб'єкти деструктивного впливу [7].

Декларативність стратегічних документів полягає у тому, що значна частина стратегій і доктрин у сфері інформаційної безпеки містить загальні цілі та напрями політики без належної деталізації механізмів їх реалізації. Відсутність чітких індикаторів ефективності, конкретних виконавців, строків виконання та ресурсного забезпечення призводить до того, що такі документи мають обмежений практичний вплив і часто залишаються на рівні політичних намірів.

Не менш важливою є інституційна неузгодженість, яка проявляється у дублюванні повноважень між різними органами державної влади, що відповідають за забезпечення інформаційної та кібербезпеки. Відсутність чітко визначеної координаційної моделі призводить до розпорошення відповідальності, конкуренції між інституціями та зниження оперативності реагування на загрози. У кризових ситуаціях це може суттєво ускладнювати прийняття ефективних управлінських рішень. Проблеми імплементації міжнародних стандартів пов'язані з тим, що запозичення зарубіжного досвіду часто має формальний характер і не супроводжується належною адаптацією до національного правового, інституційного та соціально-політичного контексту. У результаті виникає розрив між задекларованими стандартами та реальною практикою їх застосування, що знижує ефективність міжнародного співробітництва у сфері інформаційної безпеки [8].

Нарешті, слабкість правозастосування залишається однією з найбільш проблемних сфер. Вона проявляється у недостатньому рівні інституційної спроможності органів влади, браку спеціалізованих знань і технічних ресурсів, а також складності доказування правопорушень у кіберпросторі. Додатковими чинниками

є низький рівень координації між правоохоронними органами та судовою системою, що ускладнює притягнення винних до відповідальності та знижує превентивний ефект правових норм.

Узагальнюючи, зазначені проблеми мають не ізольований, а взаємопов'язаний характер, що свідчить про необхідність комплексного реформування нормативно-правового забезпечення інформаційної безпеки, орієнтованого на системність, адаптивність та ефективність реалізації.

Заразом, необхідно з'ясувати ролі органів публічної влади у формуванні та реалізації відповідної державної політики. Такий підхід зумовлений тим, що ефективність правового регулювання безпосередньо залежить від інституційної спроможності суб'єктів публічного управління забезпечувати узгоджене, системне та адаптивне впровадження визначених норм у практичну площину. В даному контексті органи публічної влади постають як ключові суб'єкти формування політики у сфері інформаційної безпеки, виконуючи функції стратегічного планування, нормативного регулювання та організаційного забезпечення. Їх діяльність спрямована на визначення пріоритетів державної політики, інтеграцію питань інформаційної безпеки до системи національної безпеки, а також формування інституційного середовища, здатного ефективно реагувати на сучасні інформаційні загрози, що мають гібридний і транснаціональний характер.

Особливого значення набуває функція забезпечення міжінституційної координації, яка виступає необхідною умовою цілісності системи публічного управління у сфері інформаційної безпеки. З огляду на багатосуб'єктний характер цієї сфери, що охоплює органи виконавчої влади, силові структури, регуляторні органи, а також суб'єктів приватного сектору та громадянського суспільства, ефективна координація передбачає не лише розмежування повноважень, але й формування сталих механізмів взаємодії, обміну інформацією та спільного реагування на загрози. Відсутність належної координації зумовлює фрагментацію управлінських рішень, дублювання функцій і зниження оперативності реагування, що, у свою чергу, негативно впливає на загальний рівень інформаційної безпеки [9].

Не менш важливою є роль органів публічної влади у впровадженні інноваційних управлінських підходів, що відповідають викликам цифрової трансформації. Традиційні ієрархічні моделі управління поступово втрачають ефективність у динамічному інформаційному середовищі, що обумовлює необхідність переходу до гнучких, мережевих і технологічно орієнтованих форм управління. У цьому зв'язку актуалізується застосування інструментів цифрового врядування, використання аналітики великих даних для прогнозування та запобігання загрозам, а також розвиток публічно-приватного партнерства як механізму мобілізації ресурсів і компетенцій різних секторів. Така трансформація управлінських підходів сприяє підвищенню адаптивності державної політики та її здатності ефективно реагувати на швидкоплинні зміни у сфері інформаційної безпеки.

Водночас важливим напрямом діяльності органів публічної влади є формування належного рівня цифрової грамотності населення як складової соціальної стійкості до інформаційних загроз. У сучасних умовах громадяни виступають не лише об'єктами, але й активними суб'єктами інформаційного простору, що зумовлює необхідність розвитку їхніх компетентностей у сфері критичного мислення, безпечної поведінки в цифровому середовищі та протидії дезінформації. Реалізація відповідних освітніх і просвітницьких програм сприяє формуванню інформаційно стійкого суспільства, здатного мінімізувати вплив маніпулятивних інформаційних практик.

Доцільно зазначити, що органи публічної влади виконують системоутворюючу функцію у сфері забезпечення інформаційної безпеки, поєднуючи стратегічне бачення, координаційний потенціал та інноваційні управлінські інструменти. Їх ефективна діяльність є визначальним чинником формування цілісної, адаптивної та результативної державної політики, здатної забезпечити належний рівень захисту інформаційного простору в умовах сучасних глобальних викликів.

Отож, необхідно здійснювати удосконалення відповідних управлінських механізмів, адже така необхідність детермінована зростанням складності та гібридності сучасних інформаційних загроз, а також об'єктивною невідповідністю існуючих управлінських інструментів динаміці трансформацій інформаційного середовища. В даному контексті пріоритетного значення набуває гармонізація національного законодавства з міжнародними стандартами, яка повинна здійснюватися не шляхом формального запозичення правових норм, а через їх адаптацію до національних інституційних, правових та безпекових реалій. Йдеться про імплементацію кращих практик у сфері кібербезпеки, захисту персональних даних, протидії дезінформації та забезпечення стійкості критичної інформаційної інфраструктури. Така гармонізація сприятиме підвищенню сумісності національної системи безпеки з міжнародними безпековими архітектурами, а також посиленню участі держави у глобальних механізмах колективної протидії кіберзагрозам [10].

Водночас визначальним чинником ефективності публічного управління виступає розвиток інституційної спроможності органів публічної влади, що передбачає не лише вдосконалення організаційної структури та розмежування повноважень, але й підвищення кадрового, аналітичного та технологічного потенціалу відповідних інституцій. Особливої актуальності набуває формування спеціалізованих компетенцій у сфері кібербезпеки, стратегічних комунікацій та управління інформаційними ризиками, а також впровадження сучасних методів міжвідомчої взаємодії. Посилення інституційної спроможності дозволяє забезпечити належний рівень координації, оперативності та обґрунтованості управлінських рішень у сфері інформаційної безпеки. Не менш важливим напрямом є впровадження комплексного (системного)

підходу до протидії сучасним інформаційним загрозам, який передбачає інтеграцію правових, організаційних, технологічних і соціальних інструментів у єдину управлінську модель. Такий підхід базується на принципах міжсекторальної взаємодії, превентивності та адаптивності, що дозволяє не лише реагувати на наявні загрози, але й прогнозувати їх виникнення та мінімізувати потенційні ризики. Важливим елементом цього підходу є поєднання зусиль держави, приватного сектору та громадянського суспільства, що відповідає сучасним концепціям мережевого врядування.

Отже, удосконалення механізмів публічного управління у сфері інформаційної безпеки має здійснюватися на засадах комплексності, інституційної узгодженості та стратегічної орієнтованості, що дозволить забезпечити адекватність державної політики сучасним викликам інформаційного середовища. Також потрібно відмітити, що ефективне публічне управління у сфері інформаційної безпеки виступає ключовим чинником забезпечення національної безпеки, стійкості держави та захисту її інформаційного суверенітету. Саме здатність держави формувати та реалізовувати цілісну, адаптивну і науково обґрунтовану політику у цій сфері визначає її спроможність протистояти сучасним інформаційним викликам та гарантувати стабільний розвиток в умовах глобалізованого інформаційного простору.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Узагальнення результатів проведеного дослідження дає підстави констатувати, що інформаційна безпека в сучасних умовах постає як складний, багатовимірний об’єкт публічного управління, який інтегрує правові, інституційні, технологічні та соціальні компоненти. Її забезпечення виходить за межі вузькотехнічного розуміння та набуває системного характеру, охоплюючи питання національної безпеки, інформаційного суверенітету та стійкості суспільства до гібридних загроз.

Встановлено, що ефективність державної політики у сфері інформаційної безпеки значною мірою залежить від якості нормативно-правового забезпечення, яке на сучасному етапі характеризується фрагментарністю, технологічною інерційністю та недостатньою узгодженістю. Виявлені проблеми правового регулювання, у поєднанні з інституційною неузгодженістю та обмеженою ефективністю правозастосування, знижують здатність держави адекватно реагувати на динамічні інформаційні виклики.

Доведено, що ключову роль у подоланні зазначених дисфункцій відіграють органи публічної влади, які забезпечують формування стратегічних пріоритетів, координацію міжінституційної взаємодії, впровадження інноваційних управлінських підходів та розвиток цифрової компетентності населення. Їх інституційна спроможність та здатність до адаптивного управління виступають визначальними чинниками ефективності політики у сфері інформаційної безпеки.

Обґрунтовано, що подальший розвиток системи публічного управління у досліджуваній сфері потребує комплексного удосконалення, зокрема шляхом гармонізації національного законодавства з міжнародними стандартами, посилення інституційної спроможності органів влади та впровадження інтегрованого підходу до протидії сучасним інформаційним загрозам. Такий підхід має ґрунтуватися на принципах системності, міжсекторальної взаємодії та технологічної адаптивності.

Отже, ефективне публічне управління у сфері інформаційної безпеки є не лише функціональним елементом державної політики, але й стратегічним чинником забезпечення національної безпеки, стійкості держави та захисту її інформаційного суверенітету в умовах трансформації глобального інформаційного середовища.

Література

1. Єжеєв М. Система забезпечення національної безпеки як складова публічного управління країни. *Публічно-управлінські та цифрові практики.* 2024. Випуск 1. С. 45-54. https://doi.org/10.31673/2786-7412.2023.017089

2. Кочубей Л. О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). *Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса.* 2015. № 3. С. 220–237.

3. Бубела Т. З., Мельник М. Я., Назаровець О. Б., Рудик Ю. І. Аналіз визначень та нормативних вимог системи захисту об’єкта критичної інфраструктури. *Вісник ЛДУБЖД.* 2024. Випуск 29. С. 119-127.

4. Птахіна О.М. Державне управління забезпеченням національної безпеки в умовах воєнного стану.Інтеграція науки та практики управління в умовах соціокультурних трансформацій: зб. матеріалів ІІІ Міжнар. наук.-практич. конф. (25 квітня 2025 року, м. Полтава). м. Полтава : ДЗ «ЛНУ імені Тараса Шевченка», 2025. С. 293-297.

5. Пучков О. О. Нормативні засади правопорядку у сфері національної безпеки України. *Актуальні проблеми держави і права*. 2016. Випуск 77. С. 173-179.

6. Мазуренко Л. І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології».* 2022. № 42. С. 50–57. DOI: https://doi.org/10.26565/2220-8089-2022-42-08

7. Каляєв А. О. Теоретичні підходи щодо трансформації сучасних моделей державного управління у сфері безпеки та оборони. *Ефективність державного управління.* 2018. Випуск 1 (54). С. 13-19.
8. Сердюк І. А. Підходи публічного управління до інформаційної безпеки особистості. *Публічне урядування,* 2022. №3 (31). С. 53-59. https://doi.org/10.32689/2617-2224-2022-3(31)-7
9. Савченко О. С. Проблеми запровадження цифровізації у систему публічного управління. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування,* 2022. №3. С. 102-108
10. Пархоменко-Куцевіл О. І. Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування».* 2023. Випуск 3. С. 143-150. DOI: https://doi.org/10.32782/2786-5 681-2023-3.19

References

1. Ezheiev, M. (2024), "Systema zabezpechennia natsionalnoi bezpeky yak skladova publichnoho upravlinnia krainy", *Publichno-upravlinski ta tsyfrovi praktyky,* no. 1, pp. 45–54. DOI: https://doi.org/10.31673/2786-7412.2023.017089.
2. Kochubei, L. O. (2015), "Informatsiina bezpeka derzhavy: instrumenty zakhystu ukrainskoho informatsiinoho polia (na prykladi osoblyvostei informatsiino-komunikatsiinykh tekhnolohii u suchasnomu Donbasi)", *Naukovi zapysky Instytutu politychnykh i etnonatsionalnykh doslidzhen imeni I. F. Kurasa,* no. 3, pp. 220–237.
3. Bubela, T. Z., Melnyk, M. Ya., Nazarovets, O. B., Rudyk, Yu. I. (2024), "Analiz vyznachen ta normatyvnykh vymoh systemy zakhystu obiekta krytychnoi infrastruktury", *Visnyk LDUBZh*D, no. 29, pp. 119–127.
4. Ptakhina, O. M. (2025), "Derzhavne upravlinnia zabezpechennia natsionalnoi bezpeky v umovakh voiennoho stanu", *Integriatsiia nauky ta praktyky upravlinnia v umovakh sotsiokulturnykh transformatsii*: zb. materialiv III Mizhnar. nauk.-praktych. konf. (25 kvitnia 2025 roku, m. Poltava), Poltava: DZ "LNU imeni Tarasa Shevchenka", pp. 293–297.
5. Puchkov, O. O. (2016), "Normatyvni zasady pravoporiadku u sferi natsionalnoi bezpeky Ukrainy", *Aktualni problemy derzhavy i prava*, no. 77, pp. 173–179.
6. Mazurenko, L. I. (2022), "Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy", *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina, seriia "Pytannia politolohii"*, no. 42, pp. 50–57. DOI: https://doi.org/10.26565/2220-8089-2022-42-08
7. Kaliiaev, A. O. (2018), "Teoretychni pidkhody shchodo transformatsii suchasnykh modelei derzhavnoho upravlinnia u sferi bezpeky ta oborony", *Efektyvnist derzhavnoho upravlinnia,* no. 1 (54), pp. 13–19.
8. Serdiuk, I. A. (2022), "Pidkhody publichnoho upravlinnia do informatsiinoi bezpeky osobi", *Publichne uriaduvannia,* no. 3 (31), pp. 53–59. DOI: https://doi.org/10.32689/2617-2224-2022-3(31)-7
9. Savchenko, O. S. (2022), "Problemy zaprovadzhennia tsyfryzatsii u systemu publichnoho upravlinnia", *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia*, no. 3, pp. 102–108.
10. Parkhomenko-Kutsevil, O. I. (2023), "Problemy zabezpechennia natsionalnoi bezpeky v umovakh voiennoho chasu", *Naukovyi visnyk Vinnytskoi akademii bezperervnoi osvity. Seriia "Ekologiia. Publichne upravlinnia ta administruvannia*", no. 3, pp. 143–150. DOI: https://doi.org/10.32782/2786-5681-2023-3.19